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

Melanie L. Hersh*
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

Melanie L. Hersh

Abstract

This Note first presents a historical background of media regulations protecting children, and introduces COPPA. Next, it presents the arguments fueling the debate about who should regulate the Internet - the government or non-government entities. It then argues that in light of COPPA's shortcomings and faulty attempts to emulate regulations of other media, the government should step back and allow parents to maintain the bulk of regulatory responsibility. Finally, it suggests a future course of action for successfully regulating the Internet to protect children’s privacy while taking into account the Internet’s dissimilarity to previously regulated media. This Note concludes that although it may not be the perfect solution, giving responsibility for protecting children to parents and the Internet industry will best accomplish the goals underlying COPPA.

KEYWORDS: internet, children, privacy, regulate internet, protection, Child Online Privacy Protection Act, COPPA, pornography
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

Melanie L. Hersh*

The real danger is not pornography. The biggest danger is meeting strangers on line—being molested or killed.¹

INTRODUCTION

The Internet² is a rapidly growing tool that enables children and adults alike to instantly access information, resources, and other people.³ In addition to its role as an information provider, the Internet is a communication medium for thousands of political debates and social exchanges.⁴ Regulations of materials on and communication through the Internet have just begun to be issued. As a consequence, it is relatively easy for children to encounter...

---

¹ J.D. Candidate, 2002, Fordham University School of Law; MPhil (Oxon), 1999; B.A., Washington University, 1997. I would like to thank the fabulous editorial board and staff of the Fordham Urban Law Journal, Volume 28, for working so hard with me on this Note. I would like to give special thanks to my family for supporting me in all my endeavors.


materials that they would otherwise be carefully restricted from viewing. In fact, by using a Web browser and knowing how to type simple words, a child can easily come upon material many would find inappropriate.\(^5\) Parents find it difficult to restrict access, because children are often more savvy than their parents at finding and accessing Internet materials.\(^6\)

Past government regulations, both federal and state, have attempted to protect children from encountering pornographic materials on the Internet,\(^7\) but a child is at risk of encountering more than just pornography.\(^8\) There is also the risk of encountering dangerous people\(^9\) on bulletin boards\(^10\) or in chat rooms.\(^11\) The people children encounter, sometimes pedophiles, can lure them into disclosing personal information about themselves and their families.\(^12\) But unlike pornography, the threat posed by people luring children into dangerous situations is one that has not yet been dealt with by law enforcement or statutory regulation.

---

5. ACLU, 31 F. Supp. 2d at 476.
10. Bulletin boards are similar to large on-line servers, but they typically have fewer users and “cater to a wide range of specialized interests.” Edward A. CavaZos & Gavin Morin, *Cyberspace and the Law: Your Rights and Duties in the On-Line World* 3-4 (1994). Members of bulletin boards specializing in sexual topics were the first people concerned with pornography regulations. Id. at 89.
11. “Chat rooms provide additional online discussion forums that allow users to engage in real time dialogue with one or many other users by typing messages and reading the messages typed by others participating in the chat, analogous to a telephone party line, using a computer and keyboard rather than a telephone.” Cyber-space Communications, Inc. v. Engler, 55 F. Supp. 2d 737, 743 (E.D. Mich. 1999); see also Reno v. ACLU, 521 U.S. 844, 851-52 (1997).
Growing awareness of online predators has focused parental and governmental attention on the possible dangers the Internet poses for children and the apparent need for protection. In particular, many parents and privacy advocates think privacy regulation is needed to protect children from disclosing information about themselves and their families. But regulating the Internet cuts close to censorship.

Attempts to regulate the Internet are failing. Commentators and advocates disagree over who should be protecting children from the dangers of the Internet—the government, the Internet industry, or parents—and whether there even need be protection at all. The decision of which group should regulate is complicated not only by the legality of giving this power to one group, but, more importantly, by which group would be the most effective protector.

Many argue the government should not have any power to regulate the Internet; others believe government regulation will encourage new technological advances because people will have to be creative to conform to new laws. The Internet, according to

---

13. Jennifer Zwick, *Casting a Net Over the Net: Attempts to Protect Children in Cyberspace*, 10 *Seton Hall Const. L.J.* 1133, 1172 (2000) (recognizing that children under the age of thirteen are not considered able to understand the upshot of giving personal information to unknown compilers). It also has been shown that children are willing to exchange private family information for goods and services like prizes or free products. Michael Mahoney, *Report: Wired Kids Ready to Leak Private Info*, *E commerce Times*, para. 3, (Jan. 24, 2001) at http://www.newsfactor.com/perl/story/6942.html. The information given tends to be marketing information rather than something like a credit card number or Social Security number. *Id.* at para. 10.


some, can regulate itself better than any legislative action. Others counter that government is not subject to the same economic considerations that tend to jade industry regulations.

The Internet is a unique industry in that it consists of different communities of users, each holding different beliefs about what behavior and terminology is acceptable. People interact with the Internet differently than other previously regulated media. Unlike radio or television, with which a child need only flip a switch to be barraged with information, on the Internet a child must make a conscious effort to interact with someone or something. Unlike dial-a-porn phone lines, which are configured to discourage access by children, children are generally encouraged by parents and schools to interact with the Internet. This interaction is much more like the real world, and in that way, harder to regulate. Regulating Internet communication is like trying to regulate whom children can speak with on the street or playground.

There have been two major attempts to protect children's interests on the Internet, both of which have failed. The Communication Decency Act ("CDA") of 1996 and the Child Online Protection Act ("COPA") of 1997 dealt with the protection of children from exposure to obscene materials. Both of these laws mandated governmental control of regulatory issues on the Internet, and both were found unconstitutional. In response to these failed acts, The Child Online Privacy Protection Act of 1998 ("COPPA") was enacted in April 21, 2000 to deal with a different problem—privacy. COPPA grants more freedom to parents by

sumer Privacy Before the Government Steps In?, 54 Bus. Law. 349, 381-82 (1998) (calling to the industry to start regulating before the government steps in); Dawn A. Edick, Regulation of Pornography on the Internet in the United States and the United Kingdom: A Comparative Analysis, 21 B.C. Int'l & Comp. L. Rev. 437 (1998) (concluding that the government should regulate content on the Internet only to the extent it is regulated in other media); Keith J. Epstein & Bill Tancer, Enforcement of Use Limitations By Internet Services Providers: "How to Stop That Hacker, Cracker, Spammer, Spoof, Flamer, Bomber," 19 Hastings Comm. & Ent. L.J. 661, 667 (1997) (finding that because existing laws and lawmaking methods are inadequate, self regulation is the best answer).

17. See generally John S. Zanghi, "Community Standards" in Cyberspace, 21 U. Dayton L. Rev. 95 (1995) (arguing the Supreme Court needs to reconsider the traditional community standards test in obscenity cases because technological advances and computers have altered local communities into a global one).
allowing them to choose whether or not their children can access sites, in a way that is similar to regulation of other industries. However, it still places too much of the burden of regulation on website providers and the government, which leads to parental complacency. COPPA is not the answer; it is simply the latest failed attempt at statutory regulation, proving self-regulation to be far preferable to less useful statutes.\textsuperscript{22}

Part I of this Note presents a historical background of media regulations protecting children, explaining the atmosphere into which COPPA was born. This part also introduces COPPA and sets forth its goals. Part II presents the arguments fueling the debate about who should regulate the Internet—the government or non-government entities. Part III argues that in light of COPPA’s shortcomings and faulty attempts to emulate regulations of other media, the government should step back and allow parents to maintain the bulk of regulatory responsibility. Part IV then suggests a future course of action for successfully regulating the Internet to protect children’s privacy while taking into account the Internet’s dissimilarity to previously regulated media. This Note concludes that although it may not be the perfect solution, giving responsibility for protecting children to parents and the Internet industry will best accomplish the goals underlying COPPA.

\section{Protection of Children}

\subsection{Constitutional Basis for Protection}

Children cannot always protect themselves because they do not always recognize dangers that surround them.\textsuperscript{23} For this reason, it has been held that both parents and the government have a legal basis for protecting children.\textsuperscript{24} Traditionally, though, parents have been more actively responsible for regulating what their children

\textsuperscript{22} In this context, self-regulation is defined as “a system of Internet governance that relies on the private sector—the market—to lead in the definition of the rules that such a system will follow, and in the development and implementation of a set of mechanisms and activities that will support these rules and govern behavior.” \textsc{Paul A. Pierlot, Industry Canada, Self-Regulation of Internet Content: A Canadian Perspective} (1999), http://www.isoc.org/INET2000/cdproceedings/8k/8k_2.htm.

\textsuperscript{23} In terms of the Internet, “children can be easily persuaded through fun and inviting activities and visuals to submit private information about themselves, without realizing what they are giving.” \textit{Protecting Your Kids Online with Amy Aidman of the Center for Media Education} (July 20, 2000), at http://discuss.washingtonpost.com/wp-srv/zforum/00/aidman0720.htm [hereinafter Aidman].

\textsuperscript{24} “[T]here is a compelling interest in protecting the physical and psychological well-being of minors.” Sable Communications, Inc. v. FCC, 492 U.S. 115, 126 (1989).
Parents, in fact, have a distinct liberty interest in how their children are raised. As Justice Harlan explained in his dissent in Poe v. Ullman:

The home derives its pre-eminence as the seat of family life. And the integrity of that life is something so fundamental that it has been found to draw to its protection the principles of more than one explicitly granted Constitutional right. In addition, the government has the power to enact protective laws, and parents can find themselves legally accountable if they do not take all necessary steps to protect their children as prescribed by the government. Because children can access pornography and encounter dangerous people on the Internet, the government has a justification for regulating access to the Internet.

However, it is unclear whether this power extends to protection of children from people who solicit their personal information. All previous court holdings have related to a child’s encounters with preexisting materials, such as pornography; there has not yet been a court holding protecting a child from disclosing the child’s personal information. This would be much like a law that attempts to forbid a child from talking to strangers on the street; it is improbable that such a law would withstand judicial scrutiny.

B. History of Legislation

Governmental regulations protecting children now affect all different media industries, including the Internet. Each enactment has given differing amounts of power to either parents or the government. Although such regulatory efforts have been successful in

26. Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (holding that the liberty guaranteed by the Fourteenth Amendment includes the liberty to bring up children); see also Pierce v. Soc’y of Sisters, 268 U.S. 510, 534-35 (1925) (interpreting Meyer to stand for the liberty of parents to direct the upbringing and education of children under their control).
28. Id. at 551-52.
30. See Pierce, 268 U.S. at 534-35 (discussing why parents should take active roles in their children’s lives).
media such as radio, cable, and television, these regulations do not necessarily translate well to the world of the Internet.

