Northwestern Journal of Law & Social Policy

Volume 5 | Issue 2 Article 7

2010

Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era

Lauren A. Matecki

Volume 5 (Fall 2010)
Northwestern Journal of Law and Social Policy

Update: COPPA is Ineffective Legislation!

Next Steps for Protecting Youth Privacy Rights in the Social Networking Era

Lauren A. Matecki*

> Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world. . . . Let us do what is essential to permit the participants in this evolving world to make their own decisions.[1]

¶1 In 1998, Congress passed the Children's Online Privacy Protection Act in response to growing concerns over the dissemination of children's personal information over the Internet.[2] The Act responded to the growing number of children online and addressed concerns over the harms that could arise if websites were not held accountable for the manner in which they collected and used children's personal information.[3] Legislators sought to balance the benefits of the Internet as an educational tool, with the risks to children's privacy and safety that could come from the ease of sharing personal information online.[4] In particular, legislators were concerned about the ability of children to meaningfully understand the harms that could arise from giving out their personal information over the Internet, such as abuses by online marketers, deceptive trade practices, and safety concerns.[5]

¶2 The Children's Online Privacy Protection Act and the Federal Trade Commission's (FTC) subsequent Children's Online Privacy Protection Rule promulgated in 2001 (collectively, COPPA), set forth privacy standards for websites "directed towards children" under the age of thirteen, including providing notice to the nature and use of information collected, and requiring websites to obtain "verifiable parental consent"

---

* Juris Doctor, 2010, Northwestern University School of Law; Bachelor of Arts, 2007, Northwestern University. Thank you to the editors of the *Northwestern Journal of Law and Social Policy* for their helpful edits and advice. Thank you to Professor Peter DiCola for his guidance and feedback. Finally, thank you to my parents, family, and friends for their constant support and encouragement.

[1] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 215–16.

[2] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); FTC, FILE NO. 954,4807, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) [hereinafter PRIVACY ONLINE REPORT], *available at* http://www.ftc.gov/reports/privacy3/toc.shtm. The Children's Online Privacy Protection Act (COPPA) should be distinguished from the Child Online Protection Act (COPA). COPA sought to protect minors from exposure to sexually explicit materials online and was held unconstitutional on free speech grounds. ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008).

[3] PRIVACY ONLINE REPORT, *supra* note 2, at 12.

[4] *See* discussion *infra* Part II.A.

[5] PRIVACY ONLINE REPORT, *supra* note 2, at 12, 46.

before collecting or using children's personal information.[6] Consistent with traditional regulatory standards, COPPA only applies to the collection of personal information from children ages twelve and under, as such children are thought to be more susceptible to deceptive practices and therefore in greater need of protection.[7]

¶3 While the FTC has brought high-profile enforcement actions against websites that have failed to comply with COPPA regulations,[8] commentators have criticized COPPA as ineffective.[9] In particular, critics note that the practical effect of COPPA causes websites simply to ban users twelve and under.[10] While in theory this strategy may sound effective, in reality it simply encourages age fraud and allows websites to bypass the burden of obtaining parental consent.[11]

¶4 This Comment will argue that an overhaul of COPPA, providing for stricter regulation on collection and dissemination of personal information by websites themselves, is necessary to protect both children and teenagers from today's privacy threats. Ten years after the passage of COPPA, the landscape of the Internet, particularly with regard to children and adolescents, has changed dramatically. In 2009, children ages two to eleven represented 9.5% of all Internet users.[12] Studies have shown that 93% of Americans between the ages of twelve and seventeen have access to the Internet and 61% browse the Internet daily.[13]

¶5 The dramatic rise of Internet usage among children and teens creates additional opportunities for the misuse of personal information. However, a new and important trend in *how* children and teens use the Internet has also developed in recent years. This trend is the rise of social networking sites.

¶6 Launched in 2003 and 2004, respectively, websites such as Myspace.com and Facebook.com are tremendously popular among adolescent Internet users.[14] Recent surveys have found that 71% of teenagers have social networking profiles.[15] Further,

---

[6] 15 U.S.C. § 6502(b)(1)(A)(ii) (2006); Children's Online Privacy Protection Rule, 16 C.F.R. §§ 312.1–312.10 (2009); *see* discussion *infra* Part II.B.

