
ARTICLE

MINOR DISTRACTIONS: CHILDREN, PRIVACY AND E-COMMERCE

*Anita L. Allen**

TABLE OF CONTENTS

| | |
|---|-----|
| I. INTRODUCTION | 751 |
| II. HOW THE INTERNET THREATENS YOUNG FAMILIES | 754 |
| III. WHAT COPPA WAS SUPPOSED TO DO | 758 |
| IV. DOES COPPA WORK?..... | 767 |
| V. IS COPPA GOOD LAW?..... | 770 |
| VI. CONCLUSION | 776 |

I. INTRODUCTION

Without a doubt, computer use has had, and will continue to have, a major impact on the economy. Computers, the chief means by which we access the Internet,¹ are changing the way goods and services are designed, manufactured, advertised,

? Professor of Law and Philosophy, University of Pennsylvania. J.D., Harvard Law School; Ph.D., University of Michigan. I would like to thank Sue Regina Lee for her research and editorial assistance with this article.

1. Personal computers, wireless telephones, and other devices are used to gain access to the Internet. See Reuters, *Sprint Plans Wireless Internet Access*, INTERNETWEEK, Aug 12, 1999 (discussing Sprint's plans to provide wireless access to the Web from laptops, handheld computers, and mobile telephones), at <http://www.internetwk.com/story/INW19990812S0002>.

purchased, and distributed.² Computers and the Internet have changed economic, social, and political life to such an extent that questions of equity have arisen. One such question is the question of access to computers for poorer Americans.³ Must a just society insure that low-income households have access to technology comparable to that enjoyed by middle and upper income households? One might argue that everyone, regardless of economic means, requires access to the Internet in order to fully participate and compete. Another important question of equity in Internet access that has arisen is equal access to the Internet for people of all ages, including children.⁴ Must a just society insure that children will have the access to technology enjoyed by adults? In the case of responsible adults, we worry about the moral irrelevance of economic class and the potential harm of too little access to the Internet.⁵ In the case of children, whose need for basic computer literacy seems clear, we worry about the moral relevance of youth and the potential harm of too much access to the Internet.

Policymakers, business concerns, educators, and parents supported passage of the Children's Online Privacy Protection Act⁶ (COPPA). Supporters believed COPPA would reduce the risk of one class of harms posed by the new economy to children who use computers, namely, imprudent disclosures of personal information by children.⁷ Policy analysts cannot yet fairly judge COPPA's success or failure. The statute is still in its infancy.⁸

2. See generally Robert D. Hof, *What Every CEO Needs to Know About Electronic Business: A SURVIVAL GUIDE*, BUS. WK., Mar. 26, 1999, at EB8 (describing the Internet's influence on business practices).

3. See Larry Irving, *Falling Through the Net: Defining the Digital Divide*, NAT'L TELECOMM. & INFO. ADMIN., U.S. DEPT OF COMMERCE, xiii to xv (July 1999), at <http://www.ntia.doc.gov/ntia.doc.gov/ntiahome/fttn99/contents.html>.

4. See *id.* at 7.

5. Because some people seem to spend more time in the "virtual" world than the "real" world, and because the Internet can fuel addictions to gambling and shopping, too much access to the Internet is something of a concern even with respect to mature adults. Mary Mosquera, *March Madness Shows Perils of Net Gambling*, TECHWEB (Mar. 26, 1999), at <http://content.techweb.com/wire/story/TWB19990326S0025>; Evan Schuman, *It's Official: Net Abusers are Pathological*, TECHWIRE (Aug. 13, 1997) (describing Pathological Internet Use (PIU), a new disorder identified by the American Psychological Association), at <http://content.techweb.com/wire/news/aug/0813addict.html>.

6. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (Supp. V 2000).

7. In its notice of proposed rulemaking for the Children's Online Privacy Protection Rule, the FTC invited the public to submit written comments. Many who submitted comments, including parents, advertisers, media interests, and state attorneys general, supported the proposed rule. See, e.g., FTC, *Children's Online Privacy Protection Rule: Public Comments Received*, cmts. 79, 93, 114, 117 [hereinafter FTC, *Public Comments*], <http://www.ftc.gov/privacy/comments/index.html> (last updated Oct. 14, 1999).

8. CTR. FOR MEDIA EDUC., COPPA: THE FIRST YEAR: A SURVEY OF SITES 1 (2001)

Early indications of rampant non-compliance with the statute suggest partial failure.⁹ A striking illustration of the problem occurred more than a year after COPPA went into effect when operators of Brittany Spears' official Web site voluntarily closed the site down in order to revamp for COPPA compliance.¹⁰ COPPA's partial failure is also suggested by the limited degree of parental involvement in monitoring children's Internet use.¹¹ Increased parental involvement with children online was a goal of COPPA.¹² There is little evidence that parents are substantially more involved in supervising their children online after COPPA than they were prior to COPPA.¹³

If evidence of COPPA's failure is troubling, the evidence of its success should be equally troubling. The ultimate political morality of COPPA has never been entirely clear-cut, a point emphasized in this Article by examining the statute from the dual vantage points of privacy law and family law. COPPA is indeed both privacy law and family law. COPPA is Internet privacy law, governing the commercial sector and the market for information.¹⁴ COPPA is also family law, governing young families in the combined interests of child welfare and parental autonomy.¹⁵

(noting that COPPA did not become effective until April 21, 2000), at http://www.cme.org/children/privacy/coppa_rept.pdf.

9. See Press Release, FTC, Web Sites Warned to Comply with Children's Online Privacy Law (July 17, 2000) [hereinafter FTC, Web Sites] (stating that roughly half of the sites the FTC checked that collected children's information had substantial compliance problems), <http://www.ftc.gov/opa/2000/07/coppacompli.htm>; JOSEPH TUROW, THE ANNENBERG PUBLIC POLICY CTR., PRIVACY POLICIES ON CHILDREN'S WEBSITES: DO THEY PLAY BY THE RULES? 2 (2001) ("One in ten . . . of the children's sites collected personal information from visitors but did not have a privacy policy link on their home pages—a clear violation of COPPA."), available at <http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf>.

10. See Reuters, *Oops, Kids Must Be 13 to Log Onto Spears' Site*, TORONTO SUN, May 8, 2001, at 49 (explaining that the Web site for Britney Spears, whose music is enjoyed by children of all ages, has been modified to comply with federal law and will now require parental consent before disclosing personal information).

11. See Mike Snider, *Study: Kids Lacking Net Supervision*, USA TODAY, May 27, 1999, 1999 WL 6843853 (reporting on a study that found about half of parents do not closely supervise their children's Internet usage, and a fifth of parents do not monitor their children's online activities at all).

12. See Maxine Lans Retsky, *Sites Find COPPA Compliance Mandatory, Tough to Figure Out*, MARKETING NEWS, Aug. 28, 2000, 2000 WL 7464500 (noting that Senator Richard Bryan, who introduced the COPPA legislation, expressed COPPA's goals as enhancement of "parental involvement in children's online activities," maintenance of the "security of children's personally identifiable information collected online," and protection of "children's safety and privacy") (paraphrasing Senator Bryan).

13. Refer to note 11 *supra* and accompanying text.

14. See 15 U.S.C. § 6502 (Supp. V 2000) (establishing regulations for the "collection and use of personal information from and about children on the Internet").

15. See *id.* § 6502(b)(2) (enumerating instances in which parental consent is not necessary for gathering information from a child on the Internet).

The wants and needs of the young generate billions of dollars in revenue for the United States economy.¹⁶ Given the economic significance of youth and their families, normative reflections about their ideal roles in the Internet economy are anything but, excusing the pun, minor distractions. To what extent ought the commercial sector have access to children and on what terms? Are efforts to shield children from the commercial sector denying them access to information and transactions to which they are entitled as a matter of political morality?