All federal attempts to treat Internet regulation as an extension of telephone, cable, or even radio regulations have been challenged and struck down in court.\textsuperscript{32} Courts have recognized the Internet as a new technology, not subject to the same broadcast limitations found in other communications media.\textsuperscript{33} In fact, it has been noted that each media “is a law unto itself.”\textsuperscript{34} This is why each must be regulated separately, and often in different ways.\textsuperscript{35} “The Internet’s predecessors . . . television, radio, and telephone, presently offer the same global capability as the Internet, but are still comparatively easy to regulate.”\textsuperscript{36} In particular, the analogy to cable television and radio fails because the Internet’s loose regulatory system “is not ‘reasonably ancillary’ to the FCC’s obligation to regulate broadcasters or common carriers.”\textsuperscript{37} In addition, the costs of Internet use—including start-up costs and maintenance—are generally appreciably lower than those of other forms of mass media, so there are many more people who have access to this particular medium.\textsuperscript{38}

Internet regulation has faced further challenges in the courts. Grappling with the balance between protecting children from harm and preserving First Amendment rights has proven difficult. The two major attempts to protect children from accessing pornographic material on the Internet, CDA and COPA, were both found unconstitutional.\textsuperscript{39} The Supreme Court has expressly recognized the complexity of Internet regulation and the possibility that

\begin{itemize}
\item \textsuperscript{34} Kovacs v. Cooper, 336 U.S. 77, 97 (1949).
\item \textsuperscript{36} Shipchandler, \textit{supra} note 32, at 450.
\item \textsuperscript{38} ACLU v. Reno, 31 F. Supp. 2d 473, 482 (E.D. Pa. 1999).
\item \textsuperscript{39} \textit{Infra} Parts I.B.2.c. & d.
government may be overstepping its bounds attempting to regulate it: "[T]he Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not . . . interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion."40

Further, it is difficult to determine in which jurisdiction cases involving Internet regulation should be prosecuted, and whether these regulations even apply to websites outside of the United States.41 The United States government will face significant enough challenges in policing its own citizens' compliance with its Internet regulation, without assuming the additional burden of attempting to enforce compliance internationally. Additionally, it is not always clear who is to be held responsible for activity on the Web, the Web server, the Web provider, the website creator, or the government of the nation in which any of the three are based?

1. Protection of Children in Other Media

There have been numerous attempts, both successful and unsuccessful, to regulate children's interactions with offensive materials in other media.42 These attempts are an important starting point for understanding how the government regulates media in general, and why the government has been attempting to regulate the Internet in the manner it has.

a. Cable Television

Since its advent, cable television has offered a broader range of content than traditional networks, including channels broadcasting risqué and even pornographic programming. Protecting children from offensive cable programming became necessary because children were increasingly able to access pornographic materials at their discretion, from their own homes, simply by turning on the television.43 In its early attempts to regulate cable, however, the

---

41. Information that does not meet American standards of decency may easily be sent from another country that does not have the same standards. Edmund L. Andrews, Smut Ban Backed For Computer Net, N.Y. TIMES, Mar. 24, 1995, at A1. It is important to remember, though, that U.S. sites clearly dominate the children's Internet industry. Privacy Protections, supra note 9.
42. See Reno v. ACLU, 521 U.S. 844, 870-74 (1997) (noting the difficulty of defining the word "offensive").
government found it difficult to determine who was to be held responsible, and how to prevent a restriction of the programming to appropriate audiences only. In *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, the Supreme Court held that portions of the Cable Television Consumer Protection and Competition Act of 1992 offered the least restrictive means of shielding minors from indecent material because it permitted, rather than required, cable operators to allow or ban indecent programming over leased access channels. This successful governmental action was not struck down by courts, and gave more discretion to parents.

Another area of regulation with respect to cable television is the attempt to shield children from watching scrambled pictures on blocked cable channels, such as Playboy. Section 505 of the Communications Decency Act of 1996 ("§ 505") attempts to eliminate "signal bleed." The attempt was made by limiting the transmission of targeted programming to hours when children most likely will not be watching television. Playboy challenged the constitutionality of these restrictions, winning an injunction against the enforcement of § 505 until the matter could be heard by a three-judge panel. When the case was heard a month later, the temporary restraining order was lifted, and the preliminary injunction was denied. Two years later, the United States District Court for the District of Delaware found § 505 unconstitutional, holding the provision was not the least restrictive means available to address the issue of signal bleed. This decision was upheld by the Supreme Court.

---

955, 969 (1997) (observing that the Court chose to classify a regulation of cable television channels as a child protection measure, rather than one which fundamentally alters the regulatory framework of leased cable channels).

46. 518 U.S. at 753.
53. United States v. Playboy Entm't Group, 529 U.S. 803 (2000) (finding provision under which viewers could order signal blocking was an effective alternative to provi-
It is tempting to analogize the Internet to cable television. However, cable television is distinguished from the Internet by the limited amount of content that can be broadcast on its channels, a constraint resulting from the scarcity of broadcast frequencies. The Internet, by contrast, has unlimited broadcasting potential.\textsuperscript{54} In addition, cable industry regulations are not an appropriate analogy to Internet regulation because their own law—The Cable Communications Policy Act of 1984—governs cable communications.\textsuperscript{55}

\textbf{b. Radio}

Regulation of radio attempts to protect children from inadvertently encountering indecent broadcasts. Radio presents an even bigger regulatory problem than cable regulation, because radio may be accessed at no charge through cheap machinery, and is therefore harder for parents to control. The debate about regulation was sparked when a parent complained to the Federal Communications Commission ("FCC") that he and his child had encountered a George Carlin monologue entitled "Filthy Words" on the radio during daytime hours.\textsuperscript{56} In response, the Supreme Court held that the broadcast of indecent language at times of the day when children might be listening is inappropriate.\textsuperscript{57} This problem was particularly troubling because the radio may intrude into the home where the child may be part of the audience.\textsuperscript{58} Radio is held to a different standard than a communications medium like television, because while a child may just avert his or her eyes from the television set if something offensive appears, a child may not in the same way turn away from the radio to avoid something indecent being played.\textsuperscript{59}

In looking to protect children, the Court specifically limited the times of day when patently offensive broadcasts, as measured by contemporary communication standards, could air.\textsuperscript{60} They particu-


\textsuperscript{56} FCC v Pacifica Foundation, 438 U.S. 726, 729-30 (1978).

\textsuperscript{57} \textit{Id.} at 750.

\textsuperscript{58} \textit{Id.} at 749.

\textsuperscript{59} \textit{Id.} at 747 n.25; Cohen v. California, 403 U.S. 15, 21 (1971) (holding that restriction of speech is needless when a disinclined audience member may simply avert his or her eyes).

\textsuperscript{60} Pacifica, 438 U.S. at 731-32.
larly noted the FCC's suggestion that patently offensive broadcasts that had some literary, artistic, political, or scientific value would not be "indecent" in the late evening, but would be so during the day.61 The Court found that the FCC was warranted in concluding that indecent language, within the meaning of The Radio Act of 1927,62 was used in the challenged broadcast.63 This case was representative of the Court's general recognition that children need extra protection from this media source.64

c. Television

In *Action for Children's Television v. FCC* ("ACT I")65 the FCC's definition of "indecency" adopted in *FCC v Pacifica Foundation*66 was applied to television,67 and the decision was affirmed in *Action for Children's Television v. FCC* ("ACT II").68 Based on these holdings, the FCC is authorized to regulate content it deems indecent on television and radio through 18 U.S.C.S. §1464.69 Recognizing the need to protect children, the Court concluded that "[a]lthough the restrictions burden the rights of many adults, it seems entirely appropriate that the marginal convenience of some adults be made to yield to the imperative needs of the young."70

There also has been an attempt at self-regulation of television through use of V-chip technology.71 In response to growing wor-

---

61. *Id.* at 732 n.5.
65. 852 F.2d 1332 (D.C. Cir. 1988). In *Action for Children's Television v. FCC*, petitioners, who were public and commercial networks, broadcasters, journalists, and public interest groups, sought a review of an order in which the FCC adopted a new gauge for restraining "indecent broadcast material" only allowing the broadcasting of those materials between midnight and 6:00 a.m. *Id.* at 1334-35.
67. "We have upheld the FCC's generic definition of indecency in light of the sole purpose of that definition: to permit the channeling of indecent material, in order to shelter children from exposure to words and phrases their parents regard as inappropriate for them to hear." *Id.* at 1340.
68. 58 F.3d 634, 683 (D.C. Cir. 1995).
69. *Id.* at 667. The consequence of the regulation is that "whoever utters any obscene, indecent, or profane language by means of radio communication shall be fined not more than $10,000 or imprisoned not more than two years, or both." 18 U.S.C.S. § 1464 (1994).
70. *Action for Children's Television v. FCC*, 58 F.3d at 667.
71. The V-chip is technology that permits viewers to block programs according to their specific ratings. Andrea K. Rodgers, *United States v. Playboy Entertainment Group, Inc. and Television Channel Blocking Technology*, 400 Jurimetrics J. 499, 513.
ries about violence on television, the Telecommunications Act of 1996 includes a section about the use of lock-out technology. The Act requires all new televisions larger than thirteen inches to include a feature design that enables parents to block a channel or program. The bill also instructs the television industry to establish a rating system for violence and other distasteful content. While this legislation gives a choice to the parent, it is permissive and does not force a parent to regulate content.

The American Civil Liberties Union ("ACLU"), however, believes that the Telecommunications Act of 1996 will detach parents from the process of deciding what television programs they allow their children to watch. "Rather than support the development of independent private rating systems and technology, the President and Congress will force the broadcasters to comply with a singular, federally-controlled rating system." If parents have no part in rating programs they will, no doubt, have less incentive to use the V-chip technology that utilizes these ratings.

d. Dial-A-Porn

Regulation of the dial-a-porn industry is arguably the most analogous to Internet regulation. Courts often suggest that the Internet is most like this industry in terms of intrusiveness into the

---

76. Id. (quoting Daniel E. Katz, ACLU Legislative Counsel).
77. "Dial-a-porn" is the conventional way to refer to the industry consisting of telephone providers who offer "sexually oriented prerecorded telephone messages." Sable Communications, Inc. v. FCC, 492 U.S. 115, 117-18 (1989). Callers are charged a special fee for utilizing these services. Id. at 118. Through one phone number, as many as 50,000 people an hour can access a message lasting between thirty seconds and two minutes. Elizabeth J. Mann, Telephones, Sex, and the First Amendment, 33 UCLA L. REV. 1221, 1223 (1986).
lives of its users. A customer must proactively make a phone call to access a recorded dial-a-porn message. This is much like Internet contact, where a user must similarly proactively initiate contact with a particular website. Dial-a-porn is also similar to the Internet because regulations affect both children and adults. Also, the entities that control the mediums do not control the specific transmission channels.

Although these similarities have encouraged Internet regulation to follow the dial-a-porn model, the Internet is too broad to be restricted like Dial-a-porn. Dial-a-porn only accesses pornography, so restricting this industry only restricts access to pornography. With the Internet, on the other hand, both children and adults can encounter far more than pedophiles or pornography, including valuable information and helpful contact with peers. Restricting children's access to the Internet risks cutting them off from good as well as bad.

The Internet is also different from dial-a-porn because while the Supreme Court has ruled that access codes and credit card verification are the most effective means of regulating dial-a-porn lines, high costs prohibit the Internet from following suit. Finally, while

---


79. Sable, 492 U.S. at 127-28; see also Dial Info. Servs. Corp. v. Thornburgh, 938 F.2d 1535 (2d Cir. 1991) (requiring individuals who want to access dial-a-porn services to write requests with their company); Information Providers Coalition for Def. of the First Amendment v. F.C.C., 928 F.2d 866 (9th Cir. 1991) (finding that "there was no 'prior restraint' of speech in requiring users of dial-a-porn services to make advance requests for access or in requiring providers to notify telephone carriers that their material is sexually oriented").