[7] PRIVACY ONLINE REPORT, *supra* note 2, at 46; FTC, FREQUENTLY ASKED QUESTIONS ABOUT THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE (Oct. 7, 2008), *available at* http://www.ftc.gov/privacy/coppafaqs.shtm ("Congress determined to apply COPPA's protections only to children under 13. Congress and industry self-regulatory bodies have traditionally distinguished children aged 12 and under, who are particularly vulnerable to overreaching by marketers, from children over the age of 12, for whom strong, but more flexible protections may be appropriate. In addition, distinguishing adolescents from younger children may be warranted where younger children may not understand the safety and privacy issues created by the online collection of personal information.").

[8] *See* discussion *infra* Part III.A.

[9] *See* discussion *infra* Part III.B.

[10] *See* discussion *infra* Part III.B.

[11] *See* Doug Gross, *Social Networks and Kids: How Young is too Young?*, CNN ONLINE, Nov. 3, 2009, http://www.cnn.com/2009/TECH/11/02/kids.soc ial.networks/index.html. *See generally* Jennifer Wolcott, *A Year Later, Kids' Privacy Rule Still Debated*, CHRISTIAN SCI. MONITOR, Apr. 18, 2001 (discussing the practical effect of COPPA to encourage age falsification).

[12] Lance Whitney, *Nielsen: Kids' Online Time Leaps Dramatically*, CNET ONLINE, July 8, 2009, http://news.cnet.com/8301-10797_3-10281882-235.html.

[13] AMANDA LENHART ET. AL., PEW INTERNET & AM. LIFE PROJECT, TEENS AND SOCIAL MEDIA 3, 11, 44 (2007), *available at* http://www.pewinternet.org/Reports/2007/Teens-and-Social-Media.aspx.

[14] David Chartier, Teens on Social Networks Still Outrank Adults 2-1 (Jan. 15, 2009), http://arstechnica.com/web/news/2009/01/teens-on-social-networks-still-outrank-adults-2-1.ars.

[15] Press Release, Nat'l Ctr. Missing & Exploited Children, New Research Reveals Risky Internet Behavior Among Teens (May 7, 2007), *available at* http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=3

studies have found that up to a quarter of Internet users ages eight to twelve maintain social networking profiles.[16] Advocacy groups have expressed concern that children and adolescents' privacy rights are subject to abuse on social networking sites.[17] These concerns are compounded by the reality that many websites operate outside of COPPA regulations by making empty attempts to ban users under the age of thirteen.[18]

¶7 COPPA must be revised so that children, teenagers, and parents are provided adequate notice of the uses of personal information online (especially with regard to third parties) and a meaningful opportunity to consent to those practices. Reviewing COPPA through the lens of social networking sites, which dominate the interaction between today's young people and the Internet, shows that revisions are necessary to better protect the information of minors online, while balancing the interests of website operators as well.

¶8 In Part I, this Comment will review the methods of online data collection and the FTC's characterization of the specific risks towards children that led to the passage of the Children's Online Privacy Protection Act. Part II will review the specifics of the Children's Online Privacy Protection Act and Rule by discussing the legislative history and outlining specific objectives and aims by focusing on the statutory language. Part III of this Comment will review the criticism that COPPA has been subject to in recent years, and conclude that despite high-profile enforcement actions, COPPA has been largely unsuccessful at reaching its true aims. Part IV of this Comment will take a comprehensive look at how the Internet has changed since COPPA was enacted, and clarify the practice of behavioral targeting. In particular, Part IV will focus on the need for comprehensive online privacy protection for all adolescents, not just for those under the age of thirteen, by illustrating the privacy issues raised by the proliferation of social networking sites. Finally, Part V will examine proposed changes to online privacy laws and study proposals from children's advocacy groups and other commentators. This Comment will argue that an overhaul of COPPA is necessary and suggest provisions for a new policy so that privacy laws may become more effective in protecting today's children and adolescents online.

166.

[16] Children Signing Up for Under-Age Social Networking Profiles, http://www.ofcom.org.uk/consumer/2010/03/children-signing-up-for-under-age-social-networking-profiles/ (last visited Aug. 9, 2010).

[17] Letter from Angela J. Campbell & Coriell S. Wright, Georgetown Univ. Law Ctr. Inst. for Pub. Representation, to Donald S. Clark, Secretary, FTC (Apr. 11, 2008) [hereinafter Children's Group COPPA Letter 2008], *available at* http://www.democraticmedia.org/news_room/letters/Letter_re_behavioral_advertising_comments (explaining the practical effect of COPPA to encourage websites to simply ban users under the age of thirteen); *see* discussion *infra* Part III.C.