II. HOW THE INTERNET THREATENS YOUNG FAMILIES

As previously noted, while too little access to the Internet by adult citizen-consumers has become a major concern, too much access by minors has also emerged as a concern.¹⁷ The unlimited, unfiltered, and unfettered access to the Internet enjoyed by many minors at home, in schools, and in libraries stands as a special policy concern.¹⁸ Many young people today know more about computers and Internet use than their parents and grandparents ever will. Nevertheless, some policy-makers and children's advocates would like to see minors shielded and segregated in supervised, filtered, G-rated, advertisement-free corners of the World Wide Web.¹⁹

Even in the face of paramount liberal ideals of speech, knowledge, and the free market, Americans commonly depict use of the Internet as an intolerable threat to families with

16. See News Release, Interep, Interep Study Shows Power of Teen Consumers (March 2001) [hereinafter Interep] (estimating annual teen spending to be \$155 billion), <http://www.interep.com/pr/prmar2001h.pdf>.

17. See Mary Mosquera, *White House Backs Internet Filtering Legislation*, TECHWEB (Mar. 23, 1998) (chronicling Vice President Al Gore's support of legislation requiring schools and libraries to block inappropriate material on the Internet from children), at <http://content.techweb.com/wire/story/TWB19980323S0011>.

18. See Interep, *supra* note 16 ("8 out of 10 teens have Internet access. Almost equal percentages had accessed the Internet at home (46%) as compared to at a library or school (44%)."); News Release, Grunwald Associates, Broad New Survey Shows that 40% of All U.S. Children Are Using the Internet; More than 70% of Teens Are Online (June 7, 2000) (indicating that the majority of parents at least restrict children's Internet use at home), <http://www.grunwald.com/survey/newsrelease.html>.

19. See John Borland, *Internet World Parents Choose Supervision Over Filters*, TECHWEB (Dec. 9, 1997) (stating that some parents consider using filtering software as their children spend more time online, and that the "American Library Association and the National Education Association have angered conservative critics by failing to call for widespread adoption of the [filtering] programs"), at <http://content.techweb.com/wire/story/TWB19971209S0001>; see also Mosquera, *supra* note 17 (describing Vice President Al Gore's support for the Internet School Filtering Act that "would require schools and libraries using federal subsidies for Internet access to block inappropriate material from children").

children.²⁰ Understanding the drive to protect children from threats to their safety and moral development, civil libertarians decry the impact of Internet paternalism on classic ideals of free speech, “the right to know,” and fair market competition.²¹ COPPA, like the Family Educational Rights and Privacy Act of 1976²² (FERPA), purports to protect children’s informational privacy by investing parents with the right to bar certain disclosures of information to third parties.²³ Consumer privacy advocates generally accept the paternalism implicit in FERPA as reasonable. For some privacy advocates, though, COPPA is more controversial than FERPA. COPPA places parents and the government between children and the World Wide Web—the single most powerful source of knowledge and vehicle of communication of all time.

No one can deny, though, that Internet use *is* something of a threat to young families.²⁴ It is a threat for at least five reasons. First, Internet use, like television viewing or comic book reading, competes with activities many of us believe are better for

20. See JOSEPH TUROW & LILACH NIR, THE ANNENBERG PUBLIC POLICY CTR., THE INTERNET AND THE FAMILY 2000: THE VIEW FROM PARENTS, THE VIEW FROM KIDS 12 (May 2000) (finding that many parents believe their children’s exposure to the Internet might interfere with the values and beliefs they want to teach them), available at http://www.appcpenn.org/internet/family/finalrepor_fam.pdf. But the influence of the Internet on families is not all bad. The Internet may improve communication in some families who use email to keep in close contact. See THE PEW INTERNET & AMERICAN LIFE PROJECT, TRACKING ONLINE LIFE: HOW WOMEN USE THE INTERNET TO CULTIVATE RELATIONSHIPS WITH FAMILY AND FRIENDS 7 (2000), available at <http://www.pewinternet.org/reports/toc.asp?Report=11>.

21. See, e.g., Mo Krochmal, *First Amendment Advocates Launch Watchdog Group*, TECHWEB (Dec. 1, 1997) (describing the formation of an alliance group designed to advocate for freedom of expression on the Internet), at <http://content.techweb.com/wire/story/TWB19971201S0003>; Brian Sullivan, *Sen. Kerry: Online Taxes, Privacy Changes Coming* (May 22, 2001) (contending that traditional businesses get an unfair advantage over online businesses if online businesses are prevented from collecting information about consumer buying habits), at <http://www.cnn.com/2001/TECH/internet/05/22/kerry.taxes.idg/index.html>. See also ELEC. PRIVACY INFO. CTR., FAULTY FILTERS: HOW CONTENT FILTERS BLOCK ACCESS TO KID-FRIENDLY INFORMATION ON THE INTERNET (Dec. 1997) (reporting that filtering mechanisms prevented children from obtaining useful and appropriate information from the Internet), at <http://www.epic.org/reports/filter-report.html>.

22. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2001).

23. See *id.* § 1232g(b)(1) (withholding federal funds from institutions that disclose certain types of student information to third parties without parental consent).

24. See CTR. FOR MEDIA EDUC., WEB OF DECEPTION: THREATS TO CHILDREN FROM ONLINE MARKETING 1 (1996) [hereinafter CTR. FOR MEDIA EDUC.] (explaining how online prizes, games, surveys, and advertising invade children’s privacy and constitute unfair and deceptive advertising), available at <http://www.cme.org/children/marketing/deception.pdf>. See also TUROW & NIR, *supra* note 20, at 28 (illustrating that children and teens may be more willing than their parents to disclose personal information about themselves, their parents, and their families).

children.²⁵ These include homework, physical exercise, and conversing with parents face-to-face.²⁶ Second, inappropriate exposure to sex, violence, hate, and advertising content on the Internet can undermine parental values and authority.²⁷ Neither filtering practices nor rating systems have become pervasive or effective enough to reduce the threat of inappropriate exposure to children.²⁸ Third, the Internet can facilitate the sexual exploitation of minors by adult predators. Children who “make friends” over the Internet and agree to face-to-face meetings may discover that their new friend is actually an adult harboring criminal intent.²⁹

25. See Margie K. Shields & Richard E. Behrman, *Children and Computer Technology: Analysis and Recommendations*, 10 FUTURE OF CHILDREN 4, 6 (2000), available at <http://www.futureofchildren.org/cct/index.htm> (last updated Jan. 22, 2001).

26. See *id.* at 6–7.

27. Note the Child Online Protection Act and its uncertain constitutional status. See Child Online Protection Act, H.R. 3783, 105th Cong. § 2 (1998); *ACLU v. Reno*, 217 F.3d 162, 166 (3d Cir. 2000) (holding that the Child Online Protection Act imposed an “impermissible burden on constitutionally protected First Amendment speech”). See also Children’s Internet Protection Act, H.R. 4577, 106th Cong. § 1701 (2000).

28. See Anick Jesdanun, *Technology: Web Filters Far from Perfect*, *Consumer Reports Says*, NANDO TIMES (Feb. 15, 2001) (reporting that, although there are some good programs available, in general, Internet filtering software cannot be relied upon to block out Web sites including objectionable content; also pointing out that “[f]ilters can differ in effectiveness because of both methods and value judgments”), <http://archive.nandotimes.com/technology/story/0,1643,500310093-500498435-503504706-0,00.html> (copy on file with the Houston Law Review). Filtering software works by preventing users from accessing Web sites that are deemed prohibited. See *id.* This technology is primarily used to prevent children from accessing inappropriate sites. *Id.* Software packages use various means to block sites, including ratings, pre-approved lists, lists of prohibited sites, and key words. *Id.* Perhaps filtering software has failed to become widely used because it still is not effective in blocking out inappropriate content. See *id.* See also Media Awareness Network, *Online Rating Systems* (2000) (describing various rating systems and how they operate), <http://www.media-awareness.ca/eng/webaware/tipsheets/rating.htm>. Many different types of rating systems exist on the Internet. *Id.* Most use a system called Platform for Internet Content Selection (PICS), a framework for rating systems, to rate content. *Id.*

Rating systems operate in a variety of ways. Some label sites according to age-appropriateness and others use labels to identify approval. *Id.* Professor Jack Balkin, of the Information Society Project at Yale Law School, has proposed a rating system that consists of:

[T]hree layers placed on top of a software specification: 1. Layer One: A basic vocabulary for first-party raters; 2. Layer Two: A series of templates constructed by third-party raters that combine and rank these vocabulary elements in many different ways. In addition, multiple templates can be combined and added to refine the filter; 3. Layer Three: An assortment of blacklist filters, ancillary rating systems, and redemptive lists maintained by third-party raters, that can be combined and added to the results of layers one and two.