82. See, e.g., Jennifer Egan, Lonely Gay Teen Seeking Same, N.Y. TIMES MAG., Dec. 10, 2000, at 110 (describing Internet chat rooms as a refuge for homosexual children). "[V]ia the Internet, gay teenagers are now able to partake of the normal Sturm und Drang of adolescent life, which before was largely off limits to them." Id. at 114.


84. Sable, 492 U.S. at 121.

85. For a discussion of why these costs are higher for Internet sites, see infra Part III.B.1.
dial-a-porn phone lines are governed by the rules of all telephone providers, no centralized organization oversees the Internet; rather the Internet is a "network of networks" with no one organization in control of what happens.⁸⁶

2. Protection of Children from Pornography on the Internet

The Internet is distinguishable from traditional media in important ways.⁸⁷ It allows users to interact with other users, and with various content.⁸⁸ Communication does not invade an individual's home;⁹⁹ rather, gaining access to information, or communicating with another, "requires a series of affirmative steps more deliberate and directed than merely turning a dial."⁹⁰ In addition, unlike radio or television, the Internet is not exclusively a means of commercial communication.⁹¹ It is a "unique and wholly new medium of worldwide human communication."⁹²

The conflict between law and technological advance further complicates issues involving the Internet. Technology continues to move forward at a speed much quicker than the law; legislatures are having a hard time keeping up.⁹³ Although a discrepancy exists between the law and technological reality,⁹⁴ the Supreme Court seems unaware of the speed at which things are moving.⁹⁵ Conse-

---

⁸⁸. ACLU, 929 F. Supp. at 843-44.
⁸⁹. Id. at 844.
⁹⁰. Id. at 845. These "affirmative steps," however, may still permit children to access pornography websites by mistake. For example, simply typing "amateur" into www.altavista.com causes explicit pictures to appear on the screen. One can imagine a scenario where a child might innocently type "amateur" into the search engine, perhaps trying to find an amateur radio club, and encounter these photos. Consider, as well, the fact that while www.whitehouse.gov is the U.S. Government website, www.whitehouse.com is a pornographic site. Mistakes can easily constitute "affirmative steps."
⁹¹. Id. at 842.
⁹². Id. at 844.
⁹⁴. Id. at 134 & n.108.
⁹⁵. Id. at 134.
quently, "cyberspace regulation results in lawmakers regulating an arena they do not completely understand."96

a. Use of Filtering Technology in Libraries

Many public libraries provide free Internet access to their patrons. The American Library Association has been clear that no matter what the content, there should be unrestricted access to information.97 Nevertheless, many libraries have installed filtering software on their computers to block access to certain websites.98 To date, no case on this issue has made it to the Supreme Court, but a recent decision in the Federal District Court for the Eastern District of Virginia found mandatory filtering in libraries to be unconstitutional.99 There might soon be a federal decision on this matter.100 There also have been a number of federal bills dealing with the issue, but these seem to indicate the federal government supports Internet filtering.101 In light of all this controversy and confusion, some libraries have taken the easy approach and have simply stopped providing Internet access altogether.102

96. Werst, supra note 54, at 224.
100. The ACLU and the American Library Association plan to file a lawsuit in a Pennsylvania federal court contending that the Children's Internet Protection Act violates First Amendment freedom of speech because it predicates receiving federal funding upon the addition of filtering devices to computers in schools. John Schwartz, Internet Filters Used to Shield Minors Censor Speech, Critics Say, N.Y. Times, Mar. 19, 2001 at A15. Even some makers of the filtering technology oppose mandatory filtering bills, because they believe that filtering should be an option, not a requirement. Id. Supporters of these bills, however, believe that protecting children's interests is the kind of compelling interest that justifies bills such as this. Id. According to Jeffery Pollock, a Republican who ran for Congress in Oregon last year, it seems clear that "the founding fathers would not want this to occur." Id.
102. Zwick, supra note 13, at 1153.
b. The Internet Industry Attempts at Self-Regulation

The Internet industry also has made some attempts to regulate itself. Some Internet search engines have taken measures to reduce the amount of objectionable material encountered, and many Internet Service Providers ("ISP’s") have provided filtering devices as part of their services.

There are also attempts, within the industry, to rate web pages in order to allow Internet users to filter content. The Platform for Internet Content Selection ("PICS"), for example, is an assemblage of industry standards designed to establish a labeling system for the Internet that gives the Internet user the power to filter objectionable materials. This rating and filtering technology, routinely compared to the V-chip, permits Internet providers or any third party to take any "PICS-compatible" document and give it their own rating. Then users can choose what rating system best suits their own needs. The most attractive aspect of measures such as PICS is that parents ultimately have the choice whether to implement them at all, and if so, to what extent.

Another example of an industry attempt at self-regulation is the seal program. The purpose of a seal is primarily to assure customers that the website on which the seal appears is abiding by its posted privacy policy. The best known seal providers are

103. For example, the search engine www.altavista.com has something called "Family Filter," where parents can regulate what may come up on searches.
104. America Online, for example, has "Parental Controls" that allows an account owner to alter the levels of access that each screen-name on that account is allowed to have. There are three basic restriction categories for children under 18. "Kids Only" restricts children to certain areas on AOL and the Internet (when accessed through AOL), targeted to children twelve and under. "Young Teen" is for children aged thirteen through fifteen, and provides more freedom than a "Kids Only" screen name, but does not provide full access to content or interactive features. "Mature Teen" allows the most freedom of all children's categories, allowing access to all AOL content and the Internet, except certain sites deemed for an adult—eighteen and over—audience. It is also possible to determine exactly who may send e-mail to a child user. For extra protection, a parent may create a screen name just for chat room usage that is blocked from receiving any e-mails. This ensures that a child will not receive unsolicited e-mails after chatting online. See generally AOL Anywhere, Parental Controls, at http://www.aol.com/info/parentcontrol.html (last visited Aug. 13, 2001).
105. Id. at 824, 838; Nesson & Marglin, supra note 93, at 124.
106. For a discussion on the V-chip, see supra notes 71-74 and accompanying text.
108. Id.
TRUSTe\textsuperscript{110} and BBB Online,\textsuperscript{111} which place their seals on web pages once a website has passed an application process. This makes it easy for Internet users to know immediately, upon entering a website, whether the site has the privacy protection for which they are looking.

c. Communications Decency Act (CDA)

The Communications Decency Act of 1996 was the first substantial attempt by the government to regulate the Internet with respect to the protection of children.\textsuperscript{112} The CDA endeavored to make illegal any telecommunications contact that was intended to send indecent and obscene materials to minors.\textsuperscript{113} It even included statutory good faith defenses for ISPs that sought to limit access by underage individuals.\textsuperscript{114} Yet it was generally argued that simple legislation was not fluid enough to cope with the rapidly changing nature of the Internet.\textsuperscript{115}

The ACLU immediately challenged CDA, arguing that the provisions that banned "indecent" and "patently offensive" speech transmitted online were unconstitutional. A week later, District Court Judge Ronald L. Buckwalter issued a temporary restraining order against enforcement of the provision, finding the portions in dispute unconstitutionally vague.\textsuperscript{116} The Federal District Court for the Eastern District of Pennsylvania in 	extit{ACLU v. Reno} ultimately found the CDA to violate the First and Fifth Amendments, as there was no way to determine the ages of persons accessing the information.\textsuperscript{117} The Supreme Court then upheld the ruling, finding that Congress violated the First Amendment by attempting to regulate

\begin{itemize}
\item[110.] See http://www.truste.org/about/truste/index.html (designating TRUSTe as "an independent non-profit organization dedicated to building consumer trust and confidence in the Internet" through a seal program).
\item[111.] See http://www.bbbonline.org (defining BBBOnline as a "subsidiary of the Council of Better Business Bureaus" whose "mission is to promote trust and confidence on the Internet through the BBBOnLine Reliability and BBBOnLine Privacy programs").
\item[113.] 47 U.S.C. § 223(a).
\item[114.] \textit{Id.} § 223(c)(2)(A)-(B).
\end{itemize}
content on the Internet. The Court found the statute was overbroad and lacked the precision needed to statutorily limit the First Amendment. The Supreme Court noted that the limitation and the economic burden of age verification “must inevitably curtail a significant amount of adult communication on the Internet.” The Supreme Court, in Reno v. ACLU, made the following statement about governmental control over Internet content:

As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

The Court, therefore, attested to the Internet's uniqueness and suggested any Internet restrictions should be held to the highest level of scrutiny.

d. Child Online Protection Act

The next year, Congress promulgated COPA, a law fashioned to resolve the problems with CDA that the Supreme Court pointed out in ACLU v. Reno. This act had a much narrower focus: it attempted both to limit commercial photographers from selling their work over the Internet to minors, and to deal with the problem of “teasers.” Generally, to comply with the law, a Web publisher of harmful material must restrict access to his work by

---

119. Id.
120. Id. at 877.
121. Id. at 885.
123. ACLU, 521 U.S. at 883-85.
125. As the court in ACLU v. Reno explains, by typing in innocent words, a child may encounter “teasers,” which are “free sexually explicit images and animated graphic image files designed to entice a user to pay a fee to browse the whole site.” ACLU v. Reno, 31 F. Supp. 2d 473, 476 (E.D. Pa. 1999).
126. Harmful material is defined as:
   any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—
   (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
   (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual conduct, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
requiring proof of age by one of the following measures: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology." \(^{127}\)

The plaintiffs in *ACLU v. Reno* \(^{128}\) argued that COPA was unconstitutional in general and as applied directly to them as adult Internet users. \(^{129}\) They not only found COPA "vague, overbroad, and a direct ban on speech," but also found that affirmative defenses did not alleviate this burden because there was still an "economic and technological burden on speakers which result[ed] in loss of anonymity to users and consequently loss of users to its Web sites." \(^{130}\) The plaintiffs also argued that this act would result in an overall chilling of speech on the Web because of its over-broad nature. \(^{131}\)

The court found that the text of COPA does not limit its relevance to commercial photographers, but rather imposes liability on any commercial transaction that may involve any materials harmful to minors. \(^{132}\) "It logically follows that [COPA] would apply to any Web site that contains only some harmful to minors material." \(^{133}\) The court held that a proof of age requirement places an undue economic burden on publishers, who would have to pay for screening systems, and who could lose users who didn’t want to register:

> [There is] no way to restrict the access of minors to harmful materials in chat rooms and discussion groups . . . without screening all users before accessing any content, even that which is not harmful to minors, or editing all content before it is posted to exclude material that is harmful to minors. \(^{134}\)

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


127. *Id.* at § 231(c)(1)(A)-(C). This wording leaves room for technological advances, but at the same time is vague enough so that noncompliance is unlikely.


129. *Id.* at 478 (arguing that regulation of speech to protect children “threatens a large amount of speech that is protected as to adults”).

130. *Id.* at 479.

131. *Id.*

132. *Id.* at 480.

133. *Id.*

134. *Id.* at 495.

