Journal of Law and Policy

Volume 10 | Issue 1 Article 4

2002

COPPA: Protecting Children's Personal Information on the Internet

Danielle J. Garber

COPPA:* PROTECTING CHILDREN'S PERSONAL INFORMATION ON THE INTERNET

*Danielle J. Garber***

INTRODUCTION

Privacy in the information age is increasingly being sacrificed as the collection of information explodes.[1] The Internet[2] can

---

* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505 (Supp. IV 1998). This Act was passed as part of Pub. L. No. 105-277 on October 21, 1998. The COPPA should not be confused with the Child Online Protection Act ("COPA"), which has consistently failed to pass constitutional muster. *See* ACLU v. Reno, 217 F.3d 162, 168-69 (3d Cir. 2000) (affirming a preliminary injunction based on the likelihood of finding the COPA unconstitutional because it places an "impermissible burden" on speech protected by the First Amendment), *cert. granted sub nom*. Ashcroft v. ACLU, 121 S. Ct. 1997 (2001). Essentially, the COPA was enacted to regulate the dissemination to minors of indecent material on the Internet. *See id*. The notion of indecency was determined by whether the material published on the Internet was "harmful to minors." *Id*. In order to identify material that is harmful to minors, the COPA relied on "contemporary community standards" in the context of the Internet. *Id*. The COPPA, on the other hand, applies only to the collection of children's personal information and does not limit access to inappropriate sites, such as pornography. *See* 15 U.S.C. § 6502.

** Brooklyn Law School, Class of 2002; B.S., Cornell University, 1999. The author would like to thank her family, Steve, Sandy, and Jacki Garber, and her friends, for their unconditional love and support.

[1] *See infra* notes 34-41 and accompanying text (providing statistical information on information collection on the Internet).

[2] "The Internet is a decentralized, self-maintained networking system that links computers and computer networks around the world, and is capable of

instantaneously offer immeasurable amounts of information.[3] Once connected, the computer is transformed into an interactive world, enabling users to reap the benefits and enjoy the thrill of being online. Today, approximately seventeen million teenagers between the ages of twelve and seventeen use the Internet.[4]

---

quickly transmitting communications." ACLU v. Reno, 217 F.3d at 168 (providing a general overview of the Internet and the World Wide Web). It has further been described as "an international network of interconnected computers." Heather Miller, *Strike Two: An Analysis of the Child Online Protection Act's Constitutional Failures*, 52 FED. COMM. L.J. 155, 157 (1999). The World Wide Web is distinguished from the Internet in that it consists of millions of individual Web sites, all of which are part of the larger and more comprehensive Internet. *See* ACLU v. Reno, 217 F.3d at 168. Each distinct Web site is connected to the Internet through protocols that "permit 'the information to become part of a single body of knowledge accessible by all Web visitors.'" *Id*. at 169 (citing American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 166 (S.D.N.Y. 1997)). The World Wide Web is the most common way for computer users to access information on the Internet. *Id*. at 168.

[3] The Internet seems to have taken on the role that the encyclopedia once played in a child's life. For example, a child who needs information to write a school report on Thomas Jefferson can find a plethora of biographical and historical information on the Internet. *See, e.g.*, The Internet Public Library, Presidents of the United States ("POTUS"), *at* http://www.ipl.org/ref/POTUS/tjefferson.html (last visited Nov. 17, 2001). The Internet is also a valuable resource for information on wild animals. *See, e.g.*, Cheetah Conservation Fund, http://www.cheetah. org (last visited Nov. 17, 2001). Not only can a child obtain information on the cheetah at this Web site, but this site offers additional links to numerous other sites, such as Defenders of Wildlife and the African Wildlife and Conservation Resource. *Id*. Furthermore, the Internet allows children to participate in their studies on a new level. This is clear at the Cheetah Conservation Fund Web site, which offers children the opportunity to adopt a cheetah to further the organization's conservation efforts. Cheetah Conservation Fund, *at* http://www.cheetah.org/adopt.htm (last visited Nov. 17, 2001).

[4] Amanda Lenhart & Lee Rainie, Pew Internet & American Life Project, *Teenage Life Online*, *at* http://www.pewinternet.org/reports/pdfs/PIP_Teens_Report.pdf (June 20, 2001) [hereinafter *Teenage Life Online*] (reporting on the widespread use of the Internet by teenagers and their parents' responses). Research completed in December 2000 found that 45% of all American children under the age of eighteen use the Internet. *Id*. at 12. The survey showed that the average age that these children began using the Internet was

Twenty-nine percent of children eleven years old or younger go online.[5] This widespread use is easily explained by the extensive opportunities the Internet offers for learning, entertainment, creativity, and communication with others. Children use the Internet to get help with their homework, browse various Web sites, and play and download games.[6] The most exciting activity for children is communicating with their friends through chat rooms, bulletin boards, e-mail and instant messaging.[7] Despite

---

thirteen. *Id*.

[5] *See id*. Teenagers go online from a variety of locations, and most go online from home. *Id*. (reporting that 83% of the 754 teenagers surveyed access the Internet from home). Other common locations include school, a friend's house, and the library. *Id*. In 1999, 11.4 million children, twelve years old and under, used the Internet. Lyne Burke, *Kids' Privacy an Act, or Action?*, WIRED NEWS (Apr. 20, 2000), *at* http://wired.com/news/politics/0,1-283,35712,00.html (discussing the potential problems imposed by the COPPA). This figure is expected to escalate to 24.3 million by 2003. *Id*. Also, in 1999, it was estimated that 62% of children between the ages of eight and fifteen use the Web. Miller, *supra* note 2, at 159.

[6] *See* Federal Trade Commission ("FTC"), *Privacy Online: A Report to Congress*, *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (June 1998) [hereinafter June 1998 Report]; *see also Teenage Life Online*, *supra* note 4, at 41. Older children are involved in even more diverse activities online. These activities include obtaining news, researching an online purchase, downloading music, visiting team or club Web sites, and looking for diet, health, or fitness information. *Teenage Life Online*, *supra* note 4, at 41.

[7] *Teenage Life Online*, *supra* note 4, at 41. A chat room is where interactive online discussions take place that enable typed conversations to occur in real-time. *See, e.g.*, TechWeb.com, http://www.techweb.com/encyclopedia/defineterm?term=chat+room (last visited Aug. 27, 2001); Netdictionary.com, http://www.netdictionary.com/html/c.html (last visited Oct. 23, 2001). Bulletin Board Systems ("BBS") are dominantly used as a forum for a particular interest group where members can send e-mail, join discussion groups, and download files. *See, e.g.*, TechWeb.com, http://www.techweb.com/encyclopedia/defineterm.yb?term= BBS (last visited Oct. 23, 2001); Netdictionary.com, http://www.netdictionary.com/html/b.htm (last visited Oct. 23, 2001). Electronic mail ("e-mail") is the transmission of memos and messages over a network. *See, e.g.*, TechWeb.com, http://www.techweb.com/encyclopedia/defineterm.yb?term=e%2Dmail (last visited Oct. 23, 2001); Netdictionary.com, http://www.netdictionary.com/html/e.html (last visited Oct. 23, 2001). An even newer phenomenon is instant

such undeniable advantages, however, the Internet can pose a threat to children, exploit them, and compromise their privacy.[8]

Children's information is quite valuable.[9] It is a commodity that requires special protection because children do not have the maturity, knowledge, or experience to protect themselves. The Children's Online Privacy Protection Act ("COPPA") was adopted in 1998 to protect the personal information disclosed by children under the age of thirteen.[10] The Federal Trade Commission ("FTC") has the power to enforce the COPPA and has developed regulations to implement its requirements, which became effective on April 21, 2000.[11] While the COPPA faces

---

messaging, which is a computer conference over the Internet between two or more people. TechWeb.com, http://www.techweb. com/encyclopedia/define term.yb?term=INSTANT MESSAGING &exact=1 (last visited Oct. 23, 2001). When both parties are online at the same time, they can maintain a conversation with each other using the keyboard. Thus, instant messaging permits individuals to communicate with each other in real time. Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750, 22,753 (proposed Apr. 27, 1999) (codified at 16 C.F.R. § 312 (2001)). Today, 74% of American teenagers who access the Internet use instant messaging. Jeff Palfini, *Teenagers Do Their Talking Online*, PC WORLD.COM, *at* http://www.pcworld.com/news/article/0,aid,53444,00.asp (June 21, 2001). This means that almost thirteen million teenagers communicate using instant messaging. *Teenage Life Online*, *supra* note 4, at 3. Teenagers report that the Internet increases and broadens their network of friends. Jeff Palfini, *Teenagers Do Their Talking Online*, PC WORLD.COM, *at* http://www. pcworld.com/news/article/0,aid,53444,00.asp (June 21, 2001). Instant messaging is a casual and informal means to talk with others. *Id*.

[8] *See infra* Part I.C (discussing the threat to children and potential privacy invasions).

[9] Robert L. Hoegle & Christopher P. Boam, *Putting a Premium on Privacy Protection Policies*, NAT'L L.J., Aug. 21, 2000, at C8. "The key to success in the emerging electronic marketplace will be a company's ability to gather and use information from and about its customers quickly and efficiently." *Id*. *See also infra* Part I.B (discussing the value of personal information).

[10] *See* 15 U.S.C. § 6502.

[11] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)). The proposed rule can be found at 64 Fed. Reg. 22,750 (Apr. 27, 1999). "The proposed rule is designed to assist parents in controlling the flow of their children's personal

inevitable enforcement difficulties,[12] it is an essential legislative achievement that furthers the protection of children's privacy on the Internet. With the aid of future technological advances and useful tools to aid industry compliance, the effectiveness of the COPPA will be strengthened.

This note first discusses various methods of gathering personal information on the Internet. Second, it elaborates on the pressing concerns about online privacy and shows why children need special protection. By examining the COPPA and its implementation, this note explores whether the Act accomplishes its purported goals, namely, whether children's online privacy is adequately protected from unfair and deceptive acts with the enactment of the COPPA. Finally, this note concludes that although the COPPA presents some enforcement problems, such as the inability to detect whether children are truthfully disclosing their age, it will likely prove to be effective in making the Internet a more private and safe place for children.

I. INFORMATION GATHERING ON THE INTERNET

While gathering personal information is not a new phenomenon, the speed, accuracy, and efficiency that the Internet provides is quite innovative.[13] Personal information can be

---

information on the Internet." Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750, 22,751 (proposed Apr. 27, 1999) (codified at 16 C.F.R. § 312 (2001)).

[12] *See infra* Part III.D (discussing the nature of the industry and the characteristics of the Internet that raise compliance and enforcement difficulties).

[13] Due to higher connection speeds, new technology that provides a variety of access devices, and an extensive range of content, the Internet today is quite different from the Internet of five years ago. John B. Horrigan, Pew Internet & American Life Project, *New Internet Users: What They Do Online, What They Don't, and Implications for the Net's Future*, *at* http://www.pewinternet.org/reports/pdfs/New_User_Report.pdf (Sept. 25, 2000). Five years ago, only a small percentage of the population used the Internet. S. REP. NO. 106-404, at 170 (2000), *available at* 2000 WL 1279155. "Few new technologies have been adopted as quickly as using a personal computer to access the Internet, and its use is changing the way Americans live and work."

obtained from children both directly, with a child's consent, and indirectly, without a child ever knowing.[14] Understanding the methods used to gather information is helpful in identifying how a large spectrum of information is actually obtained, used, and valued in the online marketplace, and how it is then manipulated to take advantage of children.

A. The Methods of Collection

There are two primary methods of collecting personal information online. The first is the active method, in which a Web site provider directly asks the child to provide the requested information.[15] The second method is through passive data collection, whereby information is collected without the child's knowledge or voluntary consent.[16]

The active method of collecting personal information online requires an affirmative step by the child to deliberately provide

---

Id. For example, publishers in the print and broadcast media lack the ability to gather personally identifiable information without the actual consent or participation of their customers. *Information Privacy: Hearing Before the Senate Comm. on Commerce, Sci. and Transp*. (July 11, 2001), *available at* 2001 WL 771617 (testimony of Marc Rotenberg, Executive Dir., Electronic Privacy Information Center) [hereinafter Information Privacy Report]. This was true of the Internet up until recently. Today, advances in Web tracking technology enable Web site operators, such as online magazines and advertisers, to collect a wide assortment of information from individual users without their consent or even their knowledge. *Id*. *See also infra* notes 28-30 and accompanying text. Other Internet users also have access to this information. For example, users who register with a site to use instant messaging can search instant messaging directories, which provide access to information such as names, e-mail addresses, gender and age. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 22,753.

[14] Martha Landesberg & Laura Mazzarella, *Self-Regulation and Privacy Online: A Report to Congress (by the FTC, July 1, 1999)*, *available at FTC.GOV.*, 607 PLI/PAT 299, 308 (2000).

[15] *See* June 1998 Report, *supra* note 6, at 8.

[16] *See* Dorothy A. Hertzel, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429, 431 (2000). Passive data collection includes clickstream data, IP addresses, cookies, and Web bugs. *Id*.

the Web site with the requested information.[17] Common examples of this type of information include the child's name, e-mail address, postal address, telephone number, age or date of birth, and gender.[18] Most users tend to voluntarily disclose this type of information, especially children.[19] Web sites typically use registration forms, order forms, surveys, contests, and games to gather this information.[20]

Web sites use many different methods to solicit personal information, specifically from children.[21] According to the FTC, some Web sites use imaginary characters to request personal information.[22] Other sites ask "children [to] sign a 'guest book,' solicit information to create home pages for children, invite

---

[17] *See* Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, 29 (2000).

[18] June 1998 Report, *supra* note 6, at 24. Some Web sites ask information about where children attend school, what sports they play, whether they have any siblings, what they have named their pets, and even whether they have time after school alone without parental supervision. 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan). Personal financial information is also collected, such as family income, ownership of stocks, and children's receipt of financial gifts from grandparents. *Id*.

[19] *See* Hertzel, *supra* note 16, at 432.

[20] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter May 2000 Report]; *see also* Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1 (1999) (discussing that Web sites frequently gather personal information from online registration forms, mailing lists, surveys, user profiles, and order fulfillment forms). Cyberkids' Privacy Policy explains that the site requires registration or asks for personal information only for "certain special technology features, such as posting messages, chatting, entering contests and drawings, downloading free software, or receiving our e-mail bulletins." Cyberkids, *at* http://www.cyberkids.com/info/legal/privacypolicy/html (last visited Aug. 8, 2001). This site is compliant with the COPPA, and its Privacy Policy continues: "After you fill out a fast, one-time registration form—and, if you are under 12, you print out the permission form and have your parent sign and return it—you can log into these areas anytime." *Id*.

[21] *See* June 1998 Report, *supra* note 6, at 33.

[22] June 1998 Report, *supra* note 6, at 33.

children to participate in chat and electronic pen pal programs, require children to register with the site for updates and information, and offer prizes and other incentives for completing surveys and polls."[23] Finally, children commonly reveal personal information while participating in chat rooms or posting messages on electronic bulletin boards.[24]

The second method of collecting information, passive data collection, is less obvious because it is collected surreptitiously.[25] Each time a person visits a particular site, an "electronic marker" is left whereby the individual unknowingly provides valuable information to the Web site operator.[26] The type of information revealed includes the user's Internet service provider, type of computer and software, the site from which she linked, the files accessed, and the amount of time she spent on each page.[27] Web

---

[23] June 1998 Report, *supra* note 6, at 33. Questionnaires are also used to obtain information about the children's age, gender, geographic location, and personal finances. June 1998 Report, *supra* note 6, at 33.