J.M. BALKIN ET AL., INFORMATION SOCIETY PROJECT AT YALE LAW SCHOOL, FILTERING THE INTERNET: A BEST PRACTICES MODEL 33–34 (1999), available at <http://www.yale.edu/lawweb/jbalkin/articles/Filters0208.pdf>.

29. Law enforcement is using the Internet to deter potential sex offenders and crimes against children. See Randy Dotinga, *Ex-Disney Executive Gets Probation in Sex Case* (Aug. 10, 2000) (describing the case of Patrick Naughton, an ex-Disney executive, who actually flew from

The fourth reason Internet use is a threat to young families is that it can compromise child welfare by facilitating knowing and unknowing criminality by children. Juvenile hackers, identity thieves, and viral agents are familiar banes.³⁰ The list of concerns about criminality among teens online was made a little longer and more interesting by Jonathan Lebed. This New Jersey youth capitalized on the anonymity of the Internet and the gullibility of greedy adults to earn \$800,000 by trading stocks.³¹ Mom, Dad, and the Securities and Exchange Commission eventually “grounded” the high-flying investor.³² Lebed reluctantly agreed to give up some of the money he had earned.³³ Bewildered by the SEC’s enforcement effort targeting his high schooler, Greg Lebed, Jonathan’s father, blamed access to the Internet for his family’s woes: “Ever since that computer came into the house, this family was ruined.”³⁴

The fifth and final reason Internet use is viewed as a threat to young families is because the informational privacy of young families is threatened by children’s participation in e-commerce.³⁵ Children are often indifferent to the forms of informational privacy and data protection of concern to adults.³⁶ At present, e-businesses generally must collect personal data to

Seattle to Santa Monica to meet and seduce a person he met online; he thought she was a thirteen year old girl, but the person turned out to be an undercover FBI officer), at http://www.apbnews.com/newscenter/breakingnews/2000/08/10/naughton0810_01.html.

30. See, e.g., Associated Press, *Teen Hackers Tracked Down Via Stolen Credit Card Numbers* (Jan. 26, 1999) (disclosing a teen computer hacking scheme whereby five teens stole multiple credit card numbers), available at <http://www.usatoday.com/life/cyber/tech/ctb104.htm>; CyberCrime, *Teen Virus Writer Goes Legit* (Nov. 10, 2000) (recounting the story of a Tucson high school student, who changed his ways after being arrested for inserting a virus into his school’s computer network), at <http://www.techtv.com/print/story/0,23102,3010689,00.html>; Reuters, *Teen Hackers to be Grounded* (July 30, 1998) (noting two California teens pleaded guilty to illegally accessing restricted U.S. Military computers), at <http://www.wired.com/news/print/0,1294,14119,00.html>.

31. Michael Lewis, *Jonathan Lebed’s Extracurricular Activities*, N.Y. TIMES MAGAZINE, Feb. 25, 2001, at 6, 26.

32. See *id.*

33. *Id.* (reporting that Jonathan Lebed agreed to give up his illicit gains, plus interest, totaling \$285,000).

34. *Id.*

35. This is a major finding of Joseph Turow’s and Lilach Nir’s Annenberg Report. See TUROW & NIR, *supra* note 20, at 4 (“American parents and youngsters are often of very different minds when it comes to giving personal information to Web sites. Kids’ release of information to the Web could well become a new arena for family discord.”). See also CTR. FOR MEDIA EDUC., *supra* note 24, at 4–5 (“[T]he advertising industry is learning how to exploit young computer users more effectively The sooner marketers can reach children, the more products they can sell to them over the years.”).

36. See TUROW & NIR, *supra* note 20, at 35 (finding that children are substantially more likely than parents to give up personal information to a Web site when free gifts are offered).

process purchases; they may, and often do, collect personal data simply to create customer profiles for lucrative marketing purposes or to compile commercially valuable customer mailing lists.³⁷ Children can be lured by online games and prizes into disclosing personally identifiable information and family finances to e-businesses.³⁸ COPPA was enacted to curb the informational privacy loss that threatens families with young children.³⁹

III. WHAT COPPA WAS SUPPOSED TO DO

COPPA went into effect on April 21, 2000.⁴⁰ The legislation was preceded by several private and public sector studies citing informational privacy losses, along with exploitation by advertisers, accessibility to child sexual predators, and exposure to adult content as major risks of children's use of the Internet.⁴¹ The intent of the legislation was to make it more difficult for Web sites to collect personal information directly from young children without a parent's knowledge and consent.⁴² Specifically, COPPA requires commercial Web site operators to obtain the verifiable consent of a parent or similar guardian before collecting personal information from children under thirteen.⁴³ COPPA also limits operators' right to condition prizes and contests on the disclosure of personal information.⁴⁴

There are several key definitions and requirements. COPPA requires "verifiable parental consent for the collection, use or disclosure of personal information" obtained from children.⁴⁵ Under COPPA section 1302(1): "The term 'child' means an

37. See *id.* at 15 (detailing the various methods used by online businesses to obtain personal information from teenagers and adults).

38. See *id.* at 31 (illustrating that children are likely to disclose personal and family information in exchange for gifts).

39. 15 U.S.C. § 6502(a)(1) (Supp. V 2000) (limiting information collected from children under the age of thirteen).

40. FTC, FREQUENTLY ASKED QUESTIONS ABOUT THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE [hereinafter FTC, FREQUENTLY ASKED QUESTIONS], <http://www.ftc.gov/privacy/coppafaqs.htm> (last visited July 9, 2001).

41. See, e.g., CTR. FOR MEDIA EDUC., *supra* note 24 (noting that online advertising and marketing practices are invading children's privacy and exploiting vulnerable, young computer users); FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 5 (1998) [hereinafter FTC, PRIVACY ONLINE] ("The FBI and Justice Department's 'Innocent Images' investigation has revealed that online services and bulletin boards are quickly becoming the most powerful resources used by predators to identify and contact children."), available at <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>.

42. See 15 U.S.C. § 6502(b)(1)(A).

43. *Id.*

44. *Id.* § 6502(b)(1)(C).

45. *Id.* § 6502(b)(1)(A)(ii).

individual under the age of 13.”⁴⁶ The statute applies to children under thirteen, although older children imprudently disclose financial information about themselves and their households, as well. In fact, one study suggested that teenagers may be a bigger problem for online disclosures of private information about their households than children under thirteen.⁴⁷ Why then are children over thirteen excluded? Notice that FERPA, the federal statute governing access to school records, extends parents’ rights through the age of eighteen.⁴⁸ Under FERPA, parents are permitted access to their under eighteen teenagers’ school records over the teens’ objections; parents can also veto disclosures of school records sought by their teenage children.⁴⁹ Under the Privacy Act, parents may access government records about their thirteen-year-old teenage children, over the teens’ objections, and also may seek to limit unwanted disclosure.⁵⁰ COPPA, by contrast, disempowers the parents of teenagers.⁵¹

Although the FTC states that the age of thirteen is the standard for distinguishing adolescents from young children who may need special protections, it fails to state why it assumes that only young children “may not understand the safety and privacy issues . . . and are particularly vulnerable.”⁵² But a number of possible grounds are evident. The framers of the statute may have presupposed that children over the age of thirteen do not recklessly disclose personal information (which seems false). The framers also may have believed that parents, schools, libraries, government, or industry could effectively educate children over the age of thirteen to reduce the likelihood of imprudent disclosures (which seems, in theory, true). Alternatively, the framers of COPPA may have concluded that teens and their families are not seriously harmed by teens’ disclosures of private information. This seems false unless there is a generic difference between the categories of personal information that teens disclose and that younger children disclose. COPPA’s framers may have presupposed that older teens would easily use

46. *Id.* § 6501(1).

47. See TUROW & NIR, *supra* note 20, at 9, 29 (reporting not only that teenagers (ages thirteen to seventeen) said they used the Web substantially more than “tweens” (ages ten to twelve), but also that more teenagers provided information to Web sites about themselves than tweens).

48. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 g(a)(4)(B)(iv) (2001).

49. *Id.* § 1232g(a)(1)(A)–(B), (a)(2), (b)(1).

50. 5 U.S.C. § 552a(h) (2001).