[18] Dorothy 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, 431–32 (2000).

I. DATA COLLECTION ONLINE AND THE ORIGINS OF COPPA

A. An Overview of Data Collection Online

¶9 There are two basic ways in which personal information is collected on the Internet: (1) a website user voluntarily submits information directly to a website, and (2) a website collects user information without the individual's knowledge.[19]

¶10 Voluntary submission to a website is the most straightforward way to share information online; a user provides an e-mail address, phone number, home address, or other personal information to a website, either for registration purposes or commercial activity.[20] The amount of information voluntarily submitted by users may encompass an even broader range of areas including hometowns, personal interests, favorite movies and television shows, educational background, even up to the minute information of a user's current whereabouts.[21]

¶11 The second category of information collection is more passive.[22] Technologies known as "cookies" permit website operators to track user's online activities outside of their own websites.[23] Cookies are small computer programs that are used by websites to store information such as username, passwords, and site preferences.[24] Once a cookie is on a user's hard drive, it essentially acts as an electronic tracking device, which keeps a record of every website a user visits and then provides that information to the original website that placed the cookie.[25]

¶12 Information is collected by websites in the form of cookies when users input information into search fields, and when users click on links and visit other websites, a practice referred to as "clickstream data."[26] Using these technologies, websites (or their advertisers) can learn much about their users, such as geographical location and Internet service provider, and can even learn of a user's interests and preferences by tracking web browsing patterns.[27] All Internet users (both children and adults alike) are vulnerable to passive data collection online, yet remain largely naïve as to how often it occurs.[28]

---

[19] *Id*.

[20] *Id*. at 431–32 ("[S]ometimes a user voluntarily discloses personal information to a Web site. For example, various Web sites require users to register in order to gain access or provide certain information in order to complete a purchase. Web site may also provide incentives to the user to provide personal information. Many users provide this information rather freely.").

[21] *See generally* Usha Munukutla-Parker, Comment, *Unsolicited Commercial E-mail, Privacy Concerns Related to Social Networking Services, Online Protection of Children and Cyberbulling*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 627, 634–65, 637–38 (2006) (providing an overview of the types of personal information collected on social networking websites).

[22] For a succinct description of how passive data collection and cookies work in practice, see *In re* DoubleClick Inc., 154 F. Supp. 2d 497, 502–03 (S.D.N.Y. 2001). *See also* Andrew Hotaling, Comment, *Protecting Personally Identifiable Information on the Internet: Notice and Consent the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 548–49 (2008).

[23] Hotaling, *supra* note 22, at 534–36.

[24] *Id*. at 534 n.32.

[25] Hertzel, *supra* note 18, at 431–32 ("By leaving an 'electronic marker' at each site or page that they visit, the user unknowingly provides information to the Web site that can be stored and reused. Unbeknownst to the user, a Web site can then 'know' [a] users' e-mail addresses, the names of their browsers, the type of computer they are using, and the universal resource locator (URL), or Internet address, of the site from which they linked to the current site.").

[26] Hotaling, *supra* note 22, at 534–35; *In re Doubleclick*, 154 F. Supp. 2d at 502–05.

[27] Hotaling, *supra* note 22, at 531–32.

[28] Hertzel, *supra* note 18, at 432.

B. Internet Privacy Concerns and Children: The Need for COPPA

¶13 In June 1998, a study was completed by the FTC that concluded by calling for greater incentives for self-regulation and better implementation of privacy policies among commercial websites.[29] In the study *Privacy Online: A Report to Congress*, the FTC outlined core traditional fair information principles, designed to ensure that collection, use, and dissemination of personal information are consistent with consumer interests.[30]

¶14 As summarized by the FTC, consumers must be given "*notice* of an entity's information practices[,] . . . *choice* with respect to the use and dissemination of information collected from or about them[,] . . . *access* to information about them collected and stored by an entity," and data collectors must "take appropriate steps to ensure the *security* and integrity of any information collected."[31] While the FTC was concerned about the mere collection of personal information online, their greater concern seemed to be *how* such information is used by websites after it is obtained.