135. *Id.*
The Court also recognized that COPA would not prevent children from accessing harmful materials on "foreign Web sites, non-commercial sites, and online via protocols other than http," thereby demonstrating the failings of the statute.\textsuperscript{136} The court further concluded that this was not the least restrictive way to protect children from harmful materials.\textsuperscript{137}

In \textit{ACLU v. Reno}, the Supreme Court found COPA unconstitutional on free speech grounds.\textsuperscript{138} The Court recognized two possible remedies for the defects: the Court could assign a more narrow meaning to the statute, or delete the unconstitutional part of the statute while retaining the rest.\textsuperscript{139} Both of these options were found unsatisfactory.\textsuperscript{140} The Court found that COPA was "more likely than not to be found unconstitutional as overbroad on the merits," but expressed faith in the feasibility of congressional regulations to protect minors with the use of evolving technology.\textsuperscript{141} The ruling here shows the difficulty in regulating the Internet without infringing on First Amendment rights.

3. Protecting Children's Privacy on the Internet

There is no broad privacy protection in the United States, despite the fact that the Supreme Court has described privacy as "implicit in the concept of ordered liberty."\textsuperscript{142} There is a collection of diverse privacy laws focusing on specific issues.\textsuperscript{143} There is no specific constitutional right to privacy, but rather "various provisions of the United States Constitution limit state and federal government activities affecting the individual's disclosural privacy."\textsuperscript{144} Privacy is protected through state and federal legislation, common-law, and self-regulation,\textsuperscript{145} and the extent of this protection depends on what information is taken, by what methods, and for what

\textsuperscript{136} Id. at 496.
\textsuperscript{137} Id. at 497.
\textsuperscript{138} 217 F.3d 162, 181 (3d Cir. 2000).
\textsuperscript{139} Id. at 177.
\textsuperscript{140} Id. at 179.
\textsuperscript{141} Id. at 181.
\textsuperscript{144} \textit{Law of Privacy Rights in a Technological Society} 14 (Irving J. Sloan ed., Legal Almanac Series No. 15, 1986).
province. There is no doubt, though, that Internet privacy rights are not, as of yet, specifically defined, and must be balanced against "other competing interest of the public, law enforcement, government agencies and private commercial interests." At the same time, Internet privacy rights certainly exist, and like all other privacy rights, can only be sacrificed for a "compelling state interest."

The uniqueness of the Internet situates the government on unfamiliar ground, making regulation difficult to enact. The government must acknowledge that the Internet is both more powerful and more expensive to maintain than other kinds of media. However, regulation is needed because the tools required to use the Internet are inexpensive and easy to obtain, making the media accessible to almost anyone. The fact that e-mail communication can be transmitted from location to location, worldwide, with no barriers, and that bulletin board postings reach thousands of Internet users daily, makes this medium particularly hard to regulate.

Efforts to protect children's privacy online generally have focused on the interest of the parent. Not only have parents been given the constitutional right to protect their children, but they are also in charge of the control and use of information found in

146. Friedman, supra note 14, at 41.
147. Law of Privacy Rights in a Technological Society, supra note 144, at 16.
148. Friedman, supra note 14, at 41.
149. Carey v. Population Servs. Int'l, 431 U.S. 678, 688 (1977) (finding that regulations infringing on this privacy interest may be justified only by a "compelling state interest" and must be narrowly drawn to respond to only those interests).
151. Id.
152. Id. In fact, even families that do not own computers can often gain Internet access at work, school, the public library, or Internet cafes. Joe Sharkey, Sales on Online Corporate Booking Systems Are Seen Growing Eightfold, to $33 Billion, by 2005, N.Y. Times, Feb. 7, 2001, at C8 (finding that "by 2005 ... 63 million employees, or about 46 percent of the domestic workforce will have full Internet access at work"); Editorial, Internet Access for Schools, N.Y. Times, May 15, 1999, at A16 (discussing the e-rate program that provides government funding for Internet hook-ups in libraries and schools in order to provide access to poorer areas); Jenny Holland, An Internet Entree with Beverages, N.Y. Times, Jan. 7, 2001, at 14:4 (explaining that Internet cafes are opening specifically for the "average guy who works in a McDonald's [and] doesn't have Internet access").
153. See generally Henry H. Perrit, Jr., Cyberspace and State Sovereignty, 3 J. Int'l Legal Stud. 155, 161 (1997) (discussing how the Internet derives uniqueness as a communications medium from its ease of access and low barriers to broadcasting).
154. Zwick, supra note 13, at 1160.
155. Supra Part I.A.
their children's educational records. Regulations protecting children on the Internet must not take away this important parental right.

Internet providers seek to obtain information from children in a number of ways. The most common procedure is requiring a child to reveal personal information in order to interact with cartoon characters, enter contests and drawings, obtain access to chat rooms, register to play a game, or obtain an e-mail address. Children's information can be disseminated even more directly than that. For example, by requiring children to list their name and address when writing on a bulletin board, or by simply having someone ask for their addresses in a chat room.

The validity of the movement to protect children's privacy on the Internet is reinforced by the fact that adults are lobbying for protection for themselves as well. A group of recent cases illustrates that adults have objected to their personal information being shared without their consent. In re Doubleclick Inc. Privacy Litigation, for example, deals with the issue of Web browsers surreptitiously downloading "cookies" onto people's computers in order to track people's "surfing" through the Internet. DoubleClick, an advertising and consumer data tracking firm, had been compiling anonymous data about people's "surfing" around

158. Ironically, this is something the government website asks them to do. Infra Part III.B.
162. A cookie, in computer terms, is a file placed on the hard drive of a computer while one is surfing the Internet that "allow[s] Web sites and advertising networks to monitor our online movements." Id.
163. For a general discussion about how a user's path through the Internet can be tracked, stored, and compiled, see FED. TRADE COMM'N, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS 3-4 (1997), available at http://www.ftc.gov/os/1997/9712/irs.pdf.
the Internet. It subsequently started to link this data to people's names and addresses found in a newly acquired database.164 Many argue this is an invasion of privacy.165 Still others have no idea this is even going on,166 which may be even more dangerous.

The abuse of children's information has also resulted in litigation. There is documentation on pedophiles using chat rooms to communicate with children. In Hatch v. Superior Court of San Diego County,167 for example, a man was prosecuted for sexually propositioning two children (really an undercover policewoman pretending to be two thirteen year old girls) over the Internet by sending lewd photos and other pornographic materials.168 There are other similar cases.169 In one shocking scenario, when the popular Internet server NBCi.com shut down all of the e-mail accounts of people registered as being under thirteen, hundreds of adult men complained their accounts had been shut down without warning.170

a. Child Online Privacy Protection Act

For years before the enactment of The Child Online Privacy Protection Act ("COPPA" or "the Act"), activist groups called for some legislation to protect children's privacy on the Internet. The Center for Media Education,171 for example, published a report in 1996 called "Web of Deception," documenting online marketing and data collection practices directed at children.172 This study

165. "I'm appalled at Doubleclick's approach to this . . . . It's clear they did it with no sensitivity whatsoever to people's privacy. They were just testing the waters to see if they could get away with it." Id. (quoting David Shenk).
166. See id.
168. Id. at 178-81.
169. Adams, supra note 159, at 414 n.74.
171. The Center for Media Education is "a national nonprofit organization dedicated to creating a quality electronic media culture for children and youth, their families and the community . . . focus[ing] on the potential—and the peril—for children and youth of the rapidly evolving digital media age." See http://www.cme.org/about.html.
prompted a Federal Trade Commission ("FTC") investigation of online marketing practices that ultimately lead to the enactment of COPPA.\(^\text{173}\) COPPA was designed to tackle two problems: "(i) overmarketing to children and collection of personally identifiable information from children that is shared with advertisers and marketers, and (ii) children sharing information with online predators who could use it to find them offline."\(^\text{174}\)

COPPA, the newest law attempting to protect children's interests on the Internet, was enacted on October 21, 1998.\(^\text{175}\) The Child Online Privacy Protection Rule ("the Rule") implementing COPPA became effective on April 21, 2000.\(^\text{176}\) The Act was developed to "enhance parental involvement in a child's activities online, protect the safety of a child while participating in online locations such as chat rooms, secure a child's personally identifiable information collected online, and limit information collection from a child absent parental consent."\(^\text{177}\) COPPA is concerned with all information collected from children\(^\text{178}\) on websites targeted towards children,\(^\text{179}\) or general websites where the operators\(^\text{180}\)

\(^{173}\) FTC—Privacy Online, supra note 12, at 23 fig.1 & 27 fig.4 (finding that while ninety-two percent of comprehensive websites collect personal information, only approximately fourteen of them disclose this practice).

\(^{174}\) Privacy Protections, supra note 9.


\(^{176}\) The FTC held a workshop to respond to concerns about how to effectively and practically obtain parental consent in compliance with COPPA. Fed. Trade Comm’n, Children’s Online Privacy Protection Rule Public Workshop, available at http://www.ftc.gov/privacy/chonlpritranscript.pdf [hereinafter Workshop]. In October 1999, the FTC released the Children’s Online Privacy Protection Rule. 16 C.F.R. 312 (2000). The Rule provides website operators with guidelines on how to comply with COPPA’s requirements. Id.


\(^{179}\) Generally, this can mean two things, “(i) a commercial website or online service that is targeted to children; or (ii) that portion of a commercial website or online service that is targeted to children.” 15 U.S.C.A. 6501(10)(A). It must be noted, however, that a commercial website or online service, or a portion of one, will not be considered to be directed towards children if it is simply linked to a site directed to children. Id. § 6501(10)(B).
have knowledge that children visit the site.\textsuperscript{181} The five key requirements of COPPA are: (1) notice, (2) parental consent, (3) parental review, (4) limits on the use of games and prizes and (5) security.\textsuperscript{182}

COPPA addresses these issues by placing restrictions on the practice of soliciting personal information from children online.\textsuperscript{183} In general, the Act requires that operators of children-focused websites that collect information provide notice on the site as to what kind of information is collected and how it is used.\textsuperscript{184} However, this does not apply to the information given out willingly by the children.\textsuperscript{185} Therefore, such information is dealt with by requiring parental consent\textsuperscript{186} for the collection, use, or disclosure of personal information\textsuperscript{187} from children. Consent may be obtained through "any reasonable effort."\textsuperscript{188} The Act also states that children focused Internet sites cannot condition participation on the

\textsuperscript{180} An "operator" is any person or company that operates a website or on-line service for commercial purposes, and that collects personal information about users. \textit{Id.} \S 6501(2). It does not include a nonprofit entity that would "otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act." \textit{Id.} \S 6501(2)(B).

\textsuperscript{181} Id. \S 6502(a)(1).

\textsuperscript{182} Laurel Jamtgaard, \textit{Symposium on Internet Privacy: Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act}, 16 \textsc{Santa Clara Computer} & \textsc{High Tech.} L.J. 385, 388 (2000).

\textsuperscript{183} 15 U.S.C. \S 6501(2).

\textsuperscript{184} \textit{Id.} \S 6502(b)(1)(A)(i).

\textsuperscript{185} See id.