51. See 15 U.S.C. § 6501(1).

52. FTC, FREQUENTLY ASKED QUESTIONS, *supra* note 40 (recommending, however, that operators afford teens privacy protection).

deception to circumvent COPPA's parental notice and consent requirements, rendering them futile. It is also possible that the framers believed children over thirteen were sufficiently sophisticated about advertising and marketing to be free game for e-commerce as a matter of policy. This is an unlikely ground for the exclusion of teens thirteen and older. State, local, and federal governments impose many restrictions on the commercial sector's ability to advertise and sell to older teenagers.⁵³

COPPA applies to "operators" of commercial Web sites and certain other online services that are "directed" to children under thirteen.⁵⁴ A Web site "operator" is defined to include primarily those operating Web sites for profit.⁵⁵ COPPA's definition of "operator" does not distinguish between domestic and foreign-based Web sites.⁵⁶ As long as Web sites are directed at, or knowingly collect information from, children in the United States, COPPA applies.⁵⁷ The rule specifies that foreign Web sites engaged in commerce in the United States or its territories are included within the definition of "operator."⁵⁸ Foreign-based Web site operators who advertise in offline media in the United States or on popular U.S. Web sites place themselves within the FTC's jurisdiction and must comply with COPPA.⁵⁹ The determination of whether a Web site is directed to children under thirteen is based not only on the intent of the Web site operator, but on the language, images, and overall design of the site as well.⁶⁰ COPPA also applies to Web sites and online services that are not specifically directed to children (but perhaps to teenagers

53. Examples of these restrictions are tobacco advertising and glue sales.

54. 15 U.S.C. § 6502(a)(1).

55. *Id.* § 6501(2)(A). The term "operator" is defined 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 or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce . . ." *Id.* Certain non-profits are excluded. *Id.* § 6501(2)(B).

56. *Id.* § 6501(2)(A)(i)-(iii).

57. *Id.* § 6502(a)(1).

58. *Id.* § 6501(2)(A)(i)-(iii).

59. See FTC, FREQUENTLY ASKED QUESTIONS, *supra* note 40 (noting that the statutory definition of "operator" includes foreign Web sites involved in commerce in the United States or its territories).

60. Media Talent Network, *How to Comply with the Children's Online Privacy Protection Rule According to the Federal Trade Commission* (Nov. 1999) ("To determine whether a Web site is directed to children, the FTC will consider several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding . . . the actual or intended audience; and whether a site uses animated characters or other child-oriented features."), at http://www.coppa.org/ftc_how_to.htm.

or to a general audience) and whose operators have “actual knowledge” that they are collecting information from a child.⁶¹ COPPA only applies to Web sites that collect “personal information.”⁶² Importantly, “personal information” is defined broadly to include a person’s name, address, e-mail address, phone number, social security number, and any other identifier deemed to enable physical or online contact.⁶³

COPPA mandates “verifiable parental consent” for data collection, but does not dictate a precise mechanism for obtaining verification.⁶⁴ The FTC has specified an array of methods of obtaining verifiable parental consent.⁶⁵ It is contemplated that the requirements will be subjected to review in 2002.⁶⁶ The operator of a Web site may obtain parental consent online and verify that consent via e-mail or telephone if the personal information is used only internally.⁶⁷ Prior to disclosing information to the general public (via chat rooms or message boards) or to third parties, an operator of a Web site must get parental consent in a more rigorous fashion, such as by a signed fax, credit card number, parent-initiated phone call or secure e-mail.⁶⁸

Exceptions apply to the requirement of parental consent for data collection. Obviously, operators are to be permitted to capture e-mail information in order to provide parental notice and seek parental consent.⁶⁹ Web site operators are also permitted to collect personal information to protect the safety of children, the security of the site, and to satisfy the demands of law enforcement.⁷⁰ In addition, Web site operators may collect an e-mail address (but not other kinds of information) on a one-time basis to process a request from a child if the operator then deletes the information.⁷¹ Parental permission must be obtained if children are to receive newsletters sent to their e-mail

61. See 15 U.S.C. § 6501(4)(B).

62. *Id.* § 6501(2)(A).

63. *Id.* § 6502 (8)(A)–(G).

64. See *id.* § 6502(b)(1)(A)(ii).

65. See FTC, FREQUENTLY ASKED QUESTIONS, *supra* note 40 (describing the various methods that operators can use to obtain parental consent, depending on how the collected information will be used).

66. See 15 U.S.C. § 6506(1).

67. FTC, FREQUENTLY ASKED QUESTIONS, *supra* note 40.

68. Media Talent Network, *supra* note 60 (listing accepted methods of obtaining parental consent to disclose children’s personal information to the public and third parties).

69. 15 U.S.C. § 6502(b)(2)(B).

70. *Id.* § 6502(b)(2)(D)–(E).

71. *Id.* § 6502(b)(2)(A).

addresses on an ongoing basis.⁷² Web sites aimed at educating and informing youth can easily run afoul of COPPA by virtue of maintaining e-mail addresses for the purpose of sending newsletters. The Web site www.thefreestudent.com, which provides news and information about youth, may be such a site.⁷³ However, the site falls outside the scope of COPPA if it is not a commercial site within the meaning of the statute.⁷⁴

Fair information practice standards first promulgated in the 1970s are embodied in COPPA's requirements of notice, access, and security.⁷⁵ COPPA requires certain fair information practices of covered Web sites.⁷⁶ Operators must provide clear "notice" on

72. See *id.* (explaining the parental consent exception only applies when the online contact information is not used to re-contact the child and is not maintained in retrievable form by the operator).

73. The Free Student, *Privacy Policy* (explaining that parental consent was not required before registering for The Free Student Bulletin), at <http://www.thefreestudent.com/about/Privacy.htm> (last visited July 25, 2001).

74. 15 U.S.C. § 6501 (2)(A).

75. U.S. PRIVACY PROT. STUDY COMM'N, *PERSONAL PRIVACY IN AN INFORMATION SOCIETY* 3-6 (1977). See also George Trubow, *Privacy and Fair Informational Practices, Informational Privacy Law and Policy in the U.S.*, NAT'L SYMPOSIUM ON PERS. PRIVACY AND INFO. TECH. (1981) (cited in RICHARD TURKINGTON and ANITA L. ALLEN, *PRIVACY LAW* 318-9 (1999)). Trubow cites a 1973 government report of the Special Advisory Committee to the Secretary of Health Education and Welfare, "Records, Computers and the Rights of Citizens," urging that data collectors follow these guidelines:

- (1) Collect only that personal information necessary for a lawful purpose;
- (2) Use only decision making data that is relevant, accurate, timely, and complete;
- (3) Give the data subject access to information about himself and a procedure by which to challenge and correct the information;
- (4) Use data only for the purpose for which it was collected;
- (5) Protect the data against unauthorized loss, alteration, or disclosure.

Id.

76. See Press Release, TRUSTe, TRUSTe Introduces Children's Privacy Seal Program Yahoo!igans! First Web Site to Participate (Oct. 13, 1998) ("The program, based on recommendations made to Congress by the Federal Trade Commission . . . calls for sites to obtain parental consent or provide parental notice in order for sites to gather and use information from children under the age of 13 . . . Sites that have successfully met TRUSTe guidelines are able to display a 'trustmark' seal to inform users of their participation in the program."), http://www.truste.org/about/about_childseal.html; U.S. DEPT OF HEALTH, EDUC. AND WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) (stating the general requirements for administrative personal data systems: "Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an administrative automated personal data, system, shall make no transfer of any such data to another organization without the prior informed consent of the individual to whom the data pertain . . ."), <http://aspe.hhs.gov/datacncl/1973privacy/c4.htm>. See also FTC, *PRIVACY ONLINE*, *supra* note 41, at 12 ("It is parents who should receive the notice and have the means to control the collection and use of personal information from their children . . . It is a deceptive practice to represent that a site is collecting personal identifying information from a child for a particular purpose . . . when the information will also be used for another purpose that parents would find material, in the absence of a clear and prominent disclosure to that effect . . .").

the Web site of what information the operator collects and how the operator will use and/or disclose information collected from children.⁷⁷ COPPA requires that operators provide parents with: (1) “a description of the specific types of personal information collected from the child by [the] operator”; (2) “the opportunity at any time to refuse to permit the operator’s further use or maintenance . . . of personal information from that child”; and (3) “a means that is reasonable . . . for the parent to obtain any personal information collected from that child.”⁷⁸

The second requirement, that parents be permitted to prohibit further use of information at any time, is a particularly strong consumer right vis-à-vis the commercial sector. This requirement merits special emphasis. The right of parents is not simply an ordinary right to “opt out” of unwanted third-party disclosures, or even a right to limit secondary uses of information. These ordinary rights appear in many formulations of fair information practices.⁷⁹ Under COPPA, parents are ascribed a powerful right to veto primary collection, primary use, secondary use, and even maintenance of data.⁸⁰ This strong right goes beyond typical formulations of fair information practices.