¶15 The FTC found that based on the emergence of the online market as a powerful platform for commerce, Congress needed to take steps to protect consumer personal information from misuse by web operators.[32] In the late 1990s, electronic commerce was a booming industry; with the rise of the online market, the FTC expressed concern that websites would not adequately protect consumers' information to ensure privacy.[33] During the early years of e-commerce many consumers were wary of sharing private information online, especially given the risks of identity theft, fraud, or the unauthorized dissemination of private information to third parties.[34]

¶16 While adults were apprehensive about the security of their personal information online, such concerns were multiplied when it came to children and the Internet. According to 1997 census data estimates, 22.6% of children and adolescents ages three to seventeen had Internet access, and participated in a wide range of activities including video games, message boards, chat rooms, and interactive homework assistance.[35] The FTC found that children who went online were submitting personal information to websites in a wide range of capacities without the knowledge or approval of their parents.[36]

¶17 Even in 1997, the opportunities for children to share personal information online were vast. A child could voluntarily submit personal information to a website (for example, by registering for a contest or signing up for an e-mail "pen pal" service), or a child could reveal personal information by participating in an online chat room or interactive message board.[37] Additionally, a child could indirectly provide a website with personal information (such as web browsing practices) through the use of cookies.[38]

---

[29] PRIVACY ONLINE REPORT, *supra* note 2, at III.
[30] *Id.*
[31] *Id.* (emphasis added).
[32] *Id.* at 3; *see also* Children's Group COPPA Letter 2008, *supra* note 17.
[33] PRIVACY ONLINE REPORT, *supra* note 2, at 3.
[34] *Id.*
[35] U.S. CENSUS BUREAU, COMPUTER USE IN THE UNITED STATES: POPULATION CHARACTERISTICS 6 (1997), *available at* http://www.census.gov/prod/99pubs/p20-522.pdf; *see generally* PRIVACY ONLINE REPORT, *supra* note 2, at 12–13 (providing an overview of children's online behaviors).
[36] PRIVACY ONLINE REPORT, *supra* note 2, at 4–5.
[37] *Id.* at 4.
[38] *Id.* at 4–5.

¶18 The collection of personal information from children online presented serious and legitimate concerns because of: (1) "the vulnerability of children," (2) "the immediacy and ease with which information can be collected from them," and (3) "the ability of the online medium to circumvent the traditional gatekeeping role of the parent."[39] Primarily, the FTC was concerned with the safety risks that could arise from children sharing their personal information online. By 1997, the FBI and Department of Justice had begun to take a more proactive role in alerting the public to the risks of meeting sexual predators online.[40] An online chat room could be a great resource for a child seeking homework help or wishing to communicate with her peers, but could also serve as a place free of parental protection, providing opportunity for a child to give her personal information to a dangerous stranger.[41]

¶19 In addition to safety concerns, the FTC also was concerned with the collection of personal information from children by commercial websites seeking such information for marketing purposes.[42] Children traditionally are thought to lack the wherewithal to protect themselves against marketing abuses.[43] Studies have shown that children under the age of twelve often have difficulty distinguishing commercial speech from noncommercial speech.[44] For example, the FTC was concerned about a children's website asking for personal information as a prerequisite to playing an online game, or as part of an online contest. As such, a child would be likely to disclose information to websites, but lack the developmental capacity to fully understand the consequences of such disclosure, such as widespread dissemination to third party advertisers.[45]

¶20 Parents, in their traditional roles, can shield children from such harms; however, given the free-flow of information online, parents may have a more difficult time regulating children's behavior and protecting them from abusive marketing practices.[46] An FTC survey revealed that 97% of parents believe that a website should not have the power to sell their child's information to a third party, and 72% objected to the collection of their child's name or address in any capacity.[47]

¶21 In a comprehensive study of websites directed towards children, the FTC found that 89% of websites collected personal information directly from children, while a mere 10% of such sites offered any mechanisms for parental control over the collection and use of such information.[48] The FTC reviewed a sample of websites directed towards children, finding that sites were asking for children's e-mail addresses, home address, age, gender, hobbies, and other personal information, while only 48% disclosed their *uses* for such