[24] *See* June 1998 Report, *supra* note 6, at 4 (emphasizing the safety and privacy concerns since these areas are publicly accessible to anyone surfing the Web).

[25] *See* Hertzel, *supra* note 16, at 431; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1226-1227 (1998). Unless Web sites provide notice, users may be completely unaware that their activities online are being monitored. *See generally* FTC, *Online Profiling: A Report to Congress, Part 2 Recommendations* (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm [hereinafter Online Profiling Report] (discussing fair information practices for online profiling by network advertising companies).

[26] *See* Hertzel, *supra* note 16, at 431-32.

[27] Hertzel, *supra* note 16, at 432; Debra A. Valentine, *Privacy on the Internet: The Evolving Legal Landscape*, 16 SANTA CLARA COMPUTER & HIGH TECH L.J. 401 (2000). *See also* Justin Matlick, *The Future of the Net: Don't Restrain Trade in Information*, WALL ST. J., Dec. 2, 1998, at A22 (providing that "[c]ookies alone cannot divulge your name or address, but they can reveal how long you stay at a page, which products you like, and which sites you visit"); Sinrod, *supra* note 20, at 4 (stating that cookies are "small files on the user's computer that can contain any information that the Web site deposits there, including the names of the pages the user visited or what the user typed").

sites gain this type of information by setting "cookies,"[28] which effectively gather information without the user's knowledge, and are useful to personalize the browsing experience.[29] Once a cookie is set, the user's computer is assigned a unique identifier so that the user can be recognized in future visits to the site.[30]

---

[28] Cookies are small text files placed on a consumer's computer hard drive by a Web server. *See* U.S. Dept. of Energy: Computer Incident Advisory Capability ("CIAC"), *at* http://www.ciac.org/ciac/bulletins/i-034.shtml (Mar. 12, 1998). They are pieces of data that are used to identify Web users. *Id*. Cookies provide information about the user, such as site preferences, search queries, and shopping habits. *See* May 2000 Report, *supra* note 20, at 6 n.45; Jessica J. Thill, *The Cookie Monster: From Sesame Street to Your Hard Drive*, 52 S.C. L. REV. 921 (2001). In addition to the particular Web site that users visit, ad banner services and advertisers also place cookies on visitors' hard drives. *See* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743 (2000) [hereinafter Schwartz, *Beyond Lessig's Code*].

[29] Kang, *supra* note 25, at 1227. Web bugs (also known as "Clear GIFs") are more advanced forms of cookies. *See* John L. Barlament, *A Primer on Online Privacy*, WIS. LAW. Feb. 2001, at 19. Often used in combination with cookies, Web bugs provide a method for passing information from the user's computer to third party Web sites, such as advertising networks. *See, e.g.*, TechWeb.com, http://www.techweb.com (last visited Aug. 27, 2001). When a network of Web bugs is created, once a user discloses personal information to one site in the Web bug network, any other Web site in the network has access to such information. *See* John L. Barlament, *A Primer on Online Privacy*, WIS. LAW. Feb. 2001, at 19. Thus, Web bugs are more invasive than cookies because users are not aware that they are potentially being monitored by a host of Web sites. *Id*.

[30] Valentine, *supra* note 27, at 402 n.4. The following five simple steps outline generally how a cookie works. First, a user chooses an Internet site to visit. John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001, at C10 [hereinafter Schwartz, *Giving Web a Memory*]. Second, the user's computer sends a request for information to the computer running the particular Web site. *Id*. Next, the Web site computer, called a server, sends the information that enables the user's computer to display the site. *Id*. At the same time, it also sends a cookie. *Id*. Fourth, the user's computer receives the cookie and stores it in a file on the hard drive. *Id*. As a result, whenever the user returns to the Web site, the server running the site retrieves the cookie to help identify the individual user. *Id*.

Barnes & Noble.com's Privacy Policy explains that its Web site uses

Thus, advertisers now have the ability to assign cookies to users' computers enabling them to track users by reading information stored in the cookies at each site visited.[31] While such information does not necessarily identify a particular individual, it can be combined with other identifying information such as online registration data, whereby an individual user profile can be created.[32]

Information collection online, through both active and passive methods, is so widespread that nearly all Web sites routinely collect personal information from consumers.[33] The FTC's May 2000 Report, which included the result of its most recent Internet survey, showed that almost all Web sites obtain an e-mail address or some other type of personally identifiable information.[34]

---

cookies to collect and store customer information in order to speed navigation, keep track of items, and provide customer-tailored content. *See* Barnes & Noble.com, *at* http://www.barnesandnoble.com/help/nc_privacy_policy.asp?userid=19YB9OKU42 (last visited Nov. 12, 2001). The site explains that cookies save customers from having to reenter their information each time they visit the Web site. *Id*. Users may elect to set their browser to refuse cookies; however, the Web site warns that this will prevent customers from benefiting from express checkout and from enjoying a personally tailored shopping experience. *Id*.

[31] Valentine, *supra* note 27, at 402 n.4. This type of passive data collection is also known as "clickstream" data. *See* Schwartz, *Giving Web a Memory*, *supra* note 30, at C10. *See also* Barlament, *supra* note 30, at 19 (discussing that clickstream data provides a virtual map of the users' travels on the Internet and typically includes information about the Web sites the user visited, purchases the user made, and ads on which the user clicked); Kang, *supra* note 25, at 1227 (explaining that the "clicktrail" of a user records pages the user visits by order, time, and duration).

[32] Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1170 (1997); Schwartz, *Giving Web a Memory*, *supra* note 29, at C10 (combining the information makes the cookie a "powerful mechanism for personal tracking").

[33] May 2000 Report, *supra* note 20, at 9.

[34] May 2000 Report, *supra* note 20, at 9 (finding that 97% in the Random Sample (335 Web sites) and 99% in the Most Popular Group (91 of the 100 busiest Web sites in January 2000) gather personal information). These statistics confirm the results of the FTC's June 1998 survey. *See* June 1998 Report, *supra* note 6, at 23 (finding that 92% of Web sites collect personal information).

Additionally, well over one-half of the sites collect non-identifying information.[35] However, the FTC found that 86% of these Web sites fail to disclose their information practices.[36] More importantly, the survey results specifically relating to children's Web sites showed that 89% of the 212 Web sites surveyed collect one or more types of personal information from youthful audiences.[37] The FTC found that Web sites collecting personally identifiable information also commonly collect several other types of information that enable them to form a detailed child profile.[38] Moreover, the survey indicates that disclosure practices for children's Web sites are significantly higher than those of the general Web site sample.[39] Yet, the presence of any

---

[35] May 2000 Report, *supra* note 20, at 9 (finding that 68% of Web sites in the Random Sample and 77% in the Most Popular Group fail to disclose such practices). Examples of non-identifying information include children's education levels, hobbies, and favorite toys. June 1998 Report, *supra* note 6, at 32; May 2000 Report, *supra* note 20, at 46 n.54. Such non-identifying information alone cannot be used to identify a specific child. May 2000 Report, *supra* note 20, at 46 n.54.

[36] June 1998 Report, *supra* note 6, at 27. The survey looked for a Privacy Policy Notice or an Information Practice Statement, and found that either's appearance was very rare. June 1998 Report, *supra* note 6, at 27. While Web site providers are not legally required to disclose their information practices, many have taken initiative to explain their privacy policies. The FTC suggests that certain guidelines be followed and incorporated into Web sites' privacy policies. *See infra* Part III.A and note 109 (discussing the FTC's Fair Information Practice Principles—Notice, Choice, Access, Security and Enforcement).

[37] June 1998 Report, *supra* note 6, at 31 (discussing the survey's findings on personal information collection from children).

[38] June 1998 Report, *supra* note 6, at 32 (specifying that 21% of the Web sites that collect children's names and/or e-mail addresses also collect five or more additional types of personal information from children, 48% collect three or more, and 77% collect one or more).

[39] June 1998 Report, *supra* note 6, at 34. Specifically, 54% of children's Web sites have an information practice disclosure. June 1998 Report, *supra* note 6, at 34. As to the specific nature of the disclosures on children's Web sites, forty-three of the 109 sites that collect personal information and have at least one information practice disclosure, provide children or their parents with choices about how their information will be used. June 1998 Report, *supra* note 6, at 35. Furthermore, 12% of these sites disclosed that they

privacy policy notice is much lower.[40] Understandably, the result of this widespread collection of personal information has raised many privacy concerns, especially about the use of the information.[41]

B. The Value of Information

Electronic commerce ("e-commerce") through the Internet has had an extraordinary impact on business and society within the last decade.[42] The information collected by a Web site is likely to be used either directly to benefit the Web site or sold to assist market research companies or direct marketing services.[43] Any benefit to the Web site arguably extends to the user who gains a more personalized Web browsing experience.[44] A user's information also may be made accessible to public online users or stored by Web sites for later use or sale.[45] Furthermore, the Internet offers advertisers and marketers the unique opportunity to gain direct access to children.[46]

---

offered access to the information or a chance to correct any mistakes. June 1998 Report, *supra* note 6, at 36. Again, only 12% said that they would notify a parent of the Web site's information practices. June 1998 Report, *supra* note 6, at 36.

[40] June 1998 Report, *supra* note 6, at 35 (stating only 24% of Web sites that collect personal information from children have a privacy policy notice).

[41] A recent survey of 1,000 adults indicated that 78% of online adults and 77% of online parents are very concerned about children's privacy. *Adults Worry About Kids' Online Privacy*, EMARKETER, *at* http://www.emarketer.com/estats/200000714_privacy.html (last visited Sept. 7, 2000). Other surveys show that parents support limiting the collection and use of their children's personal information. June 1998 Report, *supra* note 6, at 6 (stating that 97% of parents whose children use the Internet feel that Web sites should not sell children's personal information, and 72% of parents were opposed to a Web site requesting a child's name and address in order to register at a site).

[42] Saami Zain, *Regulation of E-Commerce by Contract: Is It Fair to Consumers?*, 31 UWLA L. REV. 163, 163 (2000).

[43] Sinrod, *supra* note 20, at 5.

[44] *See* Hertzel, *supra* note 16, at 433.

[45] Hertzel, *supra* note 16, at 432-33.

[46] Center for Media Education ("CME"), *Web of Deception: Threats to*

Tracking online navigational patterns, commonly by employing cookies, is useful for the Web site to make improvements to its own site and to personalize the user's online experience.[47] The information allows the Web site to monitor and understand what attracts children to the site and then tailor the site's content and services based on the children's identified interests.[48] For example, the FTC found that some sites use the information specifically to ask children for feedback about the site.[49] The FTC also found that some sites collect e-mail addresses to send children newsletters and notices about online contests and opportunities to win prizes.[50] Therefore, knowing a child's preferences gives the Web site a competitive advantage because it can tailor its content and activities to suit its specific audience.[51]

The most widespread and lucrative use of personal information is for marketing.[52] Direct marketing, also known as

---

Children From Online Marketing (1996), *available at* http://www.cme.org/children/marketing/deception.pdf [hereinafter *Web of Deception*] (explaining that direct marketers capture children's attention online through one-to-one marketing that effectively bypasses parents and teachers to directly reach children).

[47] Gindin, *supra* note 32, at 1170. While Web site operators believe that an increased use of online tracking devices, such as cookies, will increase the amount of visits to their Web sites by personalizing the user's online experience, a majority of Americans disagree. *See* John B. Horrigan, Pew Internet & American Life Project, *New Internet Users: What They Do Online, What They Don't, and Implications for the Net's Future* (Sept. 25, 2000), *available at* http://www.pewinternet.org/reports/pdfs/New_User_Report.pdf. A report, based on a survey of 4606 Americans and 2277 Internet users, revealed that only about a quarter of the Internet users (27%) agree that online tracking of their activities is helpful or useful. *Id*. Moreover, 54% of the people surveyed believe tracking that provides personal information to Web sites is harmful because it invades their privacy. *Id*.

[48] Gindin, *supra* note 32, at 1171. *See also* Matlick, *supra* note 27, at A22.

[49] June 1998 Report, *supra* note 6, at 34.

[50] June 1998 Report, *supra* note 6, at 34.

[51] *See* Hertzel, *supra* note 16, at 433; Thill, *supra* note 28, at 945.

[52] *See* Safier, *supra* note 17, at 59. *See also* Gindin, *supra* note 32, at 1171; Kang, *supra* note 25, at 1240. Companies can increase revenues by

one-to-one marketing,[53] involves the strategic positioning of goods or services to appeal to small, clearly defined groups of people.[54] The groups can be identified through the use of personal information collected by the Web sites, thereby allowing marketing and advertising to be tailored to these audiences.[55] Such personalized and focused advertising is instrumental to successful online marketing.[56] The tracking technology enables

selling advertising space that targets specific customer preferences on their Web sites. *See* Valentine, *supra* note 27, at 402 (stating that "[a]n entire industry has emerged to market a variety of software products designed to assist Internet sites in collecting and analyzing visitor data and in serving targeted advertising"). *See also* FTC, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf [hereinafter July 1999 Report] (discussing the growth of electronic commerce). The Chief Executive Officer of Newfront Productions, a company operating several Web sites including Nancydrew.com, explained that the only way to make money on the Internet is through advertising. *See* Jennifer DiSabatino, *Report: Kids' Sites Fail on Privacy*, PC WORLD.COM, *at* http://www.pcworld.com/resource/printable/article/0,aid,45744,00.asp (Mar. 28, 2001). He continued that in order to sell advertising space, a site must show traffic information. *Id*.

[53] One-to-one marketing is "'selling to customers one at a time and getting each one to buy as many products as possible over a lifetime.'" *Web of Deception*, *supra* note 46, at 5 (reporting that children as young as four years old are targeted by online advertisers).

[54] Safier, *supra* note 17, at 60.

[55] Safier, *supra* note 17, at 60. Cookies play an important role in collecting information. They provide information "to track visits to the Web site to learn what visitors like and dislike about the site, and to personalize the site so that options the user selects at the first visit can be used automatically for each successive visit." Gindin, *supra* note 32, at 1170. Cookies are especially popular on Internet shopping sites to monitor the users and the products in their shopping carts. *See* U.S. Dept. of Energy, *supra* note 28. Cookiecentral reports that the main use of cookies is for targeted marketing. *See* Cookiecentral.com, http://www.cookiecentral.com/content.phtml?area=2&id=1 (last visited Nov. 12, 2001). Cookies offer accurate counts of the number of visitors to a particular Web site and the advertisements clicked on, which is then used to target the particular user. *Id*.

[56] Hertzel, *supra* note 16, at 433. This results in the Internet user's receipt of targeted ads after showing interest in a particular topic. *See* JEFFREY ROSEN, THE UNWANTED GAZE 163-164 (2000) (citing an example where a company sends an ad for a new prostate cancer treatment to an Internet user

Web sites to follow every interaction between a child and an advertisement.[57] Companies have a financial incentive to obtain users' personal information because studies show that direct marketing receives a more favorable response than random ads sent to online users.[58] Finally, fierce competition on the Internet results in increased reliance by Web site operators on direct marketers to attract and retain customers.[59]

In addition, Web sites sell their collected information to list vendors. List vendors gather personal information by buying, selling and trading lists from both public and private sources.[60]

---

who visits a Web site about prostate cancer and proceeds to purchase a book on the subject).