The strong veto right is needed to further the objectives of the statute. COPPA’s parental veto rule is clearly needed to effect meaningful parental control.⁸¹ COPPA confers to parents the power to function as gatekeepers of children and families’ personal information; and, because small children sometimes slip personal information under the gate, parental power to recapture information previously disclosed is critical. An adult individual lacks the power to recapture personal data concerning household income and habits that he or she deems to have been imprudently disclosed by his or her spouse or teenager, but under COPPA that same individual is able to recapture data imprudently disclosed by a young child.⁸² COPPA has no exceptions for “mature minors,” analogous to the required exceptions to laws requiring parental notification or consent for

77. 15 U.S.C. § 6502(b)(1)(A)(i).

78. *Id.* § 6502(b)(1)(B)(i)–(iii).

79. *See, e.g.*, CTR. FOR DEMOCRACY & TECH., PRIVACY BASICS: GENERIC PRINCIPLES OF FAIR INFORMATION PRACTICES, CDT’s GUIDE TO ONLINE PRIVACY (claiming fair information practices include the principles of openness, individual participation, collection limitation, data quality, finality, security, and accountability), <http://www.cdt.org/privacy/guide/basic/generic.html> (last visited July 9, 2001).

80. 15 U.S.C. § 6502(b)(A)(ii), (B)(iii).

81. *See* FTC, PRIVACY ONLINE, *supra* note 41, at 37 (commenting that the role of parents in guarding their children’s privacy is essential to the implementation of fair information practice guidelines).

82. *See* 15 U.S.C. § 6502 (b)(1)(B)(i)–(iii).

abortion services.⁸³ In the realm of data privacy, unlike the realm of reproductive privacy, for children under thirteen, parents rule absolutely.

Parents cannot waive the protection entailed by certain COPPA requirements and prohibitions. For example, COPPA requires operators to establish procedures to protect the “confidentiality, security, and integrity of personal information collected from children.”⁸⁴ This obligation cannot be avoided through parental waivers.⁸⁵ Nor can COPPA’s prohibition against operators conditioning a child’s participation in online activities (for example, games and prizes) on the provision of more personal information than is reasonably necessary to participate in the activity.⁸⁶ This last prohibition disables the use of incentives that would turn simple children’s games into data bonanzas for online businesses. Policymakers did not want e-commerce to have this ability even if particular parents are indifferent.

COPPA authorizes the Federal Trade Commission (FTC) to enforce its provisions.⁸⁷ The FTC can bring enforcement actions under COPPA and impose civil penalties.⁸⁸ Prior to COPPA, the FTC displayed an aggressive interest in Internet privacy in instances in which the privacy of young families was at issue. The FTC’s very first Internet privacy case reflected concerns for children’s informational privacy online.⁸⁹ The FTC settled a deceptive practices suit against GeoCities.⁹⁰ The Commission alleged that “GeoCities misled its customers, both children and

83. See *Hodgson v. Minnesota*, 497 U.S. 417, 455 (1990) (holding that a two-parent notification and consent requirement for minor women seeking abortions is unconstitutional despite the availability of a judicial bypass that would allow minors to obtain abortion without the consent of either parent).

84. 15 U.S.C. § 6502(b)(1)(D).

85. See *id.* § 6502(a)(1), (b)(1)(D).

86. See *id.* § 6502(b)(1)(C).

87. *Id.* § 6505(a).

88. See FTC, FREQUENTLY ASKED QUESTIONS, *supra* note 40 (“Website operators who violate the Rule could be liable for civil penalties of up to \$11,000 *per violation*. The level of penalties assessed may turn on a number of factors including egregiousness of the violation, *e.g.*, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties and the size of the company.”).

89. See Press Release, FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency’s First Internet Privacy Case (Aug. 13, 1998) (charging GeoCities with misrepresenting the purposes for which it was collecting personal identifying information from children and adults), <http://www.ftc.gov/opa/1998/9808/geocitie.htm>.

90. *Id.* (disclosing GeoCities’ agreement to post on its site a clear and prominent privacy notice telling consumers what information is being collected and for what purposes, to whom it will be disclosed, how it will be disclosed, and how consumers can access and remove the information).

adults, by not telling the truth about how it was using their personal information.”⁹¹ The settlement required GeoCities to ensure parental control by obtaining parental consent prior to collecting personal information from children twelve and under.⁹² According to the FTC, industry self-regulatory guidelines already in effect in 1998 but ignored by GeoCities, urged sites to obtain parental consent for at least some transactions with children.

On May 6, 1999, the FTC announced that The Young Investor Web site operated by Liberty Financial Services, a large Massachusetts asset management company, had settled an action alleging false promises of anonymity.⁹³ As reported by the FTC, the Web site operators used contests, prizes and promises of anonymity to induce children to provide detailed financial data about their allowances, stocks, bonds, mutual funds, spending habits, college plans, and family finances.⁹⁴

The FTC initiated its first enforcement action under COPPA in a case alleging a violation of the provision against the conditioning of participation in a contest on disclosures of personal information.⁹⁵ On July 21, 2000, the Commission filed its first enforcement action under COPPA against Toysmart.com, concurrent with its settlement of charges that Toysmart had violated its own TRUSTe approved privacy policy when it sought to sell its customer database to discharge obligations in bankruptcy.⁹⁶ The COPPA violation alleged against Toysmart was that a trivia contest, which first appeared on the Toysmart Web site in May 2000, collected personal information from children under thirteen without obtaining the consent of the

91. *Id.* (quoting Jodie Bernstein, Director of the FTC’s Bureau of Consumer Protection).

92. *Id.*

93. See Press Release, FTC, Young Investor Website Settles FTC Charges (May 6, 1999) (“The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family’s finances was maintained in an identifiable manner.”), <http://www.ftc.gov/opa/1999/9905/younginvestor.htm>.

94. See *id.*

95. See *FTC v. Toysmart.com*, No. 00-11341-RGS (D. Mass. filed July 21, 2000) (“[T]hrough its dinosaur trivia contest, which was directed to children, Toysmart collected personal information from children that, in addition, it actually knew to be under the age of 13, without providing notice to parents or obtaining verifiable parental consent prior to the collection of such personal information.”).

96. See Press Release, FTC, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000) (“Toysmart has posted a privacy policy which states that information collected from customers will never be shared with third parties. When it ran into financial difficulties, however, it attempted to sell all of its assets, including its detailed customer databases. . . .”), <http://www.ftc.gov/opa/2000/07/toysmart2.htm>.

children's parents.⁹⁷ The contest conditioned participation on the disclosure of personal information.⁹⁸

On April 19, 2001, the FTC announced the settlements of its first line of civil penalty cases brought under COPPA. Monarch Services, Inc. and Girls Life, Inc., operators of www.girlslife.com; Bigmailbox.com, Inc., and Nolan Quan, operators of www.bigmailbox.com; and Looksmart Ltd., operator of www.insidetheweb.com, were charged with violating COPPA by illegally collecting personal information from children under thirteen years of age without parental consent and requiring children to disclose more personal information than was needed for participation in the activities involved.⁹⁹ To settle the charges, the operators agreed to pay \$100,000 in civil penalties.¹⁰⁰ Furthermore, the settlements bar any future COPPA violations and require the companies to delete all personally identifying information collected from children online at any time since COPPA became effective.¹⁰¹ In addition, the operators will post a privacy policy on their Web site that complies with the law, as well as a link to www.ftc.gov/kidzprivacy, the FTC's site that provides information about COPPA.¹⁰²

COPPA section 6503 provides a safe harbor for operators who follow Commission-approved self-regulatory guidelines issued by representatives of the marketing or online industries or other designated persons.¹⁰³ Several groups and companies have already applied for safe harbor status, and at least three applications have been approved.¹⁰⁴ To encourage compliance and limit the need for formal enforcement actions, the FTC is seeking to educate the public. The FTC operates multiple Web sites designed to educate the public about privacy online. For example, colorful, consumer-friendly FTC Web site called "Kidzprivacy" seeks to educate parents and children about online informational privacy, and about their rights and powers under COPPA.¹⁰⁵

97. *Id.*

98. *See Toysmart.com*, No. 00-11341-RGS.