---

[39] *Id.* "[Children's] status as a special, vulnerable group is premised on the belief that children lack the analytical abilities and judgment of adults. It is evidenced by an array of federal and state laws that protect children, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures, and make contracts with children voidable. In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize both the need for heightened protections for children and the special role that parents play in implementing these protections." *Id*. at 12.
[40] *Id.* at 5.
[41] *Id.*
[42] PRIVACY ONLINE REPORT, *supra* note 2, at 4–5.
[43] Children's Group COPPA Letter 2008, *supra* note 17.
[44] PRIVACY ONLINE REPORT, *supra* note 2, at 5.
[45] *Id.*
[46] *Id.*
[47] *Id.* at 6.
[48] *Id.* at 31–37.

information.[49] Further, only 1% of sites required a form of parental consent before information input.[50]

¶22 Based on these findings, the FTC recommended that Congress pass comprehensive legislation allowing for a greater parental control over the collection and dissemination of children's personal information.[51] Considering the principles of fair information practice, the FTC argued that it is a parent's role to have notice, access, and choice as to how their children's personal information is used and collected.[52] The FTC distinguished between children ages twelve and under and children over the age of twelve, reasoning that the former class would be particularly vulnerable to overreaching by online marketers and subject to graver safety risks.[53] In limiting the application of COPPA to children under the age of thirteen, the FTC argued that adolescents and other consumers could be protected from the misuse of personal information under the baseline powers of the Federal Trade Commission Act, which prohibits any "unfair or deceptive acts or practices in or affecting commerce."[54]

II. THE LAW ITSELF: WHAT IS COPPA AND WHAT DOES IT DO?

A. Authority from Congress: Children's Online Privacy Protection Act

¶23 In response to the FTC's Report, Congress introduced the Children's Online Privacy Protection Act in 1998, which granted the FTC the authority to create a rule responding to online privacy concerns that would give parents a greater role in the control of their children's personal information.[55] The Children Online Privacy Protection Act sought to address the FTC's concerns and requests in the Privacy Online report. As summarized by co-sponsor Senator Richard Bryan, the objectives of the Act were:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment;

---

[49] *Id.*
[50] *Id.*
[51] *Id*. at 12.
[52] *Id.*
[53] *Id*. at 46. The FTC argued that children and adolescents over the age of thirteen needed less formalized privacy protection; however, Congress' final COPPA Rule only granted protections for children under thirteen. *Id.*
[54] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (1961); Janine Hiller et al., *Pocket Protection*, 45 AM. BUS. L.J. 417, 429 (2008). The FTC originally suggested that the law apply in stages to children younger than seventeen, but backtracked on this position by the time COPPA was before Congress. Arguably, this illustrates at least an initial awareness by the FTC that its baseline provisions against deceptive practices did not directly address the specific problems of online privacy for both children and adolescents.
[55] 144 CONG. REC. S8482–83 (daily ed. July 1, 1998) (statement of Sen. Bryan) [hereinafter Sen. Bryan Statement] ("If a child answers a phone and starts answering questions, a parent automatically becomes suspicious and asks who they are talking to. When a child is on the Internet, parents often have no knowledge of whom their child is interacting. That is why we are introducing legislation that would require the FTC to come up with rules to govern these kind of activities."). As the FTC is an administrative agency, before it could implement a children's privacy protection law that carried the force and effect of law, Congress needed to pass a statute granting authority. Therefore, the Children's Online Privacy Protection Act is the delegation of authority from Congress, while the Children's Online Privacy Protection Rule is the actual FTC law under which enforcement actions are brought and fines for non-compliance may be levied. *See generally* Hiller et al., *supra* note 54, at 428.

> (2) to help protect the safety of children in online for a 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.[56]

¶24 The Act, which defines children as those under the age of thirteen, asks the FTC to implement a rule to protect privacy online in accordance with several key principals.[57] Owners of websites directed towards children are required to "provide *notice* on the website of what information is collected from children, how the operator *uses* such information, and the operator's *disclosure practices* for such information."[58]

¶25 In addition, Congress requires website owners to "obtain verifiable parental consent for the collection, use or disclosure of personal information from children."[59] Under the Act, the FTC is granted sole administration and enforcement powers.[60]

B. The FTC's Children's Online Privacy Protection Rule

¶26 Under the authority delegated by Congress, the FTC implemented the Children's Online Privacy Protection Rule, which became effective in April of 2000.[61] The Rule has many highlights that are necessary to review in order to fully comprehend its intended effect.