[57] *Web of Deception*, *supra* note 46, at 1.

[58] Hertzel, *supra* note 16, at 433. "The ultimate goal is to create personalized interactive ads designed to 'microtarget' the individual child." *Web of Deception*, *supra* note 46, at 4.

[59] Robert L. Eisenbach III, *The Internet Company's Customer List: Asset or Liability?*, 18 COMPUTER & INTERNET L. 24 (2001). The direct marketing industry generates large amounts of business. More than two-thirds of all Web sites targeted at children and teenagers use advertising as their primary source of revenue. Ellen Neuborne, *For Kids on the Web, It's an Ad, Ad, Ad, Ad World*, BUS. WK. 108 (Aug. 13, 2001), *available at* 2001 WL 2208433. In 1999, Internet advertising expenditures reached $4.6 billion. Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455 (2001). Additionally, the Direct Marketing Association ("DMA") projects online expenditures for direct marketing to reach $13.8 billion in 2005. DMA, *Economic Impact: U.S. Direct Marketing Today*, *at* http://www.thedma.org/library/publications/libres-ecoimpact2.shtml (last visited Aug. 30, 2001). Furthermore, a recent study on the interactive e-commerce marketing industry, conducted by the DMA, found that 34% of the respondents reported that an average of $99 or higher is spent per transaction. DMA, *Direct Marketers Report More Efficient Web Operations*, *at* http://www.the-dma.org/news/newsstory131.shtml (last visited Sept. 16, 2000). Forty-two percent of the Web businesses report online revenues of $200,000 or more. *Id*. Also, according to the report, respondents identify marketing information as the primary purpose of their Web sites. *Id*. The number of children's Web sites without advertising has dropped from 10% of all children's sites last year to just 2% today. Ellen Neuborne, *For Kids on the Web, It's an Ad, Ad, Ad, Ad World*, BUS. WK. 108 (Aug. 13, 2001), *available at* 2001 WL 2208433.

[60] Safier, *supra* note 17, at 61. Major firms in this industry, especially

The information obtained on the lists is reorganized to produce new lists that are geared toward specific interests.[61] Lists are created for virtually all types of consumers.[62] Thus, profiles are created that specifically identify a consumer's demographics, hobbies, interests, preferences, and other useful information.[63] Such lists are valuable to predict and indicate the demands of list buyers.[64] The value in children's personal information is undeniable, but the collection and use of the information creates great potential for misuse and threatens the privacy of children.[65]

Marketers actively pursue children as influential consumers.[66] Children not only have their own spending power but also have a strong influence on their parents' spending.[67] Furthermore, children are unique because they are often early purchasers of high-tech products, which make them a crucial target for new interactive media.[68] In 1995, children under the age of twelve spent $14 billion.[69] Moreover, the total online retail sales for 1999 were approximately $20 to $30 billion.[70] Thus, Web sites

---

credit card reporting agencies, maintain files on more than 90% of adults. Safier, *supra* note 17, at 61.

[61] Safier, *supra* note 17, at 61.

[62] *See* Safier, *supra* note 17, at 61.

[63] Safier, *supra* note 17, at 62.

[64] Safier, *supra* note 17, at 62; Robert L. Eisenbach III, *The Internet Company's List: Asset or Liability?*, LAW.COM, *at* http://www.law.com (May 29, 2001).

[65] *See* discussion *infra* Part I.C (explaining that the lack of control over children's personal information once it is disclosed poses dangers to children, such as a threat of inappropriate contact with strangers).

[66] *See* June 1998 Report, *supra* note 6, at 4; *Web of Deception*, *supra* note 46, at 4.

[67] *Web of Deception*, *supra* note 46, at 4 (finding that in 1995, children, together with teenagers, influenced $160 billion of their parents' annual spending).

[68] *Web of Deception*, *supra* note 46, at 4.

[69] *Web of Deception*, *supra* note 46, at 4. *See also* June 1998 Report, *supra* note 6, at 4 (estimating that children spend billions of dollars per year and have the ability to influence the expenditure of billions more).

[70] *See* May 2000 Report, *supra* note 20, at 1, 39 n.6. Recent surveys show that consumer online spending is increasing. *See* Press Release,

have a business incentive to collect information, and technological advances provide a means to gather unlimited amounts of personal information.

C. The Threat to Children and the Need to Protect Their Privacy

As a result of this unrestricted information collection, children's privacy online has emerged as a paramount concern.[71]

Shop.org Research, Online Retail Market in North America to Reach $65 Billion in 2001, *at* http://www.shop.org/press/01/050201.html (May 2, 2001) (according to the latest report on online retail, conducted by The Boston Consulting Group, the online retail market in North America is expected to reach $65 billion in 2001); Forrester Research, *Consumers Spent $4 Billion Online in August*, According to the Forrester Research Online Retail Index, *at* http://www.forrester.com/ER/Press/Release/0,1769,630,00.html (Sept. 25, 2001) (reporting that the total amount spent on online sales in the United States increased from $3.98 billion in July 2001 to slightly more than $4 billion in August 2001).

[71] *See supra* note 41 and accompanying text (indicating that parents are very concerned about their children's privacy). As a result of legitimate concern, many parents set time limits on their children's use of the Internet. *Teenage Life Online*, *supra* note 4, at 4. Efforts that some parents make to protect their children online include locating the family computer in a public space in the house, surfing the Internet together with their children, checking on their children's activities after the child has used the Internet, and installing filters to control the Web sites that their children can access. *Teenage Life Online*, *supra* note 4, at 4. Parents are largely motivated by fear that their children are meeting strangers online. Approximately 57% of parents surveyed are concerned that strangers will contact their children on the Internet. *Teenage Life Online*, *supra* note 4, at 5. This concern is well founded because almost 60% of the teenagers surveyed had received an instant message or e-mail from a stranger, and 63% admit that they respond to strangers online. *Teenage Life Online*, *supra* note 4, at 19. A thirteen year old girl expressed her concern for meeting strangers online and sharing personal information:

> I think people give a lot of fake info online all the time. Yeah, I guess I worry about it because of my friends' safety. They talk to people they have no idea who they are and sometime [sic] I find myself telling them that it might not be the person who they think it is. . . . Some of my friends think they're talking to Justin from N'sync, but I don't think so. There is so much information about him that anyone

It has become increasingly difficult to protect privacy interests in the face of recent technological advances.[72] Today, innovative technology encourages easier and less expensive means of gathering, storing, analyzing, transmitting, and reusing personal information that were inconceivable just a few years ago.[73] The result is a decreased ability to maintain control over one's personal information. This is a great infringement on privacy.[74]

---

can impersonate him. I think it's quite scary.

Teenage Life Online, *supra* note 4, at 23.

[72] *See infra* note 266 (explaining that because the Internet is so vast and has no boundaries, it is very difficult to police).

[73] Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, 6 (1999). The introduction of cookies to the Internet fundamentally changed the nature of surfing the Web from being a relatively anonymous activity to an environment where a record of one's transactions, movements, interests, and desires can be sorted, mined, stored and sold. *See* Schwartz, *Giving Web a Memory*, *supra* note 30, at C10.

[74] The privacy interest at issue in the collection of personal information on the Internet is distinct from the constitutional right to privacy. While the United States Constitution does not specifically guarantee a right to privacy, the U.S. Supreme Court has interpreted the Constitution to protect a right of privacy in making certain decisions from governmental intrusion. Gindin, *supra* note 32, at 1185. These personal, intimate decisions concern matters relating to contraception, marriage, reproduction, and child rearing. *See* Jed Rubenfeld, *The Right to Privacy*, 102 HARV. L. REV. 737 (1989). *See also* Roe v. Wade, 410 U.S. 113, 153 (1973) (finding a constitutional zone of privacy in a "woman's decision whether or not to terminate her pregnancy"); Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that the use of contraceptives is a private and intimate decision). Non-governmental intrusions on the right of privacy are generally protected by tort law. The four privacy torts are intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicly placing a person in false light. RESTATEMENT (SECOND) OF TORTS § 652A (1977) (classifying the various privacy torts). For a detailed discussion of the tort right of privacy, *see generally* Gindin, *supra* note 32, at 1188-1193; Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Schwartz, *Beyond Lessig's Code*, *supra* note 28, at 743; Thill, *supra* note 28, at 921. Since this Note concerns children's information on the Internet, the focus of this note is on information privacy, which is not protected under the constitution or tort law. *See infra* notes 75-76 and

The general privacy interest that is being threatened by the Internet involves the individual's right to control information about his or her person.[75] While the information itself may not be especially embarrassing or intimate,[76] it is personal because it connects the information to the individual and it could be

---

accompanying text (defining information privacy).

[75] This is known as information privacy. The definition of privacy has been widely explored. *See* Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 648 (2001) (meaning "control by an individual over data generated during Internet transactions that is either personally identifiable to that individual or which may be merged with other data to become personally identifiable to her"); Kang, *supra* note 25, at 1205 (defining information privacy as the individual's right to control the extent to which personal information is acquired, disclosed, and used); Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information Is It Anyway?*, 38 JURIMETRICS J. 565, 566-67 (1998) (discussing the individual's control over the flow of information in terms of disclosure, distribution, use, and abuse); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) (describing privacy as an individual's right to control the use of his or her personal information). Internet users should be confident that their personal information they entrust to others is protected. *See* John Schwartz, *As Big PC Brother Watches, Users Encounter Frustration*, N.Y. TIMES, Sept. 5, 2001, at C6. There is a strong congressional desire to "keep the individual's right to privacy apace with advances in technology that increase exponentially the chances that an individual's privacy can be breached." Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 238 (D.N.J. 1996). Whereas privacy protections in tort apply only to information that is sensitive, embarrassing, or intimate, information privacy recognizes a privacy interest in any personally identifiable information. *See, e.g.*, U.S. Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (identifying a strong privacy interest in the personal information maintained in FBI rap sheets); Whalen v. Roe, 429 U.S. 589, 605 (1977) (recognizing the threat to privacy imposed by the accumulation of large amounts of information in computerized data banks on individuals taking prescriptive drugs).

[76] For examples of information that is sensitive and embarrassing, *see* U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999) (discussing "customer proprietary network information" ("CPNI")); Lanphere v. Colorado, 21 F.3d 1508, 1514 (10th Cir. 1994) (sensitive information in criminal records); Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1229 (7th Cir. 1993) (detailing one's personal life).

exploited or misused.[77] In today's society, there are few facts that are not at one point disclosed to someone.[78] Thus, it is important to recognize that the interest being protected is not necessarily total nondisclosure, but rather selective disclosure.[79] The fact that certain information is attainable elsewhere in society, a strong privacy interest in that information is not improper.[80]

Personal information is subject to a multiplicity of potential invasions. First, the mere fact that a complete personal profile of a single individual is compiled is a threat to privacy.[81]

---

[77] Kang, *supra* note 25, at 1207, 1246; Gindin, *supra* note 32, at 1171. For example, a great amount of personal, yet not embarrassing, information can be retrieved simply by knowing another's driver's license number, credit card number, and social security number. *See* Michael L. Closen et al., *Notarial Records and the Preservation of the Expectation of Privacy*, 35 U.S.F. L. REV. 159, 169 nn.55, 207 (2001). Embarrassing information is more likely found in health records, which may reveal intimate details about an individual's physical and mental fitness. *Id*. The distinction between information that is embarrassing and information that is personal is what distinguishes the tort right of privacy from information privacy. The latter is not limited to embarrassing or intimate information. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1291 (2000) (explaining that tort law protects the disclosure of embarrassing personal information, not simply the collection and use of personally identifiable information). The COPPA seeks to protect children's privacy interests in non-intimate personal information. *See* 15 U.S.C. § 6501(8) (defining personal information as "individually identifiable information about an individual," such as a name, address, telephone number or social security number).

[78] *Reporters Comm.*, 489 U.S. at 763 n.14. *See also* Litman, *supra* note 77, at 1291 ("Almost everything each of us does seems to generate transactional information [that] is collected, aggregated, and stored on computers.").

[79] *Reporters Comm.*, 489 U.S. at 763 (explaining that most people cannot completely prevent others from knowing certain facts about themselves).

[80] *Id*. at 762-64 (noting that the privacy interest in maintaining the "practical obscurity" of FBI rap sheet information is very high). The court introduced this notion of the practical obscurity in information that is stored in centralized databases as compared to information that is scattered and dispersed in small pieces. *Id*.

[81] *See id*. at 764 (highlighting the difference in personal privacy between scattered pieces of information about an individual and a comprehensive

Maintenance of such comprehensive profiles is more threatening than when individual pieces of information are considered separately.[82] Furthermore, online profiles create a greater threat to privacy than the same profiles that are created in the off-line world because digital data can be preserved indefinitely.[83] An investigation by the Center for Media Education ("CME") found that the practice of soliciting personal information from children and tracking their online use was quite invasive and disturbing.[84]

A second serious invasion of privacy occurs where the personal information is disclosed to third parties without consent of the individual.[85] This is especially dangerous because it is not always apparent to whom the Web site provides the personal information.[86] Typically, the Web site sells the information collected online to marketers or other companies, or stores it for future use or sale.[87] The information may, however, also be made accessible to other online users, whose identities remain undisclosed.[88] A great harm occurs when the information is misused by direct marketers and others who overstep the boundary between persuasion and undue influence.[89] Congress

---

compilation of information in a rap sheet). *See also* Kang, *supra* note 25, at 1240, 1241 n.213.

[82] *See* Kang, *supra* note 25, 1240.

[83] Belgum, *supra* note 73, at 9 (describing various threats to online privacy with emphasis on the permanence of data stored in digital form).

[84] *Web of Deception*, *supra* note 46 (investigating new advertising and marketing techniques directed specifically at children). The study revealed collection techniques, such as offering children free gifts or prizes for providing information about themselves through online surveys, tracking children's online activities to create detailed personal profiles, and tailoring personal advertisements to particular children. *Web of Deception*, *supra* note 46, at 5.

[85] Rosenbaum, *supra* note 75, at 567. *See also supra* notes 58-60 (discussing why companies disclose such information to third parties).

[86] Hertzel, *supra* note 16, at 434.

[87] Hertzel, *supra* note 16, at 432-433.

[88] June 1998 Report, *supra* note 6, at 36 (listing the two primary methods that Web sites use to disclose children's information to third parties).

[89] Gindin, *supra* note 32, at 1171; Kang, *supra* note 25, at 1215. The direct marketers make an important countervailing argument, however. They

has recognized abuse when a child's profile enables companies to target and entice him or her to purchase various products.[90] Thus, the exploitation of vulnerable children using the Internet through unfair and deceptive methods of advertising and marketing is a primary threat.[91]

The collection of detailed personal information from children,

---

see the free flow of information as enhancing the market and as helpful to the consumer by providing useful information directly related to the individual's personal tastes. *See* Stephen R. Bergerson, *E-commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527 (2001).