99. Press Release, FTC, FTC Announces Settlements with Web Sites That Collected Children's Personal Data Without Parental Permission (Apr. 19, 2001), <http://www.ftc.gov/opa/2001/04/girlslife.htm>.

100. *Id.*

101. *Id.*

102. *Id.*

103. 15 U.S.C. § 6503 (Supp. V 2000).

104. *See* FTC, *Safe Harbor Program* (listing the approved applications for safe harbor status of Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus, Inc., ESRB Privacy Online, and TRUSTe), at <http://www.ftc.gov/privacy/safeharbor/shp.htm> (last updated May 23, 2001).

105. *See* FTC, *How to Protect Kids' Privacy Online* (Feb. 2000) (stating that operators

IV. DOES COPPA WORK?

COPPA was designed to protect the informational privacy of children and their families from excessive and unwanted disclosures of personal information.¹⁰⁶ It was designed to impose certain fair information practices on e-commerce, and to educate the public.¹⁰⁷ COPPA was not designed to bring to a halt data collection, advertising, and sales practices that target young people and their families.¹⁰⁸

Relative to its design, COPPA's efficacy can be judged by reference to three factors. The first is whether commercial Web sites are complying with the requirements of the statute that limit excessive and unwanted disclosures of personal data. The second is whether parents are supervising children on the Internet and cooperating with industry efforts to acquire personal data within the framework set by COPPA. The third is whether the FTC has been willing and able to enforce the statute to the limits of its jurisdiction without curbing lawful forms of e-commerce.

As to industry compliance, the efficacy of the statute is, thus far, a mixed picture. Some sites comply; some do not. In July 2000, the FTC undertook to determine whether Web site operators were complying with COPPA.¹⁰⁹ Of the kid-sites visited by FTC staff, only about half were COPPA compliant.¹¹⁰ The FTC issued warning letters to several sites.¹¹¹ A recent report by

must post their privacy policy, get parental consent, get new consent when information-practices change in a "material" way, allow parents to review personal information collected from their children, allow parents to revoke their consent, and delete information collected from their children at the parents' request; parents should look for a privacy policy on any Web site directed to children, decide whether to give consent, decide whether to approve information collection from their children based on new uses for the information, ask to see the information their child has submitted, and understand that they may revoke their consent at any time and have their child's information deleted), at <http://www.ftc.gov/bcp/online/pubs/online/kidsprivacy.htm>.

106. See Press Release, FTC, New Rule Will Protect Privacy of Children Online (Oct. 20, 1999) (explaining the goals of COPPA).

107. *Id.* (detailing the requirements of the statute).

108. See *id.* (explaining that the rule "is flexible enough to accommodate the many business practices and technological changes occurring on the Internet," and that there are "several exceptions to the requirement of prior parental consent").

109. See FTC, Web Sites, *supra* note 9.

110. *Id.*

111. *Id.* ("Although the law requires that you take certain steps to protect the privacy of children online, your site appears to collect personally identifying information from children under 13 without providing a privacy policy, without giving notice to parents, and/or without getting parental consent. We recommend that you review your web site with respect to information collection from children in light of the law's requirements. Be aware that the FTC will monitor web sites to determine whether legal action is warranted.").

Professor Joseph Turow, an independent academic researcher, indicates that most commercial Web sites geared for children ignore children's privacy and the requirements of COPPA.¹¹² Many believe parental control software rather than strict compliance by industry with COPPA is the real key to protecting children from making harmful disclosures because, without close supervision, "it is clear that many of today's tech-savvy children will be able to get around parental notification and consent."¹¹³

The picture of parental involvement with children online post-COPPA is murky. It is unclear how COPPA has affected parents' and children's online behavior. Not all parents welcome the veto power COPPA confers.¹¹⁴ New power has meant new responsibility. The statute forces parents who would otherwise be content to give their children free reign over their computers to get involved in children's use of Internet sites that are geared toward children and collect personal information.¹¹⁵

COPPA is least onerous for parents whose children prefer non-commercial sites that do not collect personal information. COPPA is only moderately onerous for parents whose children are content to frequent the same one or two sites for periods of weeks or months at a time. The statute is most onerous for parents whose children are especially fond of children's sites and

112. See D. Ian Hopper, *Study: Web Sites Ignore Kids' Privacy*, L.A. TIMES, Mar. 28, 2001 (reporting on a study by Professor Joseph Turow at the University of Pennsylvania's Annenberg Public Policy Center, which found that half of the 162 sites included in the study because they have a high volume of children under thirteen who visit them—sites for video games, snack foods, children's characters and television shows—have complex, hard-to-read privacy policies, that omit COPPA-required information about parents' rights to review and remove information from sites, and have no home page or other prominent links to their privacy policies), available at <http://antionline.com/2001/03/28/---/7150-1821-kids-privacy.html>.

113. Tyler Prochnow, *Software to Help Facilitate COPPA Compliance*, E-COMMERCE, May 2000 ("To be truly good corporate citizens, sites that do not want visitors under the age of 13 should encourage the use of filtering software by parents."). Filtering software is more responsive to the policy concerns that led to the enactment of the highly controversial COPA statute than COPPA. COPA, the Children's Online Protection Act, went into law October 21, 1998. 47 U.S.C.A. § 231 (West Supp. 2000). COPA requires commercial sites that include materials harmful to minors (such as hard pornography) to ensure that minors do not access such materials. See *ACLU v. Reno*, 217 F.3d 162, 166 (3d Cir. 2000) (holding that the COPA "imposes an impermissible burden on constitutionally protected First Amendment speech").

114. In response to the FTC's notice of proposed rulemaking for the Children's Online Privacy Protection Rule, many parents expressed opposition to the rule, stating that the rule is paternalistic, parents should be responsible for protecting their children, and Web sites would pass on increased administrative costs to consumers. See, e.g., FTC, *Public Comments*, *supra* note 7, at cmts. 12, 24, 31.

115. 15 U.S.C. § 6502(b)(1)(A) (Supp. V 2000) (requiring "the operator of any website . . . that collects personal information from children . . . to obtain verifiable parental consent" even after the child has given his or her own consent).

enjoy constantly exploring the Web to discover new sites. Dynamic young Web-surfers, who enjoy visiting numerous new sites, could easily aggravate parents with repeated requests that they provide “verifiable parental consent.”

Now that COPPA is in effect, parents can respond to their children in a number of ways. “You are free, don’t bother me,” is one response; “only with me,” is a second response; and “Disney and Nickelodeon only,” is a third response. The “you are free, don’t bother me” response characterizes parents who allow their children to surf the Web without close supervision, with the understanding that the children should not repeatedly request parental help accessing sites that collect personal data and require verifiable parental consent. The danger of this approach is that it may make children more likely to visit youth-oriented sites that are not compliant with COPPA, along with sites with what most regard as age-inappropriate adult content. The “only with me” response characterizes parents who allow children to explore the Internet, so long as they do so when parents have the time and desire to work on securing COPPA-required permissions. The downside to this response is that it is time consuming and may frustrate children’s curiosity and desire for independence. The “Disney and Nickelodeon only” response characterizes parents who allow their children to visit independently a handful of specific, familiar Web sites whose data collection practices are known, trusted, and to which the parent gives consent. The downside to this approach is that site brand-limited young children do not engage in the vast educational and amusement potential of the Internet.