1. Defining "Personal Data"

¶27 First, the Rule defines the collection of personal data from children. Collection of data under the Rule includes data submitted directly by children from sources such as message boards and chat rooms as well as data received passively from devices such as online cookies.[62] Examples of personal information include first and last name, home address, e-mail or any other online contact information, phone number, social security number, or the combination of a photograph of an individual coupled with the person's last name.[63] The Rule also prohibits a website from selling, releasing, or in any way sharing personal information with a third party, and prohibits a website from making personal information collected from a child publicly available online.[64]

---

[56] *See* Sen. Bryan Statement, *supra* note 55; Danielle Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 154 (2001) (discussing legislative intent).
[57] 15 U.S.C.A § 6502 (2006).
[58] § 6502 (B)(1)(A)(i)–(ii) (emphasis added).
[59] § 6502 (B)(1)(A)(i)–(ii).
[60] 15 U.S.C.A. § 6505 (a) (2006).
[61] 16 C.F.R. § 312.2 (2009).
[62] § 312.2.
[63] § 312.2.
[64] § 312.2 (a)–(b).

2. Notice

¶28 The Rule requires a website to provide effective notice as to its data use and collection policies with regard to children, and outlines specifics as to when such notice will be deemed proper.[65] For example, such policies must be posted in links that are "clearly labeled" and placed in a "clear and prominent place and manner" on the home page.[66] The policy must contain information specifically stating the contact information of website operators collecting and maintaining information, whether the information is disclosed to third parties, and how such information is used.[67]

¶29 Additionally, adequate notice must contain the name, address, telephone number, and e-mail address of *all* operators collecting or maintaining personal information from children through the website.[68] The notice requirements also mandate that a website "make reasonable efforts, taking into account available technology" to inform parents of the content of any policies (however, the Rule does not suggest what methods might be adequate in practice).[69]

3. Verifiable Parental Consent

¶30 The crux of COPPA's protections is the requirement that website operators obtain "verifiable parental consent" before collecting information from children.[70] The Rule states: "An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children."[71]

¶31 The Rule outlines several proposed mechanisms for obtaining such consent, in light of available technology. Some suggested methods include: providing a consent form to be signed by parents and then returned to website operators by fax; requiring a parent to use a credit card in a transaction, with the reasoning that children under the age of thirteen do not have access to credit cards; having a parent call a toll-free number staffed by personnel trained to recognize voice difference between children and adults; and using digital certificates based on available technology to verify age.[72] The Rule creates an exception to parental consent in instances where a website operator is collecting personal information (such as an e-mail address) for the specific purpose of obtaining parental consent.[73]

¶32 Further, the Rule enacts what is referred to as a "sliding scale" of consent; that is, the efforts that website operators must take to ensure that parental consent is legitimate are proportional to the degree to which the personal information will be used.[74] Under

---

[65] 16 C.F.R. § 312.4 (b) (2010).
[66] § 312.4 (b)(1)(ii).
[67] § 312.4 (b)(1)(i)–(iii) (overview of proper placement of notice); § 312.4 (b)(2)(i)–(iii) (overview of content of proper notice).
[68] § 312.4 (b).
[69] § 312.4 (c).
[70] 16 C.F.R. § 312.5 (a) (2010).
[71] § 312.5(a)(1).
[72] § 312.5(b)(2).
[73] § 312.5(c)(1)–(4) (providing that other exceptions to parental consent include when purpose of collection is a one-time correspondence, and where the collection of such data may be necessary to protect child's safety).
[74] FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,908 (Nov. 3, 1999) (codified at 16 C.F.R. § 312).

this test, e-mail verification of parental consent is justified when the website operator does not provide information to third parties, but a "higher" method of consent (such as a print and mail form) would be necessary for activities that could pose a greater risk to children.[75] The FTC originally intended the "sliding scale" rule to act as a temporary measure until "secure electronic methods become more widely available" (which, as discussed below, was far too optimistic).[76]

¶33 The "sliding scale" addressed concerns over e-mail's viability as a means to obtain consent. While e-mail is certainly the most efficient and inexpensive means of obtaining consent, it is also the form most vulnerable to abuse or falsification.[77] At the time of the Rule's enactment in 2000, the FTC believed that technological advances would soon provide for more cost efficient methods of age-verification online.[78] The sliding scale was meant to serve as a temporary measure, which would be reviewed and overturned in a matter of years.[79]