[90] 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan) (emphasizing that children are communicating with Internet marketers without the parent's knowledge). Senator Bryan explains that such communication could lead to an interactive relationship with the child. *Id*. He offers the comparison that if a child were to talk to a stranger and start answering questions, a parent would quickly become suspicious and question to whom he or she was talking. *Id*. However, when a child is online, the danger increases because parents typically have no knowledge about who may be interacting with their child. *Id*.

[91] *Web of Deception*, *supra* note 46, at 7-8, 13 (recognizing that marketers have the ability to pursue children with little regulatory or legal restraint). For example, "entire electronic advertising 'environments' have been built to entice children to spend countless hours playing with such popular product 'spokescharacters' as Tony the Tiger, Chester Cheetah, and Snap! Crackle! & Pop!." *Web of Deception*, *supra* note 46, at 1. Very young children often confuse "fantasy and real-live characters" and elementary schoolchildren tend to identify with fictional characters and emulate their behavior. *Web of Deception*, *supra* note 46, at 18. Thus, the potential for exploitation and manipulation increases when marketers use spokescharacters in combination with one-to-one marketing. *Web of Deception*, *supra* note 46, at 18. These interactive experiences are developed to encourage children to click on icons that immediately transfer them to advertising sites. *Web of Deception*, *supra* note 46, at 2. Ad banners are used to meet online advertisers' goals of capturing and holding children's attention at the Web site for as long as possible. *Web of Deception*, *supra* note 46, at 13. The use of an ad banner is one of the most common methods of advertising on the Internet. *Web of Deception*, *supra* note 46, at 13. "When children click on a banner, they are whisked away to an interactive advertising environment, with activities designed to keep children engaged for extended periods of time." *Web of Deception*, *supra* note 46, at 13. These activities include playing games, downloading movie and sound clips, and interacting with coloring book pages. *Web of Deception*, *supra* note 46, at 14.

without parental consent or guidance, poses unique privacy and safety concerns.[92] Minor children have always received greater protection because they are considered less capable of protecting themselves.[93] Furthermore, children do not maintain the cognitive ability to fully recognize and understand privacy concerns.[94] Children become completely absorbed in their online experience, and this creates a golden opportunity for all sorts of potential threats and propositions by advertisers.[95] The greatest safety concern is posed by the availability of children's personally identifiable information in interactive public areas.[96] Places such as chat rooms and bulletin boards are accessible to all online users.[97] Thus, children are able to freely interact with strangers; the anonymity[98] of the Internet does not afford them the ability to

---

[92] June 1998 Report, *supra* note 6, at 4.

[93] Hertzel, *supra* note 16, at 434. Children have not been afforded the same degree of constitutional protections as adults. *See* Michele D. Sullivan, *From Warren to Rehnquist: The Growing Conservative Trend in the Supreme Court's Treatment of Children*, 65 ST. JOHN'S L. REV. 1139, 1139 (1991). *See also* Bethel Sch. Dist. v. Fraser, 478 U.S. 675, 682 (1986) (acknowledging that children in public schools are not bestowed the same First Amendment privileges as adults); H.L. v. Matheson, 450 U.S. 398, 413 (1981) (allowing the state to require parental notification before dependant, unmarried minor child may have an abortion); Ginsberg v. New York, 390 U.S. 629, 649-50 (1968) (upholding a state's right to limit a minor's access to sexually explicit material).

[94] Hertzel, *supra* note 16, at 434. Children are not likely to comprehend the nature of the information being sought or its intended uses. Hertzel, *supra* note 16, at 434.

[95] June 1998 Report, *supra* note 6, at 5; *Web of Deception*, *supra* note 46, at 5.

[96] June 1998 Report, *supra* note 6, at 5. Many children using the Internet commonly encounter attempted password theft and inappropriate propositions in children's chat rooms. June 1998 Report, *supra* note 6, at 5.

[97] June 1998 Report, *supra* note 6, at 5. Children's use of chat rooms and bulletin boards that are accessible to all online users presents serious safety risks because the enhanced communication with strangers creates an opportunity for predators to identify and contact children. June 1998 Report, *supra* note 6, at 5.

[98] Users' identities can remain secret through the use of screen names and IP addresses. *See* Thill, *supra* note 28, at 921. Thus, users are able to access

recognize whether they are communicating with another child or an adult posing as a child.[99] The privacy concern inherent in marketing to children online is that marketers have the power to circumvent the child's guardian.[100] Children can be reached directly online without the traditional protection of a parent or teacher.[101] This, coupled with children's more vulnerable and trusting characteristics,[102] allows companies to establish individual relationships with children online.[103] Therefore, when a child receives a personalized message from his or her favorite cartoon character, it will be especially difficult for the child to ignore.[104]

Children need special protection from unwarranted disclosures of their personal information. It is ironic that the same extraordinary innovations in computers and the Internet that

---

information, chat rooms, and Web sites with the protection of a fictional identity. *See* Thill, *supra* note 28, at 921.

[99] June 1998 Report, *supra* note 6, at 5, 8.

[100] *Web of Deception*, *supra* note 46, at 5. Invasions of privacy are further increased due to the immediacy and ease with which personal information can be collected online. June 1998 Report, *supra* note 6, at 6; May 2000 Report, *supra* note 20, at 33 (stating that "the prevalence, ease, and relatively low cost of [personal] information collection and use . . . raises significant consumer privacy concerns"). Children should be able to take advantage of the Internet without sacrificing their personal privacy and safety. *See* Landesberg & Mazzarella, *supra* note 14; *see also supra* Part I.A (discussing the methods of collecting information).

[101] *Web of Deception*, *supra* note 46, at 5.

[102] Children tend to be more trusting than adults and, therefore, more easily enticed. In *United States v. Reaves*, defendant used his computer to show sexually explicit images to entice his victims, minor children, to engage in illicit sexual conduct. 253 F.3d 1201 (10th Cir. 2001). Furthermore, defendant participated in an online chat with his victim discussing sexual topics, luring the victim into sexual activities and pornography production. *Id*.

[103] *Web of Deception*, *supra* note 46.

[104] *Web of Deception*, *supra* note 46, at 5. Unlike their parents, children are unaware of the potential danger of disclosing personal information about themselves and their parents. *Web of Deception*, *supra* note 46, at 7. They are not adept at deciphering the motives behind online contests and surveys. *Web of Deception*, *supra* note 46, at 7. Therefore, they "easily fall prey to such marketing techniques." *Web of Deception*, *supra* note 46, at 7.

allow children to enjoy new experiences and use exciting resources are also "leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers and criminals."[105] Thus, given the ease with which data is collected, the high value placed on such information and the threats specific to child online users, federal legislation to protect children's privacy is necessary. The COPPA is designed to combat these privacy and safety concerns.

II. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Congress enacted the COPPA in response to the FTC's comprehensive study, *Privacy Online: A Report to Congress*,[106] in order to regulate unfair and deceptive practices in the collection and use of children's personal information on the Internet.[107] The COPPA is designed to incorporate the five essential Fair Information Practice Principles that are recognized by the United States and other countries.[108] Government reports, guidelines, and model codes have identified Notice, Choice, Access, Security, and Enforcement as core principles of privacy protection since 1973.[109] While the COPPA readily recognizes the unlimited

---

[105] 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan). While the Internet allows people to browse, shop, and search for almost anything online from the privacy of their own homes, the dissemination of private information required for business transactions "to even the most minuscule fraction of users of the Web . . . represents a catastrophic loss of privacy to the individual or business consumer." Jeffrey A. Modisett & Cindy M. Lott, *Cyberlaw and E-commerce: A State Attorney General's Perspective*, 94 NW. U. L. REV. 643, 653 (2000).

[106] *See* June 1998 Report, *supra* note 6.

[107] 15 U.S.C. §§ 6501-6505 (Supp. IV 1998); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)).

[108] *See* June 1998 Report, *supra* note 6. *See also* July 1999 Report, *supra* note 52, at 3; May 2000 Report, *supra* note 20.

[109] May 2000 Report, *supra* note 20, at 3. Fair Information Practice Principles were first expressed in the United States Department of Health, Education and Welfare's 1973 report entitled *Records, Computers and the Rights of Citizens*. *See* June 1998 Report, *supra* note 6, at 48 n.27; Valentine,

opportunities that the Internet offers for children's growth and development, it seeks to regulate the practices of Web sites to protect children.[110] Moreover, it properly places parents in

---

supra note 27, at 406 n.22. Since 1973, various governmental and inter-governmental agencies have been instrumental in developing the principles further. Notice is described as the most fundamental principle. *See* June 1998 Report, *supra* note 6, at 7. Consumers should be given notice of an entity's information collection, use, and disclosure practices prior to collecting any personal information from them. June 1998 Report, *supra* note 6, at 7. The notice should inform the consumer as to who is collecting the information, how the information will be used, which third parties may receive the information, the nature and means by which the data is collected, and what steps, if any, are taken to ensure the consumer's confidentiality and integrity of information. June 1998 Report, *supra* note 6, at 7-8. Simply defined, the Choice Principle means providing options to consumers about how their personal information may be used. June 1998 Report, *supra* note 6, at 8. Typically, the Choice Principle allows an entity to choose between opt-in or opt-out regimes. Opt-in models require affirmative steps by the user to allow information to be collected or used. *See* July 1999 Report, *supra* note 52, at 17 n.19. On the other hand, opt-out regimes require affirmative steps to prevent the collection or use of information. July 1999 Report, *supra* note 52, at 17 n.19. *See* Belgum, *supra* note 73, at 50-51, for a general discussion of the differences between opt-in and opt-out provisions. Access refers to the individual's ability to review and contest the information for accuracy and completeness. June 1998 Report, *supra* note 6, at 9. Integrity of information ensures that it is accurate and secure. June 1998 Report, *supra* note 6, at 10. Finally, the core principles can only be effective if they are supported by enforcement mechanisms that ensure compliance or redress injured parties. June 1998 Report, *supra* note 6, at 10. While this is a broad overview of the FTC's analysis of the five core principles, it shows that they were highly regarded in the enactment of the COPPA and the FTC's Final Rule. *See infra* note 179 and accompanying text (applying the principles to the statutory requirements).

[110] 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan). For example, children can use the Internet to reference information in an encyclopedia for a research report. *Id*. Children can also communicate with each other through online chat rooms, pen-pal services, and by posting personal home pages. Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750, 22,751 (proposed Apr. 27, 1999) (codified at 16 C.F.R. § 312 (2001)). However, these experiences can pose a threat to children if they are not regulated with the interest of protecting the dissemination of information freely given by unsuspecting children. *See Web of Deception*, *supra* note 46,

control over their children's personal information online.[111]

The FTC has clearly articulated the four main goals of the COPPA:

> (1) To enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent.[112]

---

at 12.

[111] 146 CONG. REC. E616-01 (May 2, 2000) (statement of Hon. Inslee). The COPPA allows children to explore the Internet with supervision and guidance. 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan). It imposes safeguards to protect against Web sites collecting and disseminating children's personal information that threatens their safety and "most certainly invades their privacy." *Id*. Parents are an integral part of providing children with a safe and private Internet experience. Even though children's technological skills often surpass those of their parents, children lack the requisite judgment for handling communications with strangers on the Internet. *Privacy Protections for Consumers: Oversight Hearing; Recent Developments in Privacy Protections for Consumers Before the Subcomm. on Telecomm. Trade & Consumer Prot*. (Oct. 11, 2000) (testimony of Parry Aftab, Special Counsel, Darby and Darby, P.C.), *available at* 2001 WL 1517025 [hereinafter *Privacy Protections*].

[112] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 22,750; Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,908. *See also* 144 CONG. REC. S12741 (Oct. 7, 1998) (statement of Sen. Bryan). The FTC has taken a strong initiative to investigate and educate the public about online privacy issues. *See* July 1999 Report, *supra* note 52, at 3; May 2000 Report, *supra* note 20, at 42 n.21; *see also* FTC, *Privacy Initiatives*, http://www.ftc.gov/privacy/index.html (last visited Nov. 17, 2001) (listing the FTC's initiatives taken to educate the public about personal information privacy). The FTC held its first public workshop on Internet privacy in April 1995. May 2000 Report, *supra* note 20, at 42 n.21. A series of workshops followed in June 1996 and in June 1997 that focused more specifically on concerns raised by online collection of personal information from children. June 1998 Report, *supra* note 6, at 2; May 2000 Report, *supra* note 20, at 42 n.21. The FTC's primary focus has been to understand the online marketplace

In its June 1998 Report, the FTC emphasized that, because children are not always cognitively capable of protecting their own privacy rights, *parents* should receive notice and maintain control over the collection and use of their children's personal information.[113] Parents need to be given access to the information in order to promote informed consent to the retention and use of the personal information collected.[114] Thus, when children's privacy is being threatened, the FTC is concerned with *parental* notice, choice, access, security, and enforcement.[115] This section will explore the various requirements of the Act, and the following sections will discuss the FTC's rules to implement the Act and the COPPA's effectiveness in realizing its purported goals.

A. Framework

The COPPA protects the personal information of children under the age of thirteen.[116] According to the Act, "personally identifiable information means individually identifiable

---

and its information practices, to analyze the effect of these practices on consumers, and to promote and facilitate effective self-regulation of consumer privacy online. July 1999 Report, *supra* note 52, at 3. *See also* Landesberg & Mazzarella, *supra* note 14, at 309. The FTC's substantial effort has been useful among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in the field of interactive technology. July 1999 Report, *supra* note 52, at 16.

[113] June 1998 Report, *supra* note 6, at 12 (emphasis in original).

[114] June 1998 Report, *supra* note 6, at 12.

[115] June 1998 Report, *supra* note 6, at 12-14 (emphasis added).

[116] Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (Supp. IV 1998) (defining the term child as "an individual under the age of 13"). The FTC will consider a site to be directed at children by looking at the subject matter, the multimedia content, the age of the models, the language used and whether the site uses features such as games, puppets, animated characters or child oriented activities. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2001); Joseph A. Zavaletta, *COPPA, Kids, Cookies & Chat Rooms: We're from the Government and We're Here to Protect Your Children*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 249 (2001).

information about an individual collected online."[117] This includes information such as a first and last name, a home address, an e-mail address, a telephone number, a social security number, any other identifier determined by the FTC that allows an individual to be contacted, and information concerning the child or the child's parent that the Web site collects online and combines with any of the above identifiers.[118]

In general, the COPPA requires a Web site to provide notice if the site is directed at children, or if an operator has actual knowledge that it collects personal information from children.[119] The notice, which appears on the Web site, must include the information that is collected, the use of such information, and the Web site's information disclosure practices.[120] The COPPA further mandates that the operator must obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.[121] Upon request by a parent of a child that supplies personal information, the Web site must provide a description of the information that was collected and an opportunity for the parent to refuse any further use of the collected information.[122]

---

[117] 15 U.S.C. § 6501(8).

[118] *Id*. § 6501(8)(A)-(G). Examples of other identifiers are screen names that reveal children's e-mail addresses and instant messaging identifiers.

[119] The Act defines "operator" as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of . . . where such website or online service is operated for commercial purposes." *Id*. § 6501(2)(A). The COPPA is not applicable to third parties who are not involved in the collection of the personal information. *See* Hertzel, *supra* note 16, at 438. In order to determine whether an entity is an operator, the FTC will examine the relationship of the entity to the information by looking at various factors, including ownership or control of the information, the identity of the purchaser of the information, pre-existing contractual relationships, and the role of the Web site in collecting the information. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)).