Parents may want their children to have free access to the World Wide Web because they believe the risks are minimal, or because they do not have the time or interest to deal with their children’s Web activities. It is worth observing, though, that some parents may want their children to have free access to the Internet for moral or political reasons. They may believe children should have unfettered access to the Web and the public library equally, as a matter of free speech, free expression, and the right to know. They may want their children to develop judgment and taste by exposure to the best and worst of civilization in the relatively safe and private terrain of books and the Internet. COPPA’s requirements are not specifically designed to deny children access to content, but, as civil libertarians observe, that is one of their effects.¹¹⁶

116. See, e.g., FTC, *Public Comments*, *supra* note 7, cmt. 115.

A final measure of whether COPPA is working is the aggressiveness of FTC enforcement activities. As previously mentioned, the FTC has set up several Web sites to educate the public about COPPA. In addition, the FTC began sending warning letters to non-compliant Web sites in July 2000, just a few months after COPPA went into effect.¹¹⁷ It was also in July 2000, that a COPPA complaint was added to the FTC's lawsuit against Toysmart.com.¹¹⁸ This level of activity and these types of activities on the part of the FTC are not especially aggressive. However, they are arguably appropriate, given the climate of frenzied regulatory activity in the privacy arena that has caught many in the industry off guard.

Vast sectors of the economy have been hit with new privacy laws in 2000 and 2001. COPPA pertains to the e-commerce sector, HIPAA¹¹⁹ to the health care sector, and Gramm-Leach-Bliley¹²⁰ to the financial services sector. Businesses in all areas are scrambling to re-orient their practices for compliance.¹²¹ In many cases even the lawyers who serve corporate clients are not well educated about the requirements of the new privacy laws. The new body of privacy law is sending lawyers, consultants, and corporate managers back to school.¹²² For this reason the current FTC emphasis on education and warning seems warranted.

V. IS COPPA GOOD LAW?

While Congress has passed statutes governing the privacy and security of health and financial information,¹²³ no comprehensive Internet privacy law has been enacted. COPPA was the nation's first specific online privacy protection law. COPPA was cyber law, but it was also family law. COPPA did

117. See FTC, Web Sites, *supra* note 9.

118. Press Release, FTC, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), <http://www.ftc.gov/opa/2000/07/toysmart2.htm>.

119. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), available at <http://aspe.hhs.gov/admsimp/pl104191.htm>.

120. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=fpubl102.

121. See Edmund Sanders, *Privacy is Becoming Everyone's Business; Online: Firms New and Old are Offering Consultation Services, Hoping to Benefit from Growing Anxiety about Data Collection*, L.A. TIMES, May 22, 2001, § 3 (Business), at 1 (reporting that the business of providing consultation for privacy law compliance is booming).

122. See, e.g., *Compliance Coach Partners with Axiom to Assist Nation's Largest Financial Institutions in Complying with Stringent New Privacy Regulations*, BUSINESS WIRE, Jan. 16, 2001 (describing efforts to help train institutions to comply with the Gramm-Leach-Bliley Act), at <http://www.businesswire.com>; Sanders, *supra* note 121.

123. See generally Health Insurance Portability and Accountability Act of 1996, 110 Stat. 1936; Gramm-Leach-Bliley Act of 1999, 113 Stat. 1338.

what family law does. It conferred legal power over children to parents or other adult guardians,¹²⁴ enabling paternalistic and authoritarian intervention. It is a paternalistic, authoritarian measure designed to limit the ability of children under the age of thirteen to disclose personally identifying information without the knowledge and consent of their parents.¹²⁵

With COPPA, Congress attempted to strike a balance between the social good of youth access to the Internet and the free market, on the one hand, and the social good of parental supervision of Internet use and market transactions by youth on the other. But what, really, are the normative implications of making parents the guardians of children's and household privacy? Is doing so good family law? Good privacy law?

COPPA is family law when viewed as a governmental effort to compel parental child protection in the best interests of children, first, and to privilege parental over non-parental influences on young children, second. COPPA seeks to buttress the family by regulating the flow of information about children and their families to the public.

As previously noted, in May, 2000, researchers at the University of Pennsylvania's Annenberg Public Policy Center released a study showing that children are more likely than their parents to reveal personal family information online.¹²⁶ Although most parents surveyed had concerns about their children's Internet use, 89% said they believe the Internet is beneficial to schoolwork, and 85% said that children find fascinating and useful information on the Internet.¹²⁷ Parents believe Internet use benefits their children but also that children may be more likely than adults to make poor judgments about yielding personal information in the context of electronic commerce.¹²⁸ A 1996 report by the Center for Media Education noted that the "interactive nature of the Internet gives marketers unprecedented power to gather detailed personal information from children."¹²⁹ Prior to COPPA, marketers could freely elicit data from children overtly, using games and prizes as incentives, and covertly, using software that tracks online behavior.¹³⁰ Some

124. Refer to note 115 *supra* and accompanying text.

125. Refer to note 115 *supra* and accompanying text.

126. See TUROW & NIR, *supra* note 20, at 35 (finding that children are substantially more likely than parents to give up personal information to a Web site when free gifts are offered).

127. *Id.* at 12.

128. *Id.*

129. CTR. FOR MEDIA EDUC., *supra* note 24, at 7.

130. *Id.* at 7-9.

parents may want help in limiting their children's access to the Internet and may value COPPA for that reason. (Others may not.)

From a family law perspective, COPPA has several normative weaknesses. First, it draws a line of dubious justification between teenagers and "tweenagers."¹³¹ A number of younger children will be as able as many teenagers when it comes to circumventing the requirements of the statute. Some children under thirteen are no more or less in need of parental control than teenagers. Thus the statute seems morally arbitrary.¹³²

Second, the policy objective of protecting children from the harmful consequences of Internet use is barely served by COPPA. COPPA barely helps parents whose children go online. It limits access to commerce, but not to adult content.¹³³ Now, as before COPPA's enactment, direct and constant parental supervision is needed to keep children from adult content, since most Web sites that do not collect personal information, and many that do, can be visited in part or in full by children of any age.

Third, COPPA's paternalism and authoritarianism places parents between beneficial information and online activities. COPPA is paternalistic in the sense that it presumes that young children lack the judgment needed to know when the disclosure of personal information is safe and warranted. COPPA is authoritarian in the sense that it presumes that government may authorize parents to, for reasons of their own, prohibit children from exchanging personal data for access to Internet-based commerce, however desirable or useful to the children. Like other legal measures that place parents between a child and a mainstream social good, COPPA is morally problematic.

From the point of view of family law, placing parents between children and the Internet is arguably suitable. As a general rule, children need protection. The societal mandate is that public authorities protect children by looking after their best interests. In the first instance, parents are those with whom

131. "Tweenager" is "a currently fashionable marketing term for pre-teens, girls in particular, aged between 7 and 11, a group having substantial purchasing power." World Wide Words: Exploring the English Language, <http://www.worldwidewords.org/turnsofphrase/tp-twe2.htm> (last updated Apr. 28, 2001); see also TUROW & NIR, *supra* note 20, at 9, 29 (referring to children between the ages of ten and twelve as "tweens").

132. The FTC seems to address this arbitrary age distinction in the recently proposed Online Privacy Protection Act of 2001, which requires protection of privacy of personal information collected through the Internet from and about all individuals. See Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001).

133. 15 U.S.C. § 6501(2) (Supp. V 2000) (limiting the scope of the statute to those who operate a Web site or online service for "commercial purposes").

primary responsibility for executing this mandate rests. Parents should be a part of the decisions made by the minor children for whose safety and well being they are ultimately responsible. We hear this principle asserted with varying efficacy in connection with everything from teen abortion rights to the "V-chip."¹³⁴ So, it should come as no surprise to hear it in connection with the Internet.

Parents fear unfettered access. James M. Knight is an apt illustration. A parent in Exeter, New Hampshire, Mr. Knight recently brought a lawsuit to compel public school authorities to give him access to the "computer files that would reveal the Internet sites visited by all computer users in the schools of two local districts."¹³⁵ The Supreme Court has often sided with parents who wish to restrict children's access to information and services provided by public schools. The Court has famously held that Amish parents may keep children older than thirteen out of school, to inculcate Amish values.¹³⁶ COPPA can be read in that same tradition, as the Congress of the United States saying that all parents may keep children under thirteen away from e-commerce, to inculcate parental values.