\textsuperscript{186} "Parental consent" is meant to ensure that "a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices." \textit{Id.} \S 6501(9). It also authorizes the "collection, use, and disclosure" of the information and subsequent use of the information. \textit{Id.} If requested, the parent of a child who has provided personal information to a website may ask for:

(i) description of the specific types of personal information collected from the child by that operator; (ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and (iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child. \textit{Id.} \S 6502(b)(1)(B).

\textsuperscript{187} "Personal information" is defined as individually identifiable information about a person collected online. \textit{Id.} \S 6501(8). This includes:

(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of the child that the website collects online from the child and combines with an identifier described in this paragraph. \textit{Id.}

\textsuperscript{188} \textit{Id.} \S 6501(9). This includes a request for authorization for future collection, use, and disclosure described in this notice before the information is collected. \textit{Id.}
site on requiring the disclosure of more personal information than necessary to participate. Finally, it requires operators of these sites to establish procedures that will best protect the collected information.

There are certain exceptions to COPPA's rules, as well as the "safe harbor" provision, which protects websites that work to protect themselves. Parental consent, for example, is not necessary when the operator collects personal information for the sole purpose of "respond[ing] directly on a one-time basis to a specific request from the child and is not used to re-contact the child," or when personal information is needed in order to contact the parent to get permission. Under the "safe harbor" provision, websites can submit themselves to the FTC for approval.

In order to address the financial concerns of some of the smaller websites, the FTC, in the Rule, adopted a sliding scale. In the best case scenario, this would allow an operator to use varying consent mechanisms depending upon how the information collected would be used. However, any violation of these provisions would cost an offender $11,000, and empowers courts to grant injunctive or other equitable relief.

Concerns about COPPA were addressed at a public workshop hosted by the FTC in July of 1999. These concerns were prophetic, deducing many of the problems that would eventually be encountered. There were concerns about consent, and about how costly COPPA would be for smaller-sized websites. There were also concerns about how to obtain parental consent. All of these things would eventually become the Act's greatest weaknesses.

---

189. Id. § 6502(b)(1)(C).
190. Id. § 6502(b)(1)(D).
191. Id. § 6502(b)(2).
192. Id. § 6503.
193. Id. § 6502(b)(2)(A).
194. Id. § 6502(b)(2)(B).
195. Id. § 6503(a).
196. The Rule set up a sliding scale with respect to obtaining consent, based upon what the information collected will be used for. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(b)(2) (1999).
197. Id.
199. Workshop, supra note 176.
200. Id. at 15-16.
201. Id. (all three panels discuss the problems and solutions regarding attaining parental consent).
II. Government Regulation v. Self-Regulation

Every time an Internet regulation is enacted, the same issue arises: who should have the ultimate power, the government-through laws, or non-government entities-through self-regulation. The pros and cons of having either one regulate must be weighed anew for each prospective regulation because with each new law comes new issues. COPPA is the first Internet privacy regulation focused on children, so although certain regulatory issues have been debated in the past, each must now be dealt with in a new context.

A. Arguments Against Governmental Control

Some argue there should be no government regulation of the Internet, even with regard to issues of indecency. Existing laws in other media fields are presumably too static for the dynamic nature of the Internet. Many people fear the government will impede the Internet’s development by enacting laws that are too restrictive. This fear is heightened by the Government’s ignorance of the Internet and the Internet industry. People wary of government regulation contend there are other successful ways to ensure certain materials do not fall into the hands of children.

Although it is true that in the off-line world the government can regulate where pornography is placed both within a locality and within a store, there is no regulation of what a child may encounter on the street or with whom he might speak. The most obvious solution to protecting children’s privacy is to restrict Internet access to minors. But if we don’t keep children constantly off the


204. Supra notes 103-111 and accompanying text.


206. Parents, for generations, have let their children onto the streets with only the advice of “Don’t talk to strangers.” In fact, some people think it is even better for children to interact with strangers than to have no interaction at all. Gavin de Becker, Protecting the Gift: Keeping Children and Teenagers Safe (And Parents Sane) 79-90 (1999) (contending that kids who don’t talk to strangers are actually at greater risk of being victimized by a predator).
streets for fear of what or whom they might encounter, why would we keep children off the Internet for the same reason?

Another serious problem with enacting laws to regulate the Internet is that different counties and states have conflicting laws regarding the Internet that are difficult to navigate; finding jurisdiction to enforce foreign regulations can be tricky.\textsuperscript{207} There is practically no way of finding out if people are in compliance with the laws, so enforcement seems unlikely. The government cannot monitor parents or children to ensure they are doing what they should be doing, or what they say they are doing, so many laws regarding the Internet go widely unenforced.

Lastly, government regulation of the Internet does not allow parents to have enough control over what their children see or hear, and this kind of control has been constitutionally placed in their hands.\textsuperscript{208} As the court held in \textit{Action for Children's Television v. FCC},\textsuperscript{209} letting the government control what channels a child can watch infringes upon the rights of parents to raise their children.\textsuperscript{210} In \textit{FCC v. Pacifica Foundation},\textsuperscript{211} the Court held the government may not control children's access to materials contrary to the wishes of their parents.\textsuperscript{212} These two cases stand for the proposition that parents, not governments, need the power to control the actions of children when it comes to interactions with media.

\textbf{B. Arguments for Governmental Control}

There are also arguments for allowing the government to regulate the Internet. Government officials make it a point to know the

\textsuperscript{207} An example of this is found in a recent French case involving a court's attempt to prevent all French Internet users from accessing an American auction website that sells Nazi memorabilia. \textit{Union Des Etudiants Juifs de France/Ligue Contre le Racisme et L'Antisémitisme — LICRA v. Yahoo! Inc./Yahoo France [French Union of Jewish Students/ League Against Racism and Antisemitism — LICRA v. Yahoo! Inc./Yahoo France], Tribunaux de grande instance [T.G.I.] [County Court] Paris, May 22, 2000, [unpublished], J. Gomez. Rejecting the argument to dismiss the case for lack of jurisdiction, the judge called for the website to use available technology to identify French users, and restrict their use as much as possible. \textit{Id.} The French court reaffirmed this decision in November, 2000, \textit{Ligue Contre le Racisme et L'Antisémitisme — LICRA/Union Des Etudiants Juifs de France v. Yahoo! Inc./Yahoo France [League Against Racism and Antisemitism — LICRA/French Union of Jewish Students v. Yahoo! Inc./Yahoo France], T.G.I. Paris, Nov. 20, 2000, [unpublished], J. Gomez, as did a California U.S. District Court in 2001, Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, 145 F.Supp.2d 1168 (N.D. Cal. 2001).

\textsuperscript{208} \textit{Supra} Part I.A.

\textsuperscript{209} 58 F.3d 654 (D.C. Cir. 1995).

\textsuperscript{210} See \textit{id.} at 657.

\textsuperscript{211} 438 U.S. 726 (1978).

\textsuperscript{212} 438 U.S. at 750.
issues relevant to the public. Because people lobby the government, the legislatures are also likely to be informed of technological advances affecting these laws. In addition, government has a mechanism of enforcement immediately built into its laws, unlike industry regulations that have no legal authority. The government has the manpower and funds to enforce its own laws, which keeps it from needing to employ help from other channels.

It also has been seen that when people are forced to stay within the bounds of a law, they tend to become more creative when dealing with compliance. Consider the filtering devices developed in response to CDA\textsuperscript{213} and the new measures already developed to gain parental consent since the enactment of COPPA.\textsuperscript{214} Parental consent may be verified in a variety of ways: having parents sign a form and send, e-mail, or fax it back; asking parents for credit card numbers to verify their identities; maintaining a toll-free phone number parents can call in order to give consent; accepting e-mails that contain parents' digital signatures or other digital certificates that use "public key technology."\textsuperscript{215} These kinds of innovations strongly indicate that if there is government regulation, there will be many more technological advances providing ways to comply with these regulations.

On the other hand, there are many parents who simply do not understand the dangers of the Internet well enough to protect their children, and many who do not believe in the dangers about which they are warned. Many parents still do not use the Internet and others are apathetic about its potential threat.\textsuperscript{216} Because of this, the government may be better suited to regulate activities on the Internet, because it knows what dangers need to be addressed and has an interest in curtailing violations of its own laws.

\begin{itemize}
\item \textsuperscript{213} Infra note 222.
\item \textsuperscript{214} Id.
\item \textsuperscript{215} Id.
\item \textsuperscript{216} Seventy-five percent of adults still do not use e-mail. Chris Stamper, \textit{Post Office Proposes .us Mail}, ABCNEWS.COM, at http://abcnews.go.com/sections/tech/DailyNews/dotus980807.html; see also Suzanne Choney, \textit{Once Status Symbol, E-mail Now Staggering}, \textit{The San Diego Union-Tribune}, Oct. 3, 2000, at 2 (reporting a recent Pew Internet and American Life Project study finding that more than fifty percent of American adults do not use the Internet). \end{itemize}
C. Arguments For Non-Government Regulation

There have been indications that although consumers want privacy protections they feel that the industry, not the government, should be in control. In fact, the Clinton Administration actively endorsed self-regulation of privacy on the Internet:

\[\text{[G]overnments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them. Where government action or intergovernmental agreements are necessary . . . private sector participation should be a formal part of the policy making process.}\]

Ultimately, though, it is the responsibility of parents to comply with the industry regulations. This is certainly feasible, as there are numerous websites that will help a parent in this endeavor. Additionally, there is filtering software that can be used to prevent children from stumbling onto unwanted websites. Ultimately, by following a self-regulation scheme, the "individual freedom, re-

---

217. The @plan Internet Poll, administered to a random sample of 1000 adults, found that although privacy issues are of great concern, it is the industry that caused the mess and therefore the industry that must clean it up. Internet Poll Reveals Privacy as Most Important Internet Issue Among Online Users, @PLAN, INC., (Mar. 9, 2000), at http://www.e-commercealert.com/article37.html.

218. THE WHITE HOUSE, THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, PRINCIPLES § 1 (1997) (statement from the White House about self-regulation of Internet privacy) available at http://www.ecommerce.gov/framework.htm. In this statement it is argued that the private sector should take the lead in protecting privacy on the Internet through self-regulatory regimes. Id.

219. Id.

220. Fahey, supra note 1, at E1.

221. Cyberangels (http://www.cyberangels.org), for example, is one of these websites. This website is working to educate parents and children about safety on the Internet, and to provide technology to help parents in this endeavor.

222. Major examples of filtering devices on the market presently are Surfwatch, CYBERsitter, Cyber Patrol, and Net Nanny. ACLU v. Reno, 929 F. Supp. 824, 839 (E.D. Pa. 1996). Cyber Patrol, for one, allows parents to selectively block categories they deem inappropriate. Id. at 840. Parents may choose from twelve categories: Violence/Profanity, Partial Nudity, Nudity, Sexual Acts (graphic or text), Gross Depictions (graphic or text), Racism/Ethnic Impropriety, Satanic/Cult, Drugs/Drug Culture, Militant/Extremist, Gambling, Questionable/Illegal, and Alcohol, Beer & Wine. Id. To keep up with changing websites, the program can be updated every week over the Internet. Id. at 840-41.
sponsibility, and accountability” that make up the Internet culture will be fostered.\textsuperscript{223}

Web providers have the power to delete materials from their websites they deem offensive.\textsuperscript{224} The same is true of chat rooms, which Web providers can police to ensure that conversations that ensue are not offensive to other members by allowing members to become “SYSOPS” (system operators) as monitors.\textsuperscript{225} These chosen members are given the authority to take away postings or abolish users from chat or bulletin board areas.\textsuperscript{226} This kind of practice allows the Internet community to determine for itself what is offensive and to respond in the most flexible, least restrictive way.