[120] *See* 15 U.S.C. § 6502(b)(1)(A)(i).

[121] *See id*. § 6502(b)(1)(A)(ii).

[122] *See id*. § 6502(b)(1)(B)(i)-(ii).

The parental consent requirement is an important aspect of the COPPA that places parents in control of their child's online communications. To obtain verifiable parental consent, a Web site operator must make a reasonable effort, recognizing available technology:

> [This includes] a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.[123]

The consent requirement, however, is subject to various exceptions.[124] Essentially, consent is not required if the child's contact information is collected for the following reasons: to respond to a one-time specific request by a child; to obtain parental consent; or to protect the child's safety.[125]

Additional provisions of the COPPA prohibit a Web site from conditioning a child's participation in a game or receipt of a prize on his or her disclosure of more personal information than is reasonably necessary for the activity.[126] Moreover, the COPPA requires the Web site to establish and maintain reasonable

---

[123] *See id*. § 6501(9).

[124] *See id*. § 6502(b)(1)(D)(2).

[125] *See id*. § 6502(b)(1)(D)(2)(A)-(C). For example, if the only purpose for collecting a child's e-mail is for a one-time response to a request by a child for help with math homework, consent is not necessary. Other examples include mailing online newsletters and electronic postcards.

[126] *Id*. § 6502(b)(1)(C). This restriction is partly in response to results of the FTC's 1998 survey that found Web sites were requiring children to answer questions relating to their interests in order to register or to become eligible to win prizes. June 1998 Report, *supra* note 6, at 33. For example, many Web sites were suggesting that if children provided the salaries of their parents and information about where their parents worked, they would win lots of points. *See* Robert Cannon, *Children's Online Privacy Protection Act*, BOARDWATCH MAG., *at* http://www.board-watch.com/mag/2000/jul/bwm64.html (July 2000) (discussing privacy as an emerging online issue and the COPPA generally).

procedures to protect the confidentiality, security, and integrity of personal information collected about a child.[127]

Finally, the COPPA includes a safe harbor section that bears on the overall effectiveness of the Act.[128] It provides that an operator may satisfy the requirements of the Act by following self-regulatory guidelines, issued by representatives of the marketing or online industries, or by the FTC.[129] This safe harbor section comports with the FTC's emphasis on encouraging self-regulation.[130] The Act directs the FTC to incorporate into its regulations incentives for operators to exercise self-regulatory guidelines that offer children the same protection as under the COPPA.[131] The FTC has the power to determine whether a

---

[127] 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. § 312.8. Specifically, this requires operators to develop policies and procedures to protect children's personal information from "loss, misuse, unauthorized access, or disclosure." Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,906. Recommended procedural safeguards include assigning an individual the responsibility of monitoring the security of the information, storing personal information on a secure server that is not accessible from the Internet, implementing access control procedures that require passwords, limiting employee access to the information, and deleting the information when it is no longer needed. *Id*. at 59,906 nn.284 & 286. The FTC further recommends that Web site operators protect personal information in the possession of those who provide technical support for the internal operations of their sites. *Id*. at 59,890. This could be achieved by incorporating specific contractual provisions that limit the contractors' ability to use the collected information. *Id*.

[128] *See infra* Part III.C (discussing the effect of the safe harbor provision on the COPPA).

[129] *See* 15 U.S.C. § 6503(a).

[130] Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection, emphasized the FTC's encouragement of industry self-regulation: "The COPPA safe harbor provision is an example of the benefits that emerge from successful industry-government partnerships." Press Release, FTC, Entertainment Software Rating Board Awarded "Safe Harbor" Status, *at* http://www.ftc.gov/opa/2001/04/esrb.htm (Apr. 19, 2001).

[131] *See* 15 U.S.C. § 6503(b)(1). The following are illustrative incentives for operators to implement self-regulations:

> (i) Mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;

particular Web site does indeed comply with the requirements of the COPPA.[132] Thus, the COPPA is a comprehensive statute that seeks to ensure the privacy and safety of children who use the Internet.

B. The FTC's Rule

The COPPA directs the FTC to create a rule to implement the Act's requirements.[133] The FTC issued its final rule on November 3, 1999.[134] In drafting the Children's Online Privacy Protection Rule ("the Rule"), the FTC gave serious consideration to the expressed concerns about maintaining children's access to the Internet, perpetuating the interactivity of the Internet, and minimizing the potential burdens of compliance on companies, parents, and children.[135] The FTC believes that the Rule successfully balances these concerns with the COPPA's goal of

---

> (ii) Consumer redress; (iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines; (iv) Referral to the [Federal Trade] Commission of operators who engage in a pattern of practice of violating the guidelines.

Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750, 22,759 (proposed Apr. 27, 1999) (codified at 16 C.F.R. § 312 (2001)).

[132] *See* 15 U.S.C. § 6503(b)(2)-(3) ("The [Federal Trade] Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.").

[133] *Id*. § 6502(b)(1). The FTC has the authority to bring enforcement actions and impose civil penalties for violations under the rules it promulgates. *Id*. § 6503(c). *See infra* note 191 and accompanying text (discussing the FTC's authority under the Federal Trade Commission Act). Additionally, the attorney general of a state may bring a civil action for a violation of the COPPA to enjoin the prohibited conduct, enforce compliance or obtain damages. 15 U.S.C. § 6504(a)(1)(A)-(C).

[134] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)). The FTC received 132 comments, in response to its Notice of Proposed Rulemaking and Request for Public Comment, from a variety of interested parties. *Id*. The comments were used to create the Rule. *Id*.

[135] *Id*. at 59,889.

protecting children's information online.[136]

The first part of the Rule concerns the COPPA's statutory definitions and offers clear guidelines for Web site operators to comply with the statute's requirements.[137] A majority of the terms as defined by the Act remain unchanged, although Congress modified a few terms in response to the FTC's receipt of public comments.[138] The term "collects" personal information, is not explicitly defined by the Act itself. The Rule provides that the term "collect or collection" means the gathering of a child's personal information by any means, including but not limited to the following methods:

> (a) Requesting that children submit personal information online; (b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or (c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.[139]

This clarification enhances the likelihood that businesses will understand the requirements of the Rule and how it applies to them. The terms "child" and "verifiable parental consent" are not changed under the Rule; however, personal information is modified to include screen names that can be associated with

---

[136] *Id*. The FTC continues to work with consumers, parents and the online industry to ensure compliance, to educate the public about online privacy, and to eventually assess the Rule's effectiveness periodically. *Id*. For example, the FTC staff held a public workshop to obtain the public's views on how to obtain verifiable parental consent under the Rule. *Id*. at 59,888.

[137] *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2001).

[138] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,889. For example, the FTC amended the definition of "collects or collection" to clarify that the COPPA only applies to information that children submit online. *Id*.

[139] *See* 16 C.F.R. § 312.2.

individually identifiable information.[140]

In regard to the Rule's definition of Internet, the FTC recognized the dynamic characteristics of technology and the speed at which it is constantly changing and evolving.[141] Therefore, it believes that the definition, as defined in the COPPA as "the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols," prevents the Rule from becoming obsolete by technological advances.[142]

The Rule sets forth guidelines to give proper and effective notice of collection, use, and disclosure practices as required by the Act.[143] Generally, the Rule requires clear and understandable written notice.[144] The operator of a Web site or online service directed to children must post a link[145] on its home page and, wherever information is gathered, must provide a statement of its information practices.[146] The link must be clearly identifiable and prominently placed.[147] Furthermore, the content of the notice

---

[140] *See id*.

[141] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,891.

[142] *See* 16 C.F.R. § 312.2.

[143] *Id*. § 312.4.

[144] *Id*.

[145] A link is an address ("URL") on the World Wide Web to another document on the same server or on any remote server. TechWeb.com, http://www.techweb.com/encyclopedia/defineterm?term=link&x=42&y=6 (last visited Aug. 24, 2001). It is usually displayed using hypertext, which is defined as a linkage between related text. TechWeb.com, http://www.techweb.com/encyclopedia/defineterm.yb?term=hypertext (last visited Aug. 24, 2001). Only text can be used to display a link, in which case the text is underlined, or the link can be represented by an icon of any size or shape. *Id*.

[146] 16 C.F.R. § 312.4(b)(1)(ii) (requiring "clear and prominent" placement of the link to the notice). The FTC suggests that the privacy policy link should incorporate a larger font size, a different color, or a contrasting background to make the link more noticeable. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,894 (elaborating that a link "in small print at the bottom of the home page" is not sufficiently "clear and prominent").

[147] *See* 16 C.F.R. § 312.4(b)(1)(i)-(iii).

must include the contact information of the operator,[148] the types of personal information collected from children,[149] the manner in which such information is used,[150] the disclosure of the information to third parties,[151] and the rights of the parent.[152]

In addition to posting a notice on the Web site, operators must provide direct notice to parents.[153] This notice must include all of the information contained in the Web site's privacy policy, in addition to stating that (i) the operator plans to collect personal information from the child, (ii) the parent's permission is necessary prior to collecting, using, or disclosing the

---

[148] *Id*. § 312.4(b)(2)(i).

[149] This requires disclosure of whether the Web site is collecting information such as a child's name, address, e-mail, or hobbies. The notice must also convey whether the information is collected directly from the child or passively through the use of cookies. *See* FTC, *How to Comply with the Children's Online Privacy Protection Rule*, *at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (Nov. 1999) [hereinafter FTC, *How to Comply*]. For a discussion of the differences between active and passive methods of collection, *see supra* Part I.A.

[150] 16 C.F.R. § 312.4(b)(2)(iii). The operator must identify whether the collection is for marketing back to the child, notifying contest winners, or enabling the child to publicly disseminate the information through chat rooms or bulletin boards. *See* FTC, *How to Comply*, *supra* note 149.

[151] 16 C.F.R. § 312.4(b)(2)(iv). A third party is defined by the Rule as any person who is not an operator in terms of the collection or maintenance of personal information online, or a person who offers support for the internal operations of the Web site or online service and who does not use or disclose such protected information for any other purpose. *Id*. § 312.2. The notice must disclose the kinds of businesses in which a third party is engaged, the general purposes for which the information is used, and whether the third party has agreed to maintain the confidentiality and security of the information. *See* FTC, *How to Comply*, *supra* note 149.

[152] 16 C.F.R. § 312.5(a)(2). The parent has the option to consent to the collection and use of the information while refusing to consent to the dissemination of the personal information to third parties. *Id*. Section 312.5(b) discusses mechanisms by which consent can be obtained. These will be analyzed more fully *infra* Part III.D. Parents also have the right to access and review the child's personal information. *Id*. § 312.4(b)(2)(vi). Finally, parents can request that the information be deleted and can refuse to allow the Web site to continue to collect or use the child's information. *Id*.

[153] *Id*. § 312.4(c); *see also* FTC, *How to Comply*, *supra* note 149.

information, (iii) the parent can provide consent under a prescribed method, and (iv) the parent has the option to agree to the collection of information without disclosure to third parties, the right to review the collected information, and the ability to revoke prior consent.[154] This notice to the parent must be stated clearly and understandably, and cannot contain any unrelated or confusing information.[155]

The Rule preserves the parent's right to review the personal information provided by the child;[156] furthermore, it promulgates detailed guidelines for obtaining parental consent.[157] An operator must obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from the child.[158] A variety of methods can be used to notify a parent, such as sending an e-mail or letter by mail.[159] This includes consent to any material changes in the collection, use, and/or disclosure practices to which the parent has previously consented.[160] This requirement puts parents in control of their child's personal information. Thus, the critical aspects of the Act and the FTC's Rule, including notice and verifiable parental consent, satisfy the FTC's primary goals of increasing parental involvement in

---

[154] 16 C.F.R. § 312.4(c)(1).

[155] *Id*. § 312.4(a).

[156] *Id*. § 312.6.

[157] *Id*. § 312.5.

[158] *Id*. § 312.5.

[159] *Id*. § 312.5(b); *see* also discussion *infra* Part III.D (discussing a variety of methods to obtain verifiable parental consent).

[160] 16 C.F.R. § 312.5(a)(1). The FTC lessened the additional consent requirement to material changes in response to a number of comments to this section. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,898 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)). The commentators raised concerns as to the proposed rule's requirement that operators obtain new consent for any changes to the collection, use, and/or disclosure practices that previously received consent. *Id*. at 59,899. They argued that notification of minor changes would be overly burdensome, especially considering the constant changes that occur regularly in the online industry. *Id*. Thus, the FTC narrowed the Rule to require new parental consent only in the instance of material changes in the operator's collection, use, and/or disclosure practices. *Id*.

children's online activities and protecting children, and their information, on the Internet.[161] The final part of this note discusses various strengths and weaknesses of the COPPA in the attempt to assess the Act's effectiveness.

III. EFFECTIVENESS OF THE COPPA

Because the COPPA is a relatively new effort by Congress and the FTC to protect children online, it is difficult to accurately assess its effectiveness.[162] More time is needed to determine the industry compliance rate, the effect that the FTC's Rule has on enforcement, and finally, the actual protection afforded children's privacy.[163] Meanwhile, at this stage, the COPPA appears to be a valuable step in the right direction of protecting children's online privacy. It offers a uniform legal standard of care that must be adhered to by all Web site operators who collect personal information from children on the Internet.[164] Congress and the

---

[161] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 22,750, 59,908. *See also* 144 CONG. REC. S12741 (Oct. 7, 1998) (statement of Sen. Bryan); June 1998 Report, *supra* note 6.

[162] Recently, however, The Center for Media Education completed a survey of 153 commercial Web sites directed at children to determine whether they were in compliance with the Act. *See* Center for Media Education, *COPPA: The First Year* (Apr. 19, 2001), *available at* http://www.cme.org/children/privacy/ coppa_rept.pdf [hereinafter *COPPA: The First Year*].

[163] As Web sites continue to adapt to the COPPA's requirements, a variety of things would be useful to determine the COPPA's effectiveness and enhance compliance within the children's Internet industry. Possibilities include new studies identifying how children use the Internet and what tools parents want and need to better guide their children online, funding for Internet safety education, developing helplines for troubleshooting, and creating new technologies that enhance Internet safety and privacy online. *See Privacy Protections*, *supra* note 111. Furthermore, a comprehensive study on what information is being collected from children under the age of thirteen, how this information is being used and how children's Web sites are complying with the COPPA's requirements would be quite helpful to the assessment of the statute's overall effectiveness. *See Privacy Protections*, *supra* note 111.

[164] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6502(a)(1),

FTC, by shifting the burden of protection rightfully to the child's parents, emphasize the importance of parental control.[165] While only time will tell how well Web sites are able to comply with the Act, it is likely that the COPPA will be quite useful and effective; as such, the Act will prove a necessary tool for the protection of children's online privacy.[166]

A. Enforcement and the Fair Information Practice Principles

The FTC's most recent survey, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, presented in its May 2000 Report ("the Report"), is useful in analyzing the potential effectiveness of the COPPA.[167] The survey provides a review of the nature and substance of the privacy disclosures of Web sites to assess the effectiveness of self-regulation in protecting online privacy.[168] Because the COPPA is widely premised on the Fair Information Practice Principles used to encourage self-regulation,[169] the FTC survey is a helpful indication of the likelihood that Web sites will comply with the Act.[170]

The May 2000 Report confirms that Web sites collect an extensive amount of personal information.[171] The FTC further concluded that online privacy continues to be threatened, and

---

6505(b)(1)(A)-(D) (Supp. IV 1998).