COPPA is commercial sector privacy law when viewed, in the vein of the Video Privacy Act of 1988,¹³⁷ or Title V of the Financial Services Modernization Act,¹³⁸ as another measure to regulate the flow of personal information entrusted to others with expectations of confidentiality and security in an economically sensible way. Again, children may be more likely than adults to make poor judgments about yielding personal information in the context of electronic commerce.¹³⁹ To make it harder for industry to prey upon children's indifference to disclosing personal information about themselves and others of

134. See Teresa Stanton Collett, *Seeking Solomon's Wisdom: Judicial Bypass of Parental Involvement in a Minor's Abortion Decision*, 52 BAYLOR L. REV. 513, 577-78 (2000) ("The most we can do is to prevent the judicial system from being used to disrupt the wide sphere of reasonable discretion which is necessary in order for parents to properly exercise their responsibility to provide nurture, care, and discipline for their children."); James T. Hamilton, *Private Interests in "Public Interest" Programming: An Economic Assessment of Broadcaster Incentives*, 45 DUKE L.J. 1177, 1183-84 (1996) ("[P]arents must search out information on program content and then monitor television use by children.").

135. Carl S. Kaplan, *Suit Considers Computer Files*, CYBER LAW J., N.Y. TIMES, Sept. 29, 2000, available at <http://www.nytimes.com/2000/09/29/technology/29CYBERLAW.html>.

136. *Wisconsin v. Yoder*, 406 U.S. 205 (1972).

137. Video Privacy Act of 1988, 18 U.S.C. § 2710 (2000).

138. Gramm-Leach-Bliley Act of 1999, *supra* note 120, at tit. 5 (to be codified in relevant part at 15 U.S.C. §§ 6801-6809).

139. Refer to notes 126-28 *supra* and accompanying text.

the sort e-businesses most want, COPPA compels parents to get involved in the monitoring of data collection.¹⁴⁰

As privacy law, COPPA falls into a small class of privacy laws that challenge purely voluntary notions of privacy. An implicit message of COPPA is that privacy is too important to be left to the judgment of minors. The same message is implicit in the Privacy Act of 1974, which authorizes “the parent of any minor” to “act on behalf of the individual.”¹⁴¹ The Privacy Act provides, however, that a parent “*may* act on behalf of”¹⁴² a minor, leaving open the possibility that a child could assert, or refuse to assert, interests in the privacy of government records containing personal information about him or her. Looking at the entire body of American privacy law, though, it is not clear why children should not be permitted to waive their informational privacy rights online.

Children are accorded privacy rights under major privacy laws.¹⁴³ They are permitted to waive their privacy rights in a number of contexts. Indeed, most informational privacy rights recognized in American law can be waived by most people, including children. Fourth Amendment rights protecting reasonable expectations of privacy can be waived. A school child can decide she wants to show her teacher what is in her backpack, whether or not the teacher’s search would meet an exception to the Fourth Amendment’s warrant requirement.¹⁴⁴ We adults are free to invite the police into our homes, give them our blood, our thoughts and our diaries, even though the consequences may mean criminal prosecution and loss of liberty.

The Video Privacy Act does not prohibit anyone from authorizing release to third parties the titles of one’s own prior video rentals.¹⁴⁵ HIPAA does not prohibit anyone from telling someone else his or her medical history.¹⁴⁶ Although those seeking to release their records must give informed consent, they

140. Refer to note 115 *supra* and accompanying text.

141. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

142. *Id.* (emphasis added).

143. The definition of “person,” “individual,” “consumer,” “customer,” or “employee” includes minors under the Fair Credit Reporting Act, 15 U.S.C. § 1681a(b) (2000); the Privacy Act, 5 U.S.C. § 552a(a)(2) (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401(4) (2000), the Video Privacy Protection Act, 18 U.S.C. § 2710(a)(1) (2000) and the Employee Polygraph Protection Act, 29 U.S.C. § 2001(2) (2000).

144. See *New Jersey v. T.L.O.*, 469 U.S. 325, 330–33 (1985); see also *Veronica Sch. Dist. v. Acton*, 515 U.S. 646, 655–56 (1995).

145. 18 U.S.C. § 2710.

146. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

may disclose personal medical information freely.¹⁴⁷ The Privacy Act does not prohibit one from revealing the criminal history contained on his or her own “rap sheet.”¹⁴⁸ No law prohibits minors from walking into a bank and disclosing the personal information required when applying for a bank account.¹⁴⁹ COPPA does, however, block voluntary disclosures of personal data.¹⁵⁰ Prohibiting voluntary disclosures by children lacking parental consent in situations in which they and their parents may be indifferent to privacy losses and resentful of government intervention, COPPA is among the most paternalistic and authoritarian of the federal privacy statutes thus far. FERPA is more paternalistic in one sense: it extends the parental right to veto third party disclosures of their children’s educational records up through the child’s eighteenth year, while the COPPA veto expires at the thirteenth year.¹⁵¹

Privacy advocates are not so sure about COPPA, despite the characterization of its passage as a consumer privacy victory. On June 9, 2000, in testimony before the Commission on Child Online Protection, a body created by Congress in the COPPA, Electronic Privacy Information Center (“EPIC”) general counsel, David L. Sobel, urged the rejection of age verification requirements as a condition of access to the Internet.¹⁵² Instead of blocking access, efforts should be made to help young people learn to safely and responsibly navigate the Internet. Mr. Sobel argued that a new regime for the collection of personal data in the name of “child online protection” would impose additional burdens on Internet users.¹⁵³ At present, I am inclined to agree.

147. See 45 C.F.R. § 164.506 (2001).

148. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

149. See, e.g., Commerce Bank, Student Banking Program (2001), available at <http://www.commerceonline.com/glossary/showContent.cfm?subtopicid=2242> (last visited June 21, 2001).

150. Refer to note 115 *supra* and accompanying text.

151. Compare Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2000), with Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (Supp. V 2000).

152. See David L. Sobel, Statement before the Commission on Online Child Protection (June 9, 2000), http://www.epic.org/free_speech/copa/statement_6_00.html.

153. *Id.* In challenging laws that restrict access to material on the Internet, Sobel claimed that “age verification requirements will deter most adults from accessing restricted content, because Web users are increasingly unwilling to provide identifying information in order to gain access to online content,” and that this obstacle will effectively prevent users from accessing “a wide range of constitutionally protected speech.” *Id.* The ACLU has also taken a strong position against government attempts to restrict Internet content, calling self-rating “the greatest danger to free speech online.” Press Release, ACLU, Is Cyberspace Burning? ACLU Says Internet Ratings May Torch Free Speech on the Net (Aug. 7, 1997), <http://www.aclu.org/news/n080797a.html>. According to the ACLU, the notion of self-rating is “no less offensive to the First

Privacy protections that barely protect privacy, that seem morally arbitrary, that aggravate parents, frustrate children, and block access to information and communication may come at too high a cost.

VI. CONCLUSION

COPPA is coercive, both as it relates to parents and as it relates to children. The coercion was thought to be justified by the danger to children and their families posed by the Internet, dangers to which both children and their parents may be unduly inattentive. How serious are the dangers? Using the Internet without close adult supervision can be dangerous for minors. Children may recklessly or unknowingly give personal information to strangers set on illegal sexual or other exploitation.¹⁵⁴ An additional danger is that minors may be less cautious than their parents about giving out embarrassing or intimate personally identifying information about other members of their families.¹⁵⁵ Parents may worry about Internet use for reasons unrelated to informational privacy. Children's obsession with Internet-based games, music, research, and communication can impair the ability of families to spend "quality time" together. Moreover, a few notorious youth have used their computers for mischief—hacking into government networks, spreading viruses, or influencing the stock market. COPPA is not a solution to all of these problems. How effective it will be in addressing some of them remains to be seen, and will depend upon the success of government-led efforts at education and enforcement. How legitimate it will seem over time is another matter.

Amendment than a proposal that publishers of books and magazines rate each and every article or story, or a proposal that everyone engaged in a street corner conversation rate his or her comments." ACLU, *FAHRENHEIT 451.2: IS CYBERSPACE BURNING?* (1997), available at <http://www.aclu.org/issues/cyber/burning.html>. So far, EPIC and the ACLU have been successful in their constitutional challenge against the Child Online Protection Act. See *ACLU v. Reno*, 217 F.3d 162, 166 (3d Cir. 2000) (holding that the Child Online Protection Act "imposes an impermissible burden on constitutionally protected First Amendment speech").

154. Refer to notes 126–30 *supra* and accompanying text.

155. Refer to notes 126–28 *supra* and accompanying text.