Self-regulation also has the advantage of allowing government and industry groups to set industry behavioral norms together.\textsuperscript{227} An absence of regulation will inevitably cause some chaos, but even the government admits that “[t]he strength of the Internet is that chaos.”\textsuperscript{228} Although self-regulation is not perfect, and will not deter all crime or prevent all harm, “[c]ertain types of crimes . . . simply cannot be entirely prevented, short of adoption of repressive forms of order that would constitute a cure worse than the disease.”\textsuperscript{229}

\textbf{D. Arguments Against Non-Government Regulation}

Self-regulation, though, clearly has its drawbacks. Self-regulation deals with problems retroactively—only after they are perceived as problems.\textsuperscript{230} Moreover, because the Internet is made up of many different communities of people, it is difficult to self-regu-


\textsuperscript{224} For a discussion of how far an on-line provider can go when regulating a bulletin board before courts will consider the provider the author and responsible party, see Symposium, \textit{Regulating the Internet: Should Pornography Get A Free Ride on the Information Superhighway}, 14 \textit{Cardozo Arts \& Ent L.J.} 343, 353-56 (1996) (statement of Richard A. Kurnit).

\textsuperscript{225} Jamtgaard, \textit{supra} note 182, at 395.

\textsuperscript{226} \textit{Id}.


\textsuperscript{229} Johnson, \textit{supra} note 202.

\textsuperscript{230} See \textit{Privacy in Cyberspace: Hearing on Privacy in Cyberspace Before the Subcomm. on Telecomm., Trade, and Consumer Protection of the House Comm. on Commerce}, 105th Cong. (1998) (testimony of Katherine Montgomery, Ph.D., President of Center for Media Education) [hereinafter \textit{Montgomery Testimony}].
late because people place differing levels of importance on regulating different kinds of content. 231

It is also difficult to ensure that self-regulatory schemes premised on voluntary compliance are followed and enforced. 232 There is no proper monitoring system on the Internet, similar to the one used by the government, to ensure that people conform to regulations. 233 Moreover, there is no source of redress if someone violates a regulation. 234

Perhaps most importantly, industry designed regulatory schemes generally are backed by inadequate resources to fund compliance monitoring, seldom approaching the level of funding used by government to enforce similar schemes. Therefore, the consequences of not following a self-regulatory scheme might sometimes be cheaper than actually complying. 235 Although self-regulation can be successful, it is arguably more effective when used as a supplement to government enforced laws. 236

When regulation is left to the industry, there is no way of ensuring that contradictory rules will not develop. 237 These conflicting rules would leave people confused as to appropriate standards of conduct, and whether they are breaking them or not. In addition, while self-regulations are appropriate for dealing with behavioral standards, they “will not suffice to determine legal issues as complex as copyrights, free speech, obscenity, or fraud.” 238

231. Gibbons, supra note 203, at 496.
238. Id. (citing Zakalik, International Jurisdiction and Conflict of Laws in Cyberspace at http://www.libaries.wayne.edu/~jlitman/pzakalik.html (Expired Link)).
III. COPPA AS PROOF THAT PARENTS SHOULD REGULATE CHILDREN'S PRIVACY ON THE INTERNET

As with most new legislation, there is praise for what COPPA has done well and criticism for its shortcomings. As was the case when its predecessor laws were enacted, the debate is between those who believe that regulation of the Internet to protect children should come from the government and those who believe the industry should regulate itself in a way that allows families to make individualized choices. COPPA presents this regulation conflict in a new context—privacy. An analysis of the Act and what consequences have arisen since its enactment in April 2000, makes clear that in this new realm of cyberspace, the regulating power has not been placed in the right hands. COPPA’s shortcomings demonstrate, once again, that the government should not be regulating the Internet. Instead, this power should be left primarily with parents, with help from the industry.

A. Early Praise for COPPA

When COPPA was passed, privacy advocates praised the FTC for resisting pressure from companies to keep the regulations from being too strict. Many of these watchdog organizations have always been critical of self-regulation and have consistently disagreed with the government’s laissez-faire attitude toward regulation. Mark Rotenberg, the director of the Electric Privacy Information Center, admits that issues such as privacy need “government action.” Jason Catlett, the president of JunkBusters Corporation, thought that COPPA “look[ed] remarkably good,” and a member of the Center for Media Education thought the FTC had done a “conscientious job of developing rules that will be both flexible and effective.” Catlett actually went so far as to say that “self-regulation was flawed in concept as well as being an utter fail-

240. Pippin, supra note 239, at 137.
241. See MATLICK, supra note 3.
242. Junkbusters.com, who calls itself the “Master Self Defense Against Privacy Invading Marketing” is a website concerned with alerting Web users to threats to their privacy from direct marketers. For more information about Junkbusters see their website at http://www.junkbusters.com.
243. Clausing, supra note 239, at G11.
ure in practice." Proponents of the Act believe that because problems have not been remedied properly in the past, the way to correct this is to "provide the FTC with more discretion, rather than less" because "solutions need to come from Congress, the FTC and the industry itself." 

Many COPPA supporters feel that although members of the Internet value the privacy protection, their interest in keeping afloat financially will trump their concern for privacy rights. It is conceivable that a website operator might sacrifice children's privacy if the choice were between disclosure of information or having to shut down the site completely. Because such a large share of the money made on the Internet is through selling personal information, this conclusion is not unreasonable. Many COPPA supporters believe the FTC would be a better regulator of the Internet than industry for one reason: the FTC is not driven by financial incentives.

The part of COPPA designed with the most foresight is the "safe harbor resolution." In general, safe harbor regulations are considered "initiatives that, if adhered to, are considered in compliance with the U.S. privacy regulations." In this way, the government allows the industry to set its own standard upholding existing law. One member of the FTC recognized the safe harbor program as significant because it "recognizes the important role the industry can play as a partner with government to protect children's privacy on the Internet." The industry, by giving an Internet site its veritable seal of approval, can give the site assurance it will be in compliance with the law. Once the FTC approves a certain privacy program, the operator itself works the program's guidelines into its business models, thereby assuring the website is

---


245. Privacy Protections, supra note 9.

246. Id. (recalling a situation in which a representative of a children's website admitted to being "obsessed with the bottom line" rather than being focused on privacy concerns).

247. For a description of the safe harbor provision provided in COPPA, see supra notes 191-95 and accompanying text.


249. Id. at para. 4 (quoting Jodie Bernstein, director of the FTC's Bureau of Consumer Protection).
in compliance with the rule. A noncompliant website first would answer to the directors of the safe harbor program, and would only as a last resort be subject to sanctions by the FTC. The system allows the industry to become the middleman and take some control out of the hands of the government, while still making sure websites are keeping in compliance with the law.

B. Arguments Against COPPA

Despite the fact that government regulations had the potential to be successful and that COPPA addresses the specific problems of prior regulations, COPPA has nonetheless encountered many difficulties. As the most recent example of a government attempt to protect children on the Internet, COPPA’s failure to accomplish its own goals makes clear that parents, not the government or the industry, should regulate children’s privacy in this medium. Ironically, even though COPPA followed Supreme Court proscriptions and put much more of the onus on web providers, websites, and the industry itself, it created new problems. A policy of regulating many broadcast media by screening out one part of an audience will automatically encounter resistance.

COPPA has proved itself difficult to administer, has forced many websites to close down, and has not deterred children from accessing the kind of material they wish to see. It represents a failure of law, and demonstrates why parental intervention will be much more useful than any other previously attempted regulatory approach, even government-mandated parental intervention.

1. Children-Focused Sites Shutting Down

One fundamental problem with government-imposed Internet regulations is that they ignore the problem of website funding. Websites have been forced to spend inordinate amounts of money to comply with COPPA regulations, and many start-up websites simply do not have these funds. Other established websites for

---

253. Rocketcash.com spent about $100,000 on legal fees and technologies. Robin Raskin, COPPA: As Our Kids Go, So Goes the Nation, FamilyPC, Nov. 21, 2000 para. 3, at http://www.zdnet.com/zdnn/stories/news/0,4586,2656333,00.html The children’s website Zeeks.com was forced to remove e-mail and chat rooms from its website after realizing it would cost $200,000 to employ chat-room supervisors and
children, such as eCRUSH.com, decided it was simply easier to disallow children who were under thirteen to access their site altogether.

The latest, and possibly most shocking, addition to this group has been Walt Disney Co. ("Disney"), which will no longer allow children under twelve years old into its chat rooms. Disney explained that, "[r]egrettably, the overbearing scrutiny and disparity of interpretation of law and guidelines by federal regulators and advocacy groups may ultimately result in fewer and fewer options for kids to interact on the Web." Disney's reaction is just one of the many unintended effects of government attempts to regulate privacy.

The cost of compliance is simply too high. When it is cheaper and easier for companies simply not to run children-focused web-monitor phone lines to answer COPPA questions and process permission forms. Thom Weidlich, *Coping With COPPA*, DIRECT, Nov. 30, 2000, at 1; May Wong, *Sites For Kids Say New Law Hurting Business*, THE COLUMBIAN, Sep. 15, 2000, at E3. Surfmonkey.com, Inc. has reportedly spent between $50,000 and $100,000 thus far in attempting to comply with COPPA. Doug Isenberg, *Childproofing The Net*, INTERNET WORLD, July 15, 2000, at 61.

---

254. See generally www.eCRUSH.com, at http://www.ecrush.com/aboutus.phtml. eCRUSH.com is a website on which teenagers can meet up with their "crush" online. Only people who already know one another can interact, because in order to participate you must know the person's e-mail address. Participants type in the names and e-mail addresses of the people they have love interests in, and the website informs those people by anonymous e-mail that someone has an "eCRUSH" on them. They are encouraged to join the website and enter their own eCRUSHes to see if there is a love match. If so, the website facilitates a meeting between the two. Id.

255. eCRUSH.com felt that it did not have the means to verify parental consents. DeWayne Lehman, *Children's Privacy Law to Take Effect Tomorrow* para. 10 at http://www.making-a-difference.org/CRIER-2.htm (Apr. 20, 2000). Getting rid of all children under thirteen cut eCrush's audience by 5%, but the additional staffing would have cost the site an extra $50,000. Id. at ¶ 11. This is particularly sad because children thirteen years old and younger made up much of the population of users of many sites. Ben Charny, *The Cost of COPPA: Kids' Site Stops Talking*, ZDNET NEWS, at http://www.zdnet.com/zdnn/stories/news/0,4586,2627742,00.html (Sept. 13, 2000). Other websites who have followed suit are NBCi (http://www.nbcii.com), and the Thomas the Tank Engine website (http://www.thomasthetankengine.com/home/homepage.html). Strohmeyer, supra note 170.