[165] *Id*. § 6502(b)(1)(A)(i),(ii); 16 C.F.R. § 312.4 (notice to parents); 16 C.F.R. § 312.5 (parental consent).

[166] *See supra* Part II (analyzing the requirements of the Act and the FTC's Rule).

[167] *See generally* May 2000 Report, *supra* note 20 (analyzing the current state of online privacy and the efficacy of industry self-regulation).

[168] May 2000 Report, *supra* note 20, at 7.

[169] *See supra* note 109 and accompanying text (discussing the core information principles of Notice, Choice, Access, Security, and Enforcement).

[170] May 2000 Report, *supra* note 20, at 3-5 (describing the same Fair Information Practice Principles upon which the COPPA is based).

[171] May 2000 Report, *supra* note 20, at 1. *See supra* note 34 and accompanying text (providing statistics on the widespread collection of personal information).

self-regulatory industry efforts alone are insufficient.[172] The FTC greatly encourages self-regulation because it is the least intrusive and most flexible means to ensure that, given the ever-changing nature of the Internet and computer technology, fair information practices are followed, [173] Furthermore, the industry is the best cost avoider,[174] and its participants have the greatest knowledge and skill to design appropriate standards cheaply and effectively.[175]

Despite the FTC's preference for industry self-regulation, the Report indicates that more regulation is required, since only 20% of Web sites implement, at least in part, the Fair Information Practice Principles.[176] While the Report does not directly consider children's privacy concerns, its conclusion that congressional enforcement, in conjunction with self-regulation, is necessary to ensure adequate protection of online privacy[177] indicates that the enactment of the COPPA is necessary to protect children online. This is because the COPPA does not enable industry alone to affect privacy standards.[178]

It is clear from its language that the COPPA imports the long established Fair Information Practice Principles.[179] The benefit of

---

[172] May 2000 Report, *supra* note 20, at 9, 35 (stating that "[b]ecause self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders").

[173] July 1999 Report, *supra* note 52, at 6. *See also* Angela J. Campbell, *Self-Regulation and the Media,* 51 FED. COMM. L.J. 711, 743 (1999) (discussing the advantages and disadvantages of self-regulation).

[174] Campbell, *supra* note 173, at 756.

[175] Campbell, *supra* note 173, at 715.

[176] May 2000 Report, *supra* note 20, at 12-13. The Survey shows that 41% of the Random Sample of Web sites meet the basic Notice and Choice standards. May 2000 Report, *supra* note 20, at 13.

[177] May 2000 Report, *supra* note 20, at 36-38.

[178] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.9 (2001) (violating the COPPA is actionable by the FTC); *id*. § 312.10(a) (providing that if an operator complies with certain self-regulatory guidelines, the operator may qualify for the safe harbor).

[179] The Notice Principle is implemented by the statutory requirement that

the Act is that it adapts the core principles[180] to afford even greater privacy protection for children.[181] Additionally, notice to parents is an especially crucial principle when the passive data collection method is employed. Notice, combined with the Choice Principle, achieves transparency[182] when users are unaware that information is being collected from them.[183] Notice and Choice thereby allow children's parents to make informed decisions about whether to permit the collection of their child's

---

Web sites provide notice about the information collected, the method of collection and the sites' disclosure practices for such information. *See* 15 U.S.C. § 6502(b)(1)(A)(i). Obtaining verifiable parental consent provides parents with options about how their children's personal information may be used (Choice Principle). *See id*. § 6502(b)(1)(A)(ii). Parents are afforded access to their children's information and have the ability to review the information or refuse to permit the operator to continue using their children's information (Access Principle). *See id*. § 6502(b)(1)(B)(i)-(iii). The Security Principle is supported by requiring the operator to maintain reasonable procedures to protect the integrity of the personal information that it collects from children. *See id*. § 6502(b)(1)(D). Finally, the Enforcement Principle is implemented through the FTC's ability to bring suit for a violation of the Rule. *See id*. § 6502(c). For a discussion on the FTC's authority to bring an action against a Web site, *see infra* note 191 and accompanying text.

[180] *See supra* note 109 and accompanying text (identifying that notice, choice, access, security, and enforcement are crucial to ensuring privacy online).

[181] While the Fair Information Practice Principles do not directly address personal information collected from children, they are applicable to parents. *See, e.g.*, 15 U.S.C. § 6502(b)(1)(A)(i) (requiring notice to parents). The principles set out the responsibilities of Web site operators who collect personal information from children and provide rights to the parents who can further protect their children's security online. *See* Landesberg & Mazzarella, *supra* note 14.

[182] Transparency is "the maintenance of processing systems that are understandable to the concerned individual." Schwartz, *Beyond Lessig's Code*, *supra* note 28, at 780. In other words, when a Web site clearly informs a parent about what and how information is collected regarding the parent's child, and the parent has the ability to make an informed decision whether to allow the site to collect such information, transparency is achieved. *See* Online Profiling Report, *supra* note 25 (discussing transparency with regard to the Notice Principle).

[183] *See* Online Profiling Report, *supra* note 25.

information by knowing what information is being collected and how it will be used.[184] Finally, access to the children's information that is collected goes beyond simply posting a privacy policy on a Web site.[185] The paternalistic nature of the COPPA is quite appropriate since the legislation was enacted specifically for the protection of children, who are accordingly unable to protect themselves.[186]

While the theories behind the Fair Information Practice Principles are valuable, their implementation, especially in terms of children's Web sites' privacy policies, has not proven to be successful.[187] In a report entitled *Privacy Policies on Children's Websites: Do They Play By The Rules?*, the Annenberg Public Policy Center of the University of Pennsylvania concluded that the privacy policies are often "too unclear and time-consuming to realistically encourage parents to confidently guide their children's Internet experiences."[188] The industry must improve its

---

[184] *See* June 1998 Report, *supra* note 6, at 7-9.

[185] Landesberg & Mazzarella, *supra* note 14 (confirming that the COPPA successfully incorporates the Access Principle since parents have the right to review the records of the information collected about their children and to request that certain information be deleted). *See also* Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(B)(i),(ii) (Supp. IV 1998).

[186] June 1998 Report, *supra* note 6, at 4-5.

[187] Joseph Turow, The Annenberg Public Policy Center*, Privacy Policies on Children's Websites: Do They Play by the Rules?* (Mar. 28, 2001), *available at* http://www.appcpenn.org/internet/family/privacyreport.pdf.

[188] *Id*. Out of 162 children's Web sites that were studied, seventeen collected personal information but failed to have a privacy policy link on their home pages. *Id*. at 10. Furthermore, only 62% of the Web sites informed parents of their right to review their children's information, 51% told parents of their right to prevent any further collection of their children's information, and 55% of the sites notified parents of the COPPA's requirement that a site collects only information that is reasonably necessary for a child to use the site. *Id*. at 16. The report made two recommendations to increase the effectiveness of the COPPA: (1) all sites subject to the COPPA should place the same symbol ("K" for kids) on their home page in a specific location; and (2) children's Web sites should work together to create a standard privacy policy that incorporates the required privacy information, and is presented in a quick and straightforward fashion. *See id*. at 21. The idea that every Web site displays a "K" would enable parents to tell their children to interact only with

compliance with the COPPA and the Fair Information Practice Principles, for example, by creating clear and informative privacy policies.[189] Meanwhile, the FTC is taking initiative to enforce children's privacy rights through litigation.

---

sites that display that symbol. *Id*. This suggestion should be adopted by the FTC because it would help parents direct their children to COPPA compliant sites. *Id*. As a result, children's personal information disclosed on the Internet would be more secure. *See id*. The report's second recommendation of a model privacy policy, however, is less likely to be successful and may even create more risks. While it would be very efficient for parents if all children's Web sites had standardized privacy policies relaying the required information, it could also create many dangers. For example, after a parent reads a few identical policies, they could easily be misled that the next policy they read has the same information, when in fact that policy discloses different information practices. Furthermore, various Web sites often have different information practices that would make it difficult to develop one model policy for all sites to adopt.

[189] *See COPPA: The First Year*, *supra* note 162, at 10. This report agreed with the findings of The Annenberg Public Policy Center with regard to privacy policies. The CME's report, however, found that in many cases, only minor adjustments would be necessary to bring the Web sites into compliance with the Act. *COPPA: The First Year*, *supra* note 162, at 10. The report found that while a majority of the Web sites did not maintain a clear and prominent link to their privacy policy on the home page, a majority of the sites did comply with the COPPA in a number of other ways. *COPPA: The First Year*, *supra* note 162, at 10. First, seventy-two out of 100 sites (72%) "placed a link to their privacy policy on every page where data collection took place." *COPPA: The First Year*, *supra* note 162, at 10. Second, a majority of sites limit their information collection practices to take advantage of the sliding scale provision. *COPPA: The First Year*, *supra* note 162, at 7. *See infra* Part III.D (describing the sliding scale approach that offers Web site operators a simple method of obtaining parental consent). Another way that Web sites are complying with the COPPA is by providing informative privacy policies. *COPPA: The First Year*, *supra* note 162, at 8. The survey found that 76.3% of the sites "that collected personally identifiable information from children posted a privacy policy in 2001." *COPPA: The First Year*, *supra* note 162, at 8. This is clearly a great improvement from the mere 14% of Web sites that disclosed their information practices in 1998. *See supra* note 39 (describing the FTC's findings in 1998). Thus, simply by redesigning the privacy policy link on the Web sites' home pages to be more obvious, the compliance rate with the COPPA would increase. *COPPA: The First Year*, *supra* note 162, at 10.

B. Enforcement of the COPPA in the Courts

The COPPA's main advantage is that it is a legislative means to protect children's privacy rights.[190] The Act provides the FTC, as the implementing agency, with the authority to take direct action to enforce the statute's requirements.[191] Less than two years after the COPPA was enacted, the FTC took enforcement action. On July 10, 2000, the FTC filed a complaint against Toysmart.com, an Internet toy retailer,[192] in the District of Massachusetts, seeking injunctive and declaratory relief to prevent the sale of personal customer information collected on the Web site, in violation of the company's privacy policy.[193]

---

[190] The Center for Media Education concluded that a regulatory framework is needed to protect children online because efforts by children's parents and industry self-regulation are insufficient. *Web of Deception*, *supra* note 46, at 19.

[191] 15 U.S.C. § 6505(a), (d); Children's Online Privacy Protection Rule, 16 C.F.R. § 312.9 (2001). Pursuant to the Federal Trade Commission Act, the FTC has the authority to take action against organizations, with some exceptions, that engage in "unfair or deceptive acts or practices in or affecting commerce" and to commence civil actions to recover penalties of up to $10,000 per violation. Federal Trade Commission Act, 15 U.S.C. § 45 (1994). There is no private right of action for a violation of the FTC Act. However, state attorney generals have authority under the Act to enforce compliance with the FTC's Rule by filing actions in federal court after first serving written notice upon the FTC. 15 U.S.C. § 6504.

[192] Toysmart.com is no longer in business as a result of bankruptcy. Greg Sandoval & Jeff Palline, *Toysmart Shutting Down*, CNET NEWS.COM, *available at* http://news.cnet.com/news/0-1007-200-1920890.html (May 22, 2000). The company was forced to cease operations as a result of increased competition and a declining market. *Id*.

[193] Complaint, FTC v. Toysmart.com, LLC, No. 002-3274 (D. Mass. July 10, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcmp.htm [hereinafter Toysmart Complaint]. The FTC became aware of Toysmart.com's unlawful behavior when the company advertised for a buyer of its assets, including its customer lists. *See* Eliot Spitzer, *An Analysis of Recent Privacy Issues by the Attorney General of the State of New York*, 632A PLI/PAT 231 (2001).. The company collected personal information of approximately 250,000 consumers from the time they began operations. Jerry Guidera & Frank Byrt, *Judge Refuses to Set Conditions on Toysmart Sale*, WALL ST. J., Aug. 18, 2000, at B6, *available at* 2000 WL-WSJ 3040641. Toysmart.com

Toysmart.com collected personal information from customers, including names, addresses, billing information, shopping preferences, and family profiles.[194] This information was compiled into detailed customer lists.[195] Toysmart.com's privacy policy on its Web site assured customers that their information would not be shared with third parties.[196] The FTC claimed that Toysmart.com, a company in bankruptcy, violated section 5 of the FTC Act by falsely promising consumers that their personal information would not be disseminated to third parties, and then selling its customer lists as part of the disposition of assets in bankruptcy.[197] Toysmart.com later informed the FTC that it would not sell its customer lists to a third party without bankruptcy court approval.[198]

On July 21, 2000, the FTC filed an amended complaint, which stated its first claim under the COPPA.[199] Toysmart.com sold educational and non-violent children's toys over the Internet and collected personal information from children through a

---

placed advertisements for a buyer in the *Boston Globe* and the *Wall Street Journal*. *See* Eliot Spitzer, *An Analysis of Recent Privacy Issues by the Attorney General of the State of New York*, 632A PLI/PAT 231 (2001).

[194] Toysmart Complaint, *supra* note 193.

[195] Toysmart Complaint, *supra* note 193.

[196] Toysmart Complaint, *supra* note 193. The privacy policy stated that "[p]ersonal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by Toysmart.com is used only to personalize your experience online." Toysmart Complaint, *supra* note 193. The policy continued to explain that "[w]hen you register with toysmart.com, you can rest assured that your information will never be shared with a third party." Toysmart Complaint, *supra* note 193. *See also* Press Release, FTC, FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors, *available at* http://www.ftc.gov/opa /2000/07/ toysmart.htm (July 10, 2000).

[197] Toysmart Complaint, *supra* note 193.

[198] Toysmart Complaint, *supra* note 193.

[199] First Amended Complaint, FTC v. Toysmart.com, LLC, No. 00-1341 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/ toysmartcomplaint.htm.

dinosaur trivia contest.[200] Specifically, the complaint alleged that the Web site collected children's personal information, including names, e-mail addresses, and ages of children under thirteen, without notifying the children's parents or obtaining parental consent.[201]

On the same day that the FTC filed its first amended complaint, the parties entered into a settlement agreement.[202] The settlement agreement provided that Toysmart.com could only assign or sell its customer information as part of the sale of its goodwill and only to a qualified buyer approved by the bankruptcy court.[203] The FTC's Stipulated Consent Agreement and Order ("Consent Agreement") enjoined Toysmart.com from making any false or misleading representations about the disclosure of customer information to third parties, and prevented Toysmart.com from disclosing, selling, or offering for sale, any customer information to any third party, except as provided for by the bankruptcy court.[204] Additionally, the Consent Agreement required Toysmart.com to delete or destroy all information

---

[200] *See id*. ¶¶ 6, 14.

[201] *See id*. ¶¶ 15, 19.

[202] *See* Stipulation and Order Establishing Conditions on Sale of Customer Information, *In re* Toysmart.com, LLC, No. 00-13995 (Bankr. D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartbankruptcy.1.htm [hereinafter Toysmart Stipulation & Order]. Toysmart.com filed a motion with the bankruptcy court to approve this stipulation with the FTC and for authority to enter into a consent agreement. *See* Spitzer, *supra* note 193. Approval of this agreement would have resolved the FTC's pending complaint in the District of Massachusetts. *Id*. at 293. *See also supra* notes 193, 199 (identifying the FTC's Complaint and First Amended Complaint).

[203] Toysmart Stipulation & Order, *supra* note 202. A qualified buyer was defined as "an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, including commerce, content, product and services, and (2) expressly agrees to be Toysmart's successor-in-interest as to the Customer Information," and expressly agrees to comply with the terms of the order. Toysmart Stipulation & Order, *supra* note 202.

[204] *See* Stipulated Consent Agreement and Final Order, FTC v. Toysmart.com, LLC, No. 00-11341 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartconsent.htm.

collected from children in violation of the COPPA.[205] The bankruptcy court, however, denied Toysmart.com's motion to approve the Consent Agreement.[206] In January 2001, a settlement was finally reached in the bankruptcy court whereby the Walt Disney Company paid Toysmart.com $50,000 to destroy the information.[207] Thus, the FTC successfully prevented the sale of children's personal information to unqualified third parties. This is the first illustration of how the privacy of children's information can be ensured through enforcement of the Act.[208]

Less than one year after the action against Toysmart.com, the FTC filed complaints against three Web site operators for violations of the COPPA.[209] The operators of the Web sites

---

[205] *See id*.; *see also* Toysmart Complaint, *supra* note 193.

[206] Spitzer, *supra* note 193 (denying approval because the Consent Agreement failed to fully protect the consumer's privacy interests and did not offer adequate notice and consent).

[207] *Id*. at 299. A subsidiary of the Walt Disney Co., Buena Vista Internet Group, was a majority owner of Toysmart.com. *Disney Unit Offering $50,000 to Toysmart to Kill Customer List*, WALL ST. J., Jan. 9, 2001, at B2, *available at* 2001 WL-WSJ 2850403. They were willing to pay $50,000 to buy and then destroy the customer list to prevent its sale to another company. *Id*.

[208] Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection stated, "this settlement shows that the FTC is serious about enforcing the Children's Online Privacy Protection Act . . . [this] is only the start of our efforts to ensure the Web sites . . . comply with the parental notification requirements of the law." Press Release, FTC, FTC Announces Settlement With Bankrupt Web site, Toysmart.com, Regarding Alleged Privacy Policy Violations, *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (July 21, 2000). However, a recent article stated that compliance with the COPPA has been very poor. *See* DiSabatino, *supra* note 52. A report that focused on how well Web sites have complied with the COPPA examined 162 Web sites with the highest percentage of child visitors under the age of thirteen. DiSabatino, *supra* note 52. The results showed the Web sites did not often comply with the law. DiSabatino, *supra* note 52. Privacy policies posed the biggest problems for these sites; they were often unclear, or the Web site failed to provide a link to the privacy policy from its home page. DiSabatino, *supra* note 52. This made it difficult for parents to access the privacy policies. DiSabatino, *supra* note 52.

[209] Complaint, United States v. Monarch Serv., Inc. and Girls' Life, Inc., No. 01 CV 1165 (D. Md. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/girlslifecmp.pdf [hereinafter Girls' Life Complaint]; Complaint,

Girlslife.com,[210] Bigmailbox.com,[211] and Insidetheweb.com[212]

United States v. Bigmailbox.com, Inc., No. 01-605-A (D. Va. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/ bigmailboxcmp.pdf [hereinafter Bigmailbox Complaint]; Complaint, United States v. Looksmart Ltd., No. 01-606-A (D. Va. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/looksmartcmp.pdf [hereinafter Looksmart Complaint].

On August 15, 2001, the Electronic Privacy Information Center ("EPIC") and others filed an amended complaint before the FTC requesting that the FTC investigate Microsoft's allegedly unfair and deceptive practices related to information collection online and enjoin Microsoft from violating the COPPA. Complaint, *In re* Microsoft Corp., *at* http://www.epic.org/privacy/consumers/ S_complaint.pdf (July 26, 2001). One of the allegations in the complaint involved Microsoft's Kids Passport system. *Id*. at 7. Kids Passport enables Microsoft to collect personal information from children that will subsequently be disclosed to Microsoft partners and other online entities. *Id*. at 12. The complainants allege that Kids Passport fails to comply with the COPPA because the system requires parents to read the privacy policies of each and every Web site that they give consent for their children to use, rather than providing one comprehensive privacy notice as required. Amended Complaint, *In re* Microsoft Corp., *at* http://www.epic.org/privacy/consumers/MS_ complaint2.pdf (Aug. 15, 2001); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(b) (2001). Other alleged violations include failing to provide a clear and prominent link to Microsoft's privacy policy on the Kids Passport site and collecting unnecessary personally identifiable information from children. *Id*. at 8-10. FTC officials will not confirm whether the agency will commence a formal investigation. *See* Brian Krebs, *Groups Ask FTC to Probe Microsoft Passport, XP Features*, NEWSBYTES NEWS NETWORK, Aug. 15, 2001, *available at* 2001 WL 23417425.

[210] Monarch Services, Inc. and Girls' Life, Inc., operate www.girlslife.com, which targets girls between the ages of nine and fourteen, offering online articles, advice columns, contests, bulletin boards, e-mail accounts and a variety of products. *See* Girls' Life Complaint, *supra* note 209, at 5; Press Release, FTC, FTC Announces Settlements with Web Sites that Collected Children's Personal Data Without Parental Permission, *at* http:// www.ftc.gov/opa/2001/04/girlslife.htm (Apr. 19, 2001).

[211] Bigmailbox and Nolan Quan operate www.bigmailbox.com, which sends advertising and direct marketing materials to the site's e-mail account holders. *See* Bigmailbox Complaint, *supra* note 209, at 5.

[212] Looksmart.com, Ltd. is the operator of www.insidetheweb.com, and offers a free online message board service through the site. *See* Looksmart Complaint, *supra* note 209, at 6.

collected and used personally identifiable information from children under the age of thirteen.[213] The three Web site operators were charged with the following violations of the COPPA: (a) failing to provide sufficient notice on the Web site, or to parents, about their information collection, use, and disclosure practices;[214] (b) failing to obtain verifiable parental consent before collecting, using, and disclosing children's personal information;[215] (c) failing to provide reasonable means for children's parents to review the personal information and to refuse the continued use and maintenance of the information;[216] and (d) conditioning children's participation in an online activity on their disclosing more personally identifiable information than reasonably necessary to participate in such activity.[217]

Settlement agreements were reached in all three cases. As part of each settlement, the sites are required to delete all personal information collected from children since April 21,

---

[213] *See* Press Release, FTC, FTC Announces Settlements with Web Sites that Collected Children's Personal Data Without Parental Permission, *at* http://www.ftc.gov/opa/2001/04/girlslife.htm (Apr. 19, 2001).

[214] *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(c) (2001); Girls' Life Complaint, *supra* note 209, at 9; Bigmailbox Complaint, *supra* note 209, at 9; Looksmart Complaint, *supra* note 209, at 7-8. Children who registered at these sites were asked to provide information including their name, address, e-mail address, username, password, gender, age, their system software, and their browser. *See* Girls' Life Complaint, *supra* note 209, at 5-6; Bigmailbox Complaint, *supra* note 209, at 6; Looksmart Complaint, *supra* note 209, at 6. Bigmailbox's Web site used children's e-mail addresses to send them advertising and direct marketing materials. *See* Bigmailbox Complaint, *supra* note 209, at 7. Furthermore, Bigmailbox disclosed the children's personal information to third parties. Bigmailbox Complaint, *supra* note 209, at 7.

[215] *See* 16 C.F.R. § 312.5(a)(1); Girls' Life Complaint, *supra* note 209, at 9; Bigmailbox Complaint, *supra* note 209, at 9; Looksmart Complaint, *supra* note 209, at 8.

[216] *See* 16 C.F.R. § 312.6(a); Girls' Life Complaint, *supra* note 209, at 9-10; Bigmailbox Complaint, *supra* note 209, at 9; Looksmart Complaint, *supra* note 209, at 8.

[217] *See* 16 C.F.R. § 312.7; Girls' Life Complaint, *supra* note 209, at 10; Bigmailbox Complaint, *supra* note 209, at 9; Looksmart Complaint, *supra* note 209, at 7.

2000, the date the COPPA became effective.[218] The Web sites must also post a privacy policy that complies with the COPPA.[219] In particular, they must clearly, understandably, and completely disclose the information collection, use, and disclosure practices of the Web sites.[220] The FTC also required that the sites post a link to the FTC site at www.ftc.gov/kidzprivacy, which provides useful information to consumers about the COPPA.[221] Girls' Life was required to pay a civil penalty of $30,000.[222] Bigmailbox and Looksmart were each required to pay civil penalties of $35,000.[223] These settlements mark the first civil penalty cases the FTC has brought under the COPPA. Thus, the FTC has

---

[218] *See* Consent Decree and Order, United States v. Monarch Serv., Inc., No. 01 CV 1165 (D. Md. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/girlslifeorder.pdf. [hereinafter Girls' Life Order]; Consent Decree and Order, United States v. Bigmailbox, Inc., No. 01-605-A (D. Va. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/bigmailbox-order.pdf [hereinafter Bigmailbox Order]; Consent Decree and Order, United States v. Looksmart Ltd., No. 01-606-A (D. Va. Apr. 19, 2001), *available at* http://www.ftc.gov/os/2001/04/looksmartorder.pdf [hereinafter Looksmart Order].

[219] Girls' Life Order, *supra* note 218, at 3; Bigmailbox Order, *supra* note 218, at 4; Looksmart Order, *supra* note 218, at 3.

[220] Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(A)(i) (Supp. IV 1998); 16 C.F.R. § 312.4.

[221] Girls' Life Order, *supra* note 218, at 3; Bigmailbox Order, *supra* note 218, at 4; Looksmart Order, *supra* note 218, at 3.

[222] Girls' Life Order, *supra* note 218, at 4.

[223] Bigmailbox Order, *supra* note 218, at 4; Looksmart Order, *supra* note 218, at 4. Not only are all three defendants required to pay substantial civil damages, but they are also under strict scrutiny by the FTC for five years. Girls' Life Order, *supra* note 218, at 7; Bigmailbox Order, *supra* note 218, at 8; Looksmart Order, *supra* note 218, at 7. During this period, they must make available to the FTC, upon request, a print or electronic copy of all documents demonstrating compliance with the COPPA. Girls' Life Order, *supra* note 218, at 7; Bigmailbox Order, *supra* note 218, at 8; Looksmart Order, *supra* note 218, at 7. These documents include a sample copy of every different information collection form, Web page or screen, and a sample copy of every different disclosure that the defendants make regarding their collection, use, and disclosure practices concerning personal information. *See* Girls' Life Order, *supra* note 218, at 7; Bigmailbox Order, *supra* note 218, at 8; Looksmart Order, *supra* note 218, at 7.

shown its ability to protect children through the earnest enforcement of the law.[224]

C. The Safe Harbor[225]

Enforcement is paramount to any effective self-regulatory or legislative effort. The ability of the FTC to enforce the COPPA is critical to its success. Based on the FTC's recent negative assessment of the effectiveness of industry self-regulation,[226] it is not surprising that the success of the safe harbor provision of the COPPA has been met with skepticism.[227] Under the Rule, a Web

---

[224] *But see* Zavaletta, *supra* note 116, at 272 (concluding that "the COPPA only requires children to get a permission slip for a field trip on the information highway"). The article asserts that the COPPA merely protects Web site operators from liability, rather than children. Zavaletta, *supra* note 116, at 272. However, the author does not place sufficient emphasis on the fact that the COPPA provides the first legal standard of care for the online collection of personal information from children. *See* Zavaletta, *supra* note 116, at 271. Since the COPPA is the first comprehensive statute that addresses children's online privacy, it is a useful and necessary legislative tool. While the COPPA may not be flawless, partly due to the inherent anonymity of the Internet, it prevents Web site operators from freely exploiting children online. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.7 (2001) (preventing Web site operators from conditioning a child's participation in an online activity on providing more personal information than is reasonably necessary); *id*. § 312.8 (requiring the Web site operator "to protect the confidentiality, security, and integrity" of children's information).

[225] A safe harbor is defined as (1) "[a]n area or means of protection;" and (2) "[a] provision (as in a statute or regulation) that affords protection from liability or penalty." BLACK'S LAW DICTIONARY 1336 (7th ed. 1999).

[226] May 2000 Report, *supra* note 20.

[227] David McGuire, *Privacy Advocate Applauds Kids Privacy Safe Harbor*, NEWBYTES, *at* http://www. newsbytes.com (Feb. 2, 2001) (claiming consumer advocates criticize general safe harbor provisions as "backdoor loopholes that allow companies to avoid abiding by the law"). A general criticism against safe harbor provisions is that they "severely weaken" any act employing them. Jenab, *supra* note 75, at 648. Opponents to safe harbor provisions express the following sentiment:

> [Safe harbor provisions] undermine the essential purpose of the legislation, which is to provide a uniform environment in which consumers and market entities may contract for rights around a

site's compliance with an FTC approved self-regulatory guideline will serve as a safe harbor in any enforcement action for violations of the Rule.[228] For approval, the applicant's guidelines must implement requirements substantially similar to those set forth by the Rule itself,[229] provide an effective, mandatory mechanism for the independent assessment of compliance with the guidelines,[230] and contain effective incentives for compliance.[231] The assessment requirement is satisfied by periodic reviews on a regular and random basis, either by the industry group that sets forth the guidelines or by some independent entity.[232] This last requirement helps balance

> default rule protecting privacy; i.e., one in which a consumer may be reasonably confident that she understands what is going to happen to her data once she releases it.

Jenab, *supra* note 75, at 670. *See also* Campbell, *supra* note 173, at 743 (arguing that the threat of governmental regulation and the lack of government oversight are insufficient to overcome the obstacles of effective self-regulation to protect consumer Internet privacy). Despite the skepticism, the safe harbor provision of the COPPA is a "useful model" of self-regulation as an adjunct to government regulation. Campbell, *supra* note 173, at 771.

[228] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,906 (Nov. 3, 1999) (codified at 16 C.F.R. § 12 (2001)). The guidelines may be issued by members of the marketing or online industries, or by other people that the FTC approves. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.10(a) (2001). As of May 23, 2001, the FTC approved three safe harbor applications. Press Release, FTC, TRUSTe Earns "Safe Harbor" Status, *at* http://www.ftc.gov/opa/2001/05/truste.htm (May 23, 2001). These include the Children's Advertising Review Unit of the Council of Better Business Bureaus ("CARU"), the Entertainment Software Rating Board ("ESRB"), and TRUSTe, an Internet privacy seal program. *Id*.

[229] *See* 16 C.F.R. § 312.10(b)(1).

[230] *Id*. § 312.10(b)(2).

[231] *Id*. § 312.10(b)(3).

[232] *Id*. § 312.10(b)(2)(i)-(ii). Seal programs may qualify to meet this requirement. *See id*. § 312.10(b)(4). Seal programs require the Web sites that register with them to comply with certain codes of online information practices and to submit various types of compliance monitoring schemes in order to display a privacy seal on their sites. July 1999 Report, *supra* note 52, at 9. Seal programs, such as TRUSTe and BBBOnline, provide an easy method for consumers to identify Web sites that adhere to information practice principles. July 1999 Report, *supra* note 52, at 9. However, the seal programs have failed

concerns of relaxed enforcement because the safe harbor provision does not simply surrender enforcement to the efficacy of self-regulation.[233] Instead, it incorporates a review mechanism by an independent entity.[234] The independent review avoids relegating authority right back to the industry itself, where the harmful practices originated.