257. Id.

ultimately, there will be fewer choices for child appropriate Internet content websites, but perhaps no greater security for children. In other industries, companies can pass along to their customers the costs of regulatory compliance, but because most websites do not charge customers for the use of their services, this funding mechanism is not available. The irony, of course, is that children will likely end up looking at the sites the law was originally trying to protect them from because there will be no sites left specifically for them. If parents were monitoring their children, however, as opposed to putting the onus on the industry alone, these types of costs, if not all costs, would be almost eliminated. Furthermore, if members of the industry were making the laws, they would purposely make compliance cheaper in order to keep more websites financially afloat.

2. Industry Noncompliance

Another problem with government regulations, as demonstrated by COPPA, is the lack of industry compliance with rules that members themselves did not create. The FTC recently announced that a sweep of children-focused websites revealed that half of the sites have “substantial compliance problems” with COPPA. The newest group of noncomplying websites consists of websites founded and run by teens themselves. Because the FTC’s enforcement is

259. Firms May Need to Examine Kid Oriented Privacy, FINANCIAL NET NEWS, July 31, 2000, at 7. The Liberty Financial website decided not to endure the cost of COPPA compliance, and stopped plans to make a website aimed at children. Id.

260. Net Privacy Law Costs Children’s Sites, USA TODAY TECH REPORT (explaining that the interactive nature of the Internet means that children will just gravitate to the sites that allow them access) available at www.usatoday.com/life/cyber/tech/cti526.htm (Sept. 14, 2000). COPPA does not apply unless a site has a section intended for children; it is therefore conceivable that children will at some point find it easier to access adult sites than children’s sites. Aidman, supra note 23.

261. Steven Bryan, the CEO of Zeeks.com, said, “Without question, that is where the kids will go to find these activities. We’ve closed the playgrounds and sent the kids to play in the street.” Federal Sites Breaching Children’s Privacy Law, DALLAS MORNING NEWS, Oct. 7, 2000, at 3F. Before COPPA, Zeeks.com had 1000 kids signing up daily for chat room and e-mail usage, but since COPPA’s enactment that number has dropped to 100. Weidlich, supra note 253.

262. FTC Warns Web Sites: Play Fair With Kids, SALT LAKE TRIB., July 20, 2000, at C5. According to Joseph Turow, a professor at the University of Pennsylvania’s Annenberg Public Policy Center, and the author of a recent study that checked websites for privacy compliance, “In some cases the letter of the rules is not being followed, but in many more cases the spirit of the rules is not being followed.” Schwartz, supra note 178.

lax, it is not surprising many websites do not abide by COPPA’s requirements. Website providers know that the government cannot possibly police the whole Internet, the chances they will get caught are slim. Additionally, in many cases, the price of non-compliance is not high enough, and websites are simply risking getting caught for not abiding by the rules.

Amazingly, even the U.S. government’s website is not in compliance. The “White House for Kids” site hosted at www.whitehouse.gov collects personally identifiable information about children without getting demonstrable parental permission, and does not offer parents the opportunity to control the information collected. Although COPPA does not directly apply to government sites, the administration’s Office of Management and Budget issued a directive in June that specifically required federal sites to abide by the same standard. Because the government made it a point to force COPPA-compliance upon itself, it is surprising it ultimately has failed to follow its own rule.

The White House website encourages children to submit personal information when they write e-mails. The government admits its failure to comply, but it argues that the site is also subject to the Presidential Records Act that requires that all e-mails sent to the president and his family be saved. The Environmental Protection Agency website and the National Aeronautics and Space Administration violated the same COPPA requirements. The White House for Kids failed to control the use of personally identifiable information. The White House for Kids site hosted at www.whitehouse.gov collects personally identifiable information about children without getting demonstrable parental permission, and does not offer parents the opportunity to control the information collected.

264. When the FTC found sites in noncompliance they simply sent warning e-mails. Toysmart.com First Company Charged With Violating Children's Privacy Law, EDUC. TECH. NEWS, Aug. 16, 2000 [hereinafter Toysmart].

265. Recall, the fines are only $10,000 for each violation. Supra note 198 and accompanying text.


268. PRIVACILLA, supra note 267.

269. Id.


271. 44 U.S.C. §§ 2201-2207 (1991) (governing all official records of Presidents and Vice Presidents created or received after January 20, 1981, including paper, audiovisual, and electronic media).

Space Administration website, two other government sites, also collect personal information from children who submit artwork to be posted on the site.\textsuperscript{273} The government itself is demonstrating to the Internet community how difficult it is to comply with COPPA. People, however, look to the government to set an example and expect it to follow its own laws. When the government itself flaunts its disregard for the rules, Web providers will not likely find it necessary to comply with COPPA either.

With so many websites in noncompliance, including a website that promised to comply even though it had no need to do so, it seems that COPPA’s rules are not as easy to follow as the FTC believes. Not only has the FTC expressed the ease with which a website may comply with its rules, but it has also been attempting to help with compliance.\textsuperscript{274} Looking at the recent levels of noncompliance, thought, these attempts by the FTC appear unsuccessful. As Robert Levitan of Flooz.com\textsuperscript{275} said, “We need a uniform code across the country. We need a standard law on privacy and taxation. But let’s do it wisely and make it easy for Internet companies to comply.”\textsuperscript{276}

3. General Noncompliance

It is not only the industry itself that is in noncompliance. Many children find it easy to circumvent the law, primarily because of their parents’ lack of knowledge about computers\textsuperscript{277} and the relating privacy policies.\textsuperscript{278} To verify age, many websites merely ask a user to check a box indicating whether he or she is over the age of thirteen.\textsuperscript{279} This barrier will not stop astute children from accessing a Web page, for they will check the box that allows them access and

\textsuperscript{273} Hopper, \textit{supra} note 270, at A4.
\textsuperscript{274} Press Release, Fed. Trade Comm’n, Web Sites Warned to Comply With Children’s Online Privacy Law (July 17, 2000), \textit{available at} http://www.ftc.gov/opa/2000/07/coppacompli.htm. The FTC has created a special website, http://www.ftc.gov/kidzprivacy, to help parents and children understand COPPA. \textit{Id.} They also conducted a public training program to help web providers with COPPA compliance. \textit{Id.}
\textsuperscript{275} Flooz.com (http://www.flooz.com) is a website that deals in online gift certificates.
\textsuperscript{276} Jeri Clausing, \textit{Fate Unclear for F.T.C.’s Privacy Push}, N.Y. TIMES, May 22, 2000, at 1C.
\textsuperscript{277} Raskin, \textit{supra} note 253; Isenberg, \textit{supra} note 253 (speculating that COPPA’s rules are easy to circumvent through forgery of parental consent).
\textsuperscript{278} D. Ian Hopper, \textit{Web Sites For Kids Skirt Law on Privacy}, COLUMBIAN, Apr. 5, 2001, at D1 (presenting an Annenberg Public Policy Center study that found that “privacy policies were difficult to find, read, and understand”).
\textsuperscript{279} See http://www.altavista.com for an example of this type of age verification.
move onward. As Jennifer Widstrom, the Director of EmailAbuse.org, predicted, "Many children are going to magically have their thirteenth birthdays today." In fact, some parents would prefer to have their children lie about their ages than to give out their credit card numbers to verify their permission, as required by COPPA. Many children have realized that all they need to do is open an e-mail account under a parent's name, and give permission to themselves.

It is turning out to be even more dangerous to have COPPA than to have no regulation at all, because under COPPA, despite appearances, no one is really in control. Ironically, COPPA gives parents the false impression their role in protecting their children from the Internet is no longer needed. When Bonus.com, a game website for children, asked for parental consent from its members, only forty-nine percent of parents even responded (five percent declined). This website is losing more than half of the children who are interested in participating, and it doesn't even have chat, e-mail, e-commerce, or instant messaging—the potentially dangerous activities against which the law was intended to protect. Even so, parents are likely not doing their part because they feel someone else has already taken on that responsibility.

Supporters of COPPA maintain that the problem is not the law itself, but rather the parental enforcement of the law. "[T]he children's online laws depend on obtaining parental consent, and if parents aren't bothering to provide consent, sites are running into problems." Many websites are shutting down, not because they cannot afford compliance with COPPA, but rather, because parents simply are not supplying consent. Attempts at implementing subscription-based models have also failed because parents

---

280. The FTC is clearly working under the assumption that children over the age of thirteen lie more than children younger than thirteen. Sonia Arrison, Cybersitters Report For Assigned Duties, Washington Times, May 6, 2000, at A10.


283. Raskin, supra note 253.


285. Id.

286. Id.

287. Id.

288. See Privacy Protection, supra note 9.

289. Subscription-based models are based on requiring parents to pay for access to certain websites in order for their children to utilize their services. Id.
IS COPPA A COP OUT?

are generally unwilling to pay. Clearly the government should have realized by now that regulations requiring parents to pay extra money are less likely to be followed. The industry and the FTC claim to have educated parents about COPPA compliance though seminars and educational meetings across the country, informing parents not only about the dangers of noncompliance, but also how to go about complying. In reality, though, most of the means of finding out how to comply with COPPA are found on the Internet, thereby reaching only the people who are already most likely to understand the law. The government has targeted these sessions toward parents who are already Internet savvy rather than those who know little about computers.

4. Verification Complications

The parental verification requirements demanded by COPPA are unsuccessful because they do not take into account that many parents and websites find it difficult to comply. COPPA's measures are complicated to implement and costly to execute. Although new technologies are being developed, currently existing measures are too slow to be effective; even if verification is being performed through faxing in a credit card number, the process can take over a day. Understandably, parents are not happy supplying their credit card numbers in order to verify their adult status. This exposes them to the same privacy risks as the ones from which they are trying to protect their children. Consequently, parents will likely use slower methods such as the U.S. Postal Service or fax verification, thereby foregoing the advantage of Internet speed.

290. Id. It is ironic that in order to protect children's private information, the law is asking parents to divulge their own personal information. Arrison, supra note 280.

291. This also raises the issue of economic discrimination. If a family can afford parental verification of websites, their children could have access to more websites. This gives a distinct advantage to children from wealthier families, as opposed to children whose parents cannot afford to keep paying for extra services.

292. Supra notes 176 and 179, and accompanying text.


294. Evidently seventy-three percent of Internet users are uncomfortable providing either credit card or financial information to online businesses. Pippin, supra note 239, at 140 (citing Center for Democracy and Technology, Behind the Numbers: Privacy Practices on the Web (July 28, 1999) at http://www.privacyexchange.org).
Additionally, requiring parents to pay money for this service will further widen the rich/poor divide.\textsuperscript{295} It is important that, as technology advances, poorer families do not become isolated from it. Currently, thirty percent of poor families with young children do not have telephones,\textsuperscript{296} therefore it is unlikely that these families will be able to keep up with the growing expenses of maintaining Internet service, especially if required to pay extra money to protect their children from possible harm.