The safe harbor provision of the COPPA does not allow Web site operators to rely on self-assessment mechanisms alone to comply with the Rule's requirements.[235] The COPPA recognizes that self-assessment, without more, is not enough to measure a Web site's compliance with industry guidelines.[236] The Act maintains enforcement procedures by requiring independent, outside monitoring.[237] Furthermore, the safe harbor approach allows for flexibility, and takes advantage of the industry's superior knowledge by allowing the industry participants to

---

to establish a significant presence on the Internet. May 2000 Report, *supra* note 20, at 6. *See* July 1999 Report, *supra* note 52, at 9-12 (discussing the seal programs in detail).

[233] Campbell, *supra* note 173. Opponents of self-regulation criticize that companies will use their superior knowledge to maximize the industry's profits, rather than to benefit the public. *See* Campbell, *supra* note 173, at 717. Another concern is that self-regulatory groups will be more susceptible to industry pressures than the government. Campbell, *supra* note 173, at 717-18. However, the safe harbor provision has additional safeguards to alleviate such concerns. *See, e.g.*, 16 C.F.R. § 312.10 (providing for independent assessment of compliance).

[234] 16 C.F.R. § 312.10.

[235] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,907 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)).

[236] *Id*.

[237] The FTC believes that the independent assessment is the best and most reliable way to ensure compliance. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,907. *See supra* note 232 (describing the use of seal programs such as TRUSTe and BBBOnline). Other resources are available to Web site operators to gain assistance in complying with the COPPA. For example, one law firm, Aftab & Savit, offers services to help Internet companies meet the requirements of the COPPA. Clients are charged a $10,000 flat fee to audit their child-privacy practices. Julia Angwin, *COPPA Cost Too High for Some Sites*, ZDNET NEWS, *at* http://www.zdnet.com/zdnn/stories/ news/0,4584,2554411,00.html (Apr. 24, 2000).

remain actively involved and have the opportunity to make suggestions and changes.[238] Thus, while self-regulation rarely proves to be effective, the application of the COPPA corrects a failure inherent in self-regulatory schemes by including independent review procedures in the safe harbor provision.[239]

D. Compliance and Burden on Businesses

The enactment of the COPPA has received overwhelming complaints from industry participants that compliance is too complicated and burdensome.[240] While several children's Web site companies have announced their compliance,[241] others have decided that it is too difficult to obtain verifiable parental consent for all of the children who use their sites.[242] Companies,

---

[238] Campbell, *supra* note 173, at 771.

[239] *See* 16 C.F.R. § 312.10.

[240] *See* Burke, *supra* note 5.

[241] Burke, *supra* note 5. Companies that have announced their compliance include Headbone.com, Surfmonkey.com, and Agirlsworld.com. Burke, *supra* note 5. Other Web sites that have been described as "responsible" sites for children include, MaMaMedia.com, Hasbro-Interactive.com, ChevronCars.com, and Lunchables.com. *See* DiSabatino, *supra* note 52. Furthermore, the financial impact of adding consent verification for larger companies, such as America Online and Microsoft, is negligible. Angwin, *supra* note 237.

[242] Many startup Internet sites have explained that compliance is simply too costly and that it would be easier not to register children at all. Burke, *supra* note 5. For example, the Web site for the popular children's show "Thomas the Tank Engine" suspended its e-mail bulletin operations as a result of the COPPA. Declan McCullagh, *COPPA Lets Steam Out of Thomas*, WIRED NEWS, *at* http://www. wired.com/news/politics/0,1283,36325,00.html (May 13, 2000). Instead of refusing to register children altogether, eCrush.com simply eliminated accounts of children who were under thirteen, and other sites turned into sites for teenagers, thereby placing the sites beyond the statute's scope. *See* DiSabatino, *supra* note 52. Moreover, FreeZone.com estimated a cost of $100,000 to comply with the Act. Angwin, *supra* note 237. Critics of the COPPA argue that the Internet will not be a resource for kids because of the difficulty many Web sites have in complying with the Act. *See* DiSabatino, *supra* note 52. Supporters of the COPPA agree that the Act plays a role in the problems that children's Web sites are facing, but they place

however, have an exaggerated idea of what is actually necessary to bring their sites into compliance with the COPPA.[243] The FTC's Rule explains the various mechanisms for obtaining verifiable parental consent.[244] Possibilities include a consent form signed by a parent and returned by mail or facsimile ("print-and-send"), credit card verification, a toll-free telephone number staffed by trained personnel, digital certificates that use public key technology, or e-mail verification accompanied by a PIN or password.[245]

A primary concern of Web site operators is the ease and likelihood that a child will deceive the Web site into thinking that he or she is actually a parent.[246] The anonymity of the Internet increases the likelihood that a child will simply pretend to be a parent, thereby effectively bypassing the consent requirement.[247]

---

greater blame on parents' apathy and the FTC's restricted ability to administer the COPPA. *Privacy Protections*, *supra* note 111.

[243] *See* Burke, *supra* note 5 (discussing the compliance difficulties many Web sites are facing by the enactment of the COPPA). Surfmonkey.com established an 800 number so that parents can confirm that their children have permission to engage in the Web site's chat rooms and bulletin boards. *See* Angwin, *supra* note 237. Furthermore, Yahoo! created Family Account registration, specifically designed to prevent underage children from accessing certain services without first obtaining parental consent. When a child under the age of thirteen registers for a Yahoo! account, a parent must create a family account, which can only be achieved by providing a valid credit card number and expiration date. *See* Patricia Fusco, *Web Sites Coping with COPPA*, INTERNET.COM, *at* http://www.internetnews.com/bus-news/article/03_345401,00.html (Apr. 21, 2000).

[244] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2001). Nonetheless, one Web site, Bonus.com, reported serious lassitude on the parent's part. *See Privacy Protections*, *supra* note 111. In the Web site's attempt to gain consent from parents to use children's information for internal purposes, 51% never replied. *Privacy Protections*, *supra* note 111. Thirty-one percent did provide consent, however, and only 5% refused (13% are still pending responses). *Privacy Protections*, *supra* note 111.

[245] 16 C.F.R. § 312.5.

[246] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,910 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2001)); *see also Teenage Life Online*, *supra* note 4, at 4.

[247] The likelihood that a child will pretend to be his or her parent in order

Other concerns involve the suggested mechanisms for obtaining consent, which impose additional compliance problems.[248] Where a Web site opts for credit card verification as a means to assure parental consent, nothing stops a child from simply taking his or her parents' credit card to deceive the Web site operator. Furthermore, not every parent has a credit card, and those who do are not necessarily comfortable using one online.[249] Operators who choose to use a toll free number mechanism are faced with the burden of hiring trained staff that can differentiate between children and adult callers.[250] This can be quite costly.[251] Finally, e-mail alone is likely to be ineffective because it is easily susceptible to circumvention by children.[252]

The FTC recognizes these problems and their potential costs

---

to access a site is supported by a recent study which found that 15% of the children surveyed lied about their age to gain access to a Web site. *Teenage Life Online*, *supra* note 4, at 4.

[248] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,909 (Nov. 3, 1999) (codified at 16 C.F.R. § 312.5 (2001)). On the other hand, children's Web sites might actually be more successful if they have the Support of the children's parents. *See Privacy Protections*, *supra* note 111. While gaining consent may pose initial burdens, if parents understand the value of their children's online activities through communication with the sites themselves, it could prove to be an important asset to the site's prosperity. *Privacy Protections*, *supra* note 111.

[249] The FTC recommends that Web site operators offer parents an alternative method of providing consent for those parents who cannot or will not use the operator's primary consent method. *See* FTC, *Frequently Asked Questions About the Children's Online Privacy Protection Rule*, http://www.ftc.gov/privacy/coppafaqs.htm (last visited Sept. 1, 2001). The FTC recommends the use of a print-and-send form as a practical backup method. *Id*. Such a simple method allows parents without access to e-mail or a credit card to provide consent. *Id*.

[250] 16 C.F.R. § 312.5(b)(2); Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,900, 59,901.

[251] 16 C.F.R. § 312.5(b)(2); Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,900, 59,901.

[252] A child could easily pretend to be a parent and provide consent for himself when a child and parent share the same e-mail account. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,910.

to businesses.[253] Therefore, the Rule includes a temporary sliding scale provision effective through April 21, 2002.[254] This provision enables a Web site to choose a consent mechanism based on how the operator intends to use the child's information.[255] This approach is only temporary in order to provide operators with cost effective options until advances in technology introduce verifiable electronic methods that are more reliable and affordable.[256]

Under the sliding scale approach, if a Web site is simply

---

[253] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,909. For example, parental consent is not required when an operator: (1) collects a name or e-mail address for notice and consent purposes only; (2) collects an e-mail address to respond to a one-time request from a child and then deletes the address; (3) collects an e-mail address to respond more than once to a specific request from a child, as long as the operator ensures that a parent is notified and has the opportunity to prevent further use of the information; and (4) collects a child's name or e-mail address to protect the safety of a child who is using the Web site, or to protect the security or liability of the site, or to respond to law enforcement processes and does not use the information for any other purpose. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(c)(1)-(5) (2001).

[254] *Id*. § 312.5(b)(2). *See infra* note 256 (discussing the future of the sliding scale approach).

[255] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(b)(2) (2001) (allowing an "e-mail plus" option to obtain consent for uses other than "disclosures"). *See infra* note 260 for the definition of disclosures.

[256] After April 21, 2002, Web site operators will no longer be afforded the "e-mail plus" option. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(b)(2) (2001). Technology did not, however, advance as the FTC expected, and less costly methods are not widely available to Web site operators. *See id*. at 59,911. The FTC is currently seeking public comment on a proposal to extend the sliding scale mechanism for an additional two years. Press Release, FTC Seeks Comment on Amending Children's Internet Privacy Rule, *at* http://www.ftc.gov/opa/2001/10/ slidingscale.htm (Oct. 26, 2001) (explaining that the proposal would extend the provision from April 21, 2002 to April 21, 2004). The FTC's original expectation that new technology would be readily available to enhance methods of obtaining parental consent has not been met. *Id*. Therefore, this proposal would seek to continue the privilege of obtaining parental consent by e-mail, coupled with additional steps, for Web sites that collect personal information for internal purposes only, in order to avoid burdening operators seeking to comply with the Rule. *Id*.

collecting information from children for internal purposes only[257] and does not disclose any personally identifiable information to outside parties, e-mail verification is sufficient compliance.[258] However, the company must take additional steps to assure that the person providing consent via e-mail is actually a parent.[259] A higher method of consent is required for activities that pose greater risks to children, namely, disclosing the information to the public or to third parties.[260] When a Web site discloses information to third parties, the Web site must verify consent via a credit card, toll-free number, or print-and-send form.[261] To minimize costs, higher methods of consent may also include e-mail verification so long as it is supported by a password obtained through one or more of the verification mechanisms.[262]

The strong potential of the COPPA's effectiveness is thus illustrated through the FTC's ability to enforce the Act, the application of the safe harbor provision, and the use of a sliding scale approach to obtain parental consent. The legislature, with the help of the FTC, has taken into consideration the unique needs of children and the importance of strong enforcement mechanisms.[263] It has also recognized the importance of keeping

---

[257] Internal uses may include marketing back to a child based on his or her preferences, communicating promotional updates about site content, or e-mailing a newsletter. *See* FTC, *How to Comply*, *supra* note 149.

[258] FTC, *How to Comply*, *supra* note 149.

[259] FTC, *How to Comply*, *supra* note 149. Such additional steps include sending a confirmation e-mail to the parent after receipt of his or her consent, or confirming the parent's consent by mail or phone. FTC, *How to Comply*, *supra* note 149.

[260] 16 C.F.R. § 312.5; *Id*. § 312.2 (defining disclosures as releasing personal information to a third party or making the personal information publicly available, such as through a chat room or bulletin board).

[261] 16 C.F.R. § 312.5(b)(2).

[262] FTC, *How to Comply*, *supra* note 149. In the case of a monitored chat room, however, if the individually identifiable information is removed from the postings prior to its public disclosure, and the information is deleted from the operator's records, then the operator is not required to get prior parental consent. FTC, *How to Comply*, *supra* note 149.

[263] 144 CONG. REC. S8482-03 (daily ed. July 17, 1998) (statement of Sen. Bryan); 16 C.F.R. § 312.9.

industry involved as an active participant in protecting children's online privacy and the need to minimize the burden on businesses. In attempt to balance these concerns, Congress and the FTC have created an effective and dynamic law through the enactment of the COPPA.

CONCLUSION

The Internet is undeniably a valuable and exciting medium for both children and adults. The ease with which personal information can be collected from and about individuals, however, has led to unbridled information collection and abuse. As a result, individual privacy has been sacrificed, and individuals have lost control over the collection and distribution of their personal information. The COPPA is a critical attempt to put an end to the default notion of maximum collection and use of children's personal information on the Internet. This has already been accomplished in the children's Internet industry.[264] Most children's sites have discontinued their practices of using personal information from children for marketing, and no sites are knowingly sharing the collected information with third parties.[265] The COPPA seeks to ensure the security of children's personal information online and to limit the abuse of such information.

The success of the COPPA faces challenges inherent in Internet regulation. Because the Internet has no boundaries, it is easily manipulated, and extensive enforcement of fair information practices is difficult.[266] However, the COPPA serves to increase

---

[264] *See Privacy Protections*, *supra* note 111. *See also COPPA: The First Year*, *supra* note 162, at 17 (stating that children's Web sites are collecting less information as a requirement for using the site).

[265] *See Privacy Protections*, *supra* note 111.

[266] The nature of the Internet does not allow for perfect protection of privacy. Consider that anyone can register a domain name and create his or her own Web site. For an example of a Web site service, *see* http://www.register. com, where anyone can create his or her own Web site. This possibility makes it administratively impossible to police every Web site operator on the World Wide Web. Also, Internet users can manipulate their

children's safety online and to protect their privacy in the most effective way that the Internet currently affords. The COPPA is directed at the wrongdoings of Web site operators; it requires them to comply with standards designed to ensure children's privacy protection. More importantly, the Act emphasizes the parent's role in protecting children's privacy online.

With the shortcomings of the COPPA relative to the difficulty of policing the Internet, parents are in the best position to guarantee their child's protection. The COPPA enhances parents' knowledge about the information that is being collected, used, and disclosed about their child. If parents take this opportunity one step further by directing their children to proceed wisely on the Internet, they can continue to ensure their children's protection where the COPPA and the industry cannot. The same lesson that is drilled into children about not talking to strangers should be taught to them with regard to the Internet. The COPPA emphasizes the importance of parental involvement and, therefore, does not attempt to rely solely on Congress, the FTC, or the industry to protect children using the Internet. This is consistent with the general notion that only with a combined effort by all parties involved will information privacy on the Internet be adequately protected.

---

true identity by creating screen names. *See supra* note 98 (discussing the use of different identities). Finally, Web site operators cannot be held liable when children falsely report their age as older than thirteen because the sites lack actual knowledge that they are dealing with younger children. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,892.