5. Lack of Government Enforcement

Another problem highlighted by COPPA is that the FTC does not strongly enforce the regulations it supports.\textsuperscript{297} In fact, the FTC seems to be under the assumption that simply by policing the Internet they will be able to catch offenders.\textsuperscript{298} Jason Catlett, president of Junkbusters.com, is dubious that the FTC will, in fact, enforce COPPA: “If you look at the history of the FTC’s enforcement actions, they have been few in number and gentle in force. I would be astonished if the FTC would ring the cash register for significant sums.”\textsuperscript{299}

The only lawsuits to enforce COPPA brought to date have settled.\textsuperscript{300} The first attack by the FTC on an alleged violation by a website was filed only after the website already ceased to exist.\textsuperscript{301} The case charged that the website Toysmart.com was selling the personal information of many children.\textsuperscript{302} Although this lawsuit was intended to send a message that the FTC was serious about

\textsuperscript{295} Kathleen Haney, \textit{Rich, Poor Divide Behind Internet Gap}, DIGITRENDS.NET, eBiz, at http://www.digitrends.net/ebna/index_2611.html (June 16, 2000). A Jupiter Communications study reveals that although a digital divide exists between ethnic and age groups, that largest gap is between high and low income households. \textit{Id.} While households with incomes over $75,000 make up the largest population online, with 15 million households surfing the Web, less than half of U.S. households with incomes under $15,000 (which is true for nineteen percent of the total U.S. population) will have Internet access by 2005. \textit{Id.}
\textsuperscript{296} FRIEDMAN, supra note 14, at 83.
\textsuperscript{297} Doug Isenberg, \textit{The Year in Net Law}, INTERNET WORLD, Dec. 15, 2000, at 32.
\textsuperscript{298} The FTC admitted that it could not enforce the law as it had wished because of widespread confusion about compliance. \textit{Id.}
\textsuperscript{299} Arrison, supra note 280.
\textsuperscript{300} Burke, supra note 282.
\textsuperscript{300} In re Toysmart, No. 00-11341-RGS (D. Mass. July 10, 2000); In re Toysmart, No. 00-13995-CJK (Bkty. Ct. July 21, 2000). See Associated Press, \textit{Technology Brief-
enforcement, settling it only made the agency look less serious because the violator essentially got a slap on the wrist.

Additionally, the lawsuit only dealt with one half of what COPPA was intended to prevent—in this case, the dissemination of privacy information. In this regard, Toysmart.com is not the only offender. After a recent check of Internet sites, the FTC dealt with websites that had "substantial compliance problems" by sending warning e-mails. The problem is not only with the law itself, but also with its poor enforcement. Quite simply, websites are not deterred by the potential consequences of their noncompliance with the law.

6. Possible Constitutional Issues

COPPA has not yet been challenged constitutionally, probably because many believe the economic burden on Internet providers is easily outweighed by the government’s compelling interest in the protection of children. However, COPPA may be unconstitutional for the same reasons as COPA. The Federal District Court for the Eastern District of Pennsylvania found that COPA was overbroad and burdened more people than intended. Although COPPA has a narrower focus, targeting children only, it actually affects the Internet at large, as forcing websites to close undoubtedly affects the entire Internet community. Additionally, the court that found COPA unconstitutional noted that the proof of age requirement puts an undue economic burden on the industry. Similar reasoning may apply to COPPA. The court, when...
looking at COPA, concluded there were less restrictive means that would accomplish this task.\textsuperscript{310} Similarly, there are alternative ways to accomplish the goals of COPPA, such as filtering devices and using "parental controls" on ISPs, that are less restrictive than government intervention. Finally, there is no substantial proof that children actually are harmed when their personal information is disseminated,\textsuperscript{311} extinguishing the "compelling interest" argument.

IV. Solution for the Future

If COPPA's failings have shown anything, it is that regulation of the Internet is more difficult than was originally imagined, and unlike the regulation of encountered previously media. The government's attempts to regulate were widely found unconstitutional, and the government's delegation of responsibility to the industry, through self-regulation was found ineffective. The answer is, therefore, to cease formal regulations, and to focus more on educating parents, mentors, and teachers. These people will have the most influence over children, because they have the most at stake—the safety and happiness of their own children. They are the people who will best ensure that children use the Internet safely.

The industry and the government have their own agendas when regulating the Internet.\textsuperscript{312} Although the government desires to protect children, it often errs, as does COPPA, on the side of passing sweeping regulations that take away too many rights of In-
The industry, on the other hand, tends to do what is best for itself, because as much as it may be interested in providing a safe product to children, it is still primarily driven by economics. This means, of course, that if it does not make financial sense for a commercial website to exist, the site will simply close down, or, if the economic consequences of not following a regulation are cheap enough, it will not follow the regulation at all. Websites operators are less concerned with the ability of children to have free access to the site than they are with their own ability to make money.

It is, then, ultimately up to parents—the people most invested in protecting children—to regulate the information their children have access to on the Internet. The government and the industry should certainly help, though, by providing parents with the tools and resources for protection of children. One possibility is that the government could subsidize filtering programs that disallow children from offensive websites and chat rooms in which inappropriate conversations go on. Some of this technology already exists, and more is in development, but the cost of the technology and the updates inhibits its widespread use. Hence, while the government should in no way take over regulation, the industry should not single-handedly have the onus of protection. When responsibilities are delegated this way, regulations lay stagnant, to everyone's disadvantage.

If parents are to play a meaningful role in children's protection they need the strong support of both the government and the industry. Congress could help by allocating more money to enforcement of COPPA issues. Government officials also need to be better educated about concerns being addressed by the regulation. The FTC, which is charged with implementing COPPA, must be more diligent about its enforcement, and needs to interact more with the industry by communicating its concerns. Once the FTC finds noncompliant websites it should do more than send a warning e-mail. There need to be more serious consequences for violators.

The Internet industry is where the most important developments must take place. Industry leaders must create a centralized organization, effectively dealing with complaints from users. The industry itself must also continue cultivating new educational techniques and supporting the development of technology such as filtering devices and parental verification devices. Because the industry is in the best position to understand the problems of the Internet, it is also in the best position to help fix those problems.
It is important that the goals of protecting children do not come at the expense of the content of the Internet. In other words, regulation of the Internet should not interfere with First Amendment rights. Compromising the content of the Internet to make it child-friendly, however, is surely not the answer. The price to be paid by strictly implementing acts such as COPPA outweighs the possible benefits of protecting our children.

It is important that parents become proactive. There are many options for parents in the scheme of self-regulation of privacy, the most important one being education. Parents must educate themselves about the benefits of and problems with the Internet to understand what threatens their children. They must next educate their children on how to interact with this form of media. In addition, libraries and schools with Internet access should educate Internet users, perhaps in the form of a tutorial, before Internet use is allowed. Understanding the risks and dangers of the Internet will help children avoid dangerous situations.

It is also prudent for parents to place their computers in open spaces, where they can monitor their children’s Internet use firsthand. Once they are comfortable with the way their children use the Internet, they can then lessen the monitoring. Although filtering devices may not be the perfect solution, they are certainly a step in the right direction.

313. This fact has been well established by the Supreme Court. See, e.g., Sable Communications v. FCC, 492 U.S. 115, 126 (1989); Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 79-80 (1983); Butler v. Michigan, 352 U.S. 380, 383-84(1957).

314. Justice Scalia commented on the difficulty of monitoring children’s Internet usage during oral arguments in Reno v. ACLU: “If I had to be present whenever my 16-year-old is on the Internet, I would know less about this case ...” Joshua Quittner, The Supreme Court: Some Surprisingly Wired Justices Hear an Antiporn Case That Would Restrict Free Speech in Cyberspace, TIME, Mar. 31, 1997, at 74.

315. Recall, filtering devices are not perfect—they do not block everything and they tend to block Internet sites that are not considered offensive. Digital Chaperones For Kids, CONSUMER REPORTS, Mar. 2001, at 20 (showing that because of the arbitrary value judgment that goes into developing filtering devices, each device will filter different websites). In fact, a recent study discovered that about eighty percent of sites blocked by both Cyber Patrol and SurfWatch, two of the most popular filtering products, contained no objectionable material. Robert H. Brink & Elaine Furlow, Butt Out, Big Brother, WASH. POST, Jan. 14, 2001, at B8. Plus, filtering devices must be updated regularly to account for new websites, leading to extra expenses. See Digital Chaperones For Kids, at 20. An additional problem is that filtering devices place the responsibility in the hands of uninterested companies, rather than leaving it up to the concerned parties. Schwartz, supra note 100, at A15. Finally, some filtering software companies have discovered they can make a good deal of money by selling students’ Web “surfing” trends to private companies. Michelle Lewis, Surprise! Children’s Web Info For Sale, NEWSFACTOR.COM, available at http://www.newsfactor.com/
CONCLUSION

"[T]he Internet doesn’t create any problems, it just presents them in a new venue."316 Just as we have no control over what our children do when they are not in sight, we do not have the power to control what they do on the Web outside of parental supervision. The best-case scenario, of course, is having a parent monitor all Internet use by a child; this is, however, rarely possible. Reality dictates that education of children and advancement of technology are the next best solutions.

Parents can protect their children only to a certain extent,317 but they are certainly more successful in that endeavor than the government working alone.318 We need to accept that the Internet is more like the real world than any another media, and deal with it accordingly. We can protect children by letting parents run their own households and take care of their own children through education and love, and by facilitating parents in these tasks. This is the only way that children will be protected at all, because it is really parents who have the power to implement filtering devices, utilize rating devices, or follow industry initiatives.319 As President Clinton sensibly stated:

[W]e must realize that in the end, the responsibility for our children’s safety will rest largely with their parents. Cutting-edge technology and criminal prosecutions cannot substitute for responsible mothers and fathers. Parents must make the commitment to sit down with their children and learn together about the benefits and challenges of the Internet. And parents, now that the tools are available, will have to take upon themselves the responsibility of figuring out how to use them.320

316. Symposium, Should Cyberspace be a Free Speech Zone?: Filters, “Family Friendliness,” and the First Amendment, 15 N.Y.L. SCH. J. HUM. RTS. 1, 102 (1998) (indicating that parents cannot protect their children from all the dangers in the world so they must instead focus on educating them).

317. Id. at 103. “Pedophiles can get access to kids in candy stores, in the mall, in chess clubs, in stamp clubs, et cetera. The number of confirmed cases where the Internet facilitated pedophilia is extraordinarily small, but has become the focal point for anxiety about this new medium, and where it may take us.” Id. at 103-04.


319. Werst, supra note 54, at 239-40.

Ultimately, it is the parents who control their children’s Internet use—how often, what time of day, and for what purposes.321 The government is too removed to have a substantial influence on children’s Internet usage.

We, as a nation, value freedom of speech above many of the potential dangers that free speech may cause.322 “The potential and fear of misuse of the Internet, cannot justify over-reaching regulations encroaching on basic civil liberties.”323 Stifling not only the content but also the form of the Internet would be detrimental both to adults and children.324 Although some form of regulation is arguably necessary, the government has not effectively implemented it. Additionally, the government has shown that it, alone, is not the appropriate regulating body in this matter. As the Supreme Court itself admitted: “The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.”325

321. Matlick, supra note 3.
324. With all Internet participants fearful of criminal prosecution if certain terminology is utilized, the discussions would be stifled to the point that a teenager seeking answers to curious questions concerning a subject foremost on their mind, could not find answers via this medium. Without open discussion of how to prevent being raped or birth control or abstention, there would quite possibly be greater number of teenage pregnancy or sexually transmitted diseases. This would be contrary to the interests of the State.