4. Miscellaneous Provisions

¶34 The Rule grants parents the right to review any personal information submitted by their children and requires websites to comply with any requests to provide such information.[80] It also requires website operators to affirmatively establish procedures to protect the confidentiality of children's personal information collected.[81] The Rule explicitly prohibits a website from conditioning a child's participation in the activities of the site (for example, games, clubs, or contests) on providing more information than is reasonably necessary to engage in the activity.[82] In an effort to give websites additional incentives to comply with COPPA, the Rule outlines "safe harbor" provisions, where a website operator will be in compliance with COPPA if it follows approved industry guidelines for self-regulation.[83] Industry guidelines must be pre-approved by the FTC before receiving safe harbor protections.[84]

---

[75] FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,908.
[76] FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,908; *see infra* Part III.B.
[77] Hiller et al., *supra* note 54, at 434.
[78] *Id.*
[79] FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,888 ("A number of electronic products and services which could also be used to verify a parent's identity and obtain consent are currently available or under development.").
[80] 16 C.F.R. § 312.6 (2010).
[81] § 312.6(a)(1)–(3).
[82] 16 C.F.R. § 312.7 (2010).
[83] 16 C.F.R. § 312.10. In order to classify as a safe harbor, regulations must be approved by the FTC and are subjected to periodical reviews. *Id.* Currently, four organizations have received FTC safe harbor status under COPPA. FTC, Safe Harbor Program Application, http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html (last visited May 31, 2010).
[84] 16 C.F.R. § 312.10. Four organizations have been approved under this safe harbor provision: the Children's Advertising Review Unit, a subset of the Better Business Bureau; E.S.R.B. Privacy Online, part of the Entertainment Software Ratings Board; TRUSTe, an online privacy service; and Privo Inc., a similar privacy service. FTC, Safe Harbor Program Application, http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html (last visited May 31, 2010). To be approved by the FTC, participants must maintain self-regulatory guidelines including: (1) a requirement that participants in the safe harbor program implement substantially similar requirements that provide the same or greater protections for children as those contained in the Rule; (2) an effective, mandatory mechanism for the independent assessment of safe harbor program participants' compliance with the guidelines; and (3) effective incentives for safe harbor program participants' compliance with such guidelines. *See id.*

¶35 COPPA establishes an elaborate regulatory scheme, envisioning an Internet where websites directed towards children under the age of thirteen do not engage in any information collection practices without parental consent and involvement.[85] While it seeks to provide uniform guidelines as to the standards website operators must follow, the Rule leaves many questions unanswered. While COPPA is intended to apply only to websites "directed towards children," it does not attempt to define the term further. Website operators must determine for themselves whether or not they are likely to be found "directed towards children," and therefore whether they will be bound by COPPA's requirements.[86]

¶36 The Rule contemplates various methods for obtaining parental consent, but it does not state which method would be ideal, nor does it provide a way for websites to gauge if another standard would be sufficient.[87] On the surface, COPPA embodies the privacy scheme contemplated by the FTC—the burden of protecting children's personal information is seemingly shared between the website operators and parents. However, there have been significant discrepancies between the COPPA Rule's literal requirements and its enforcement and implementation in practice.[88]

III. ENFORCEMENT, REVIEW, AND CRITICISM OF COPPA IN PRACTICE

A. Noteworthy COPPA Enforcement Actions

¶37 Under the Children's Online Privacy Protection Act, Congress delegated all enforcement duties to the FTC, giving it the power to bring forward adjudicatory actions against websites and the power to levy fines for violations.[89] Since COPPA was enacted, there have been several high-profile enforcement actions against websites found in violation. A review of these enforcement actions demonstrates two key points. First, the FTC's strategy in seeking enforcement has shifted from targeting sites that were merely not compliant with COPPA to seeking enforcement against sites that attempted to meet COPPA's standards but were deemed ineffective. COPPA's statutory language makes predicting when such enforcements will be levied difficult for website providers. Second, COPPA enactments against social networking sites illustrate a double-bind for these websites when it comes to the problem of age-falsification, as both websites that ignore the reality of age-falsification and websites that acknowledge underage users face enforcement.

¶38 The first civil penalty cases under COPPA were settled in April 2001 against three website operators for failing to obtain parental consent before collecting personal information from children under the age of thirteen.[90] The defendant website operators

[85] *See* Hiller et al., *supra* note 54, at 442.
[86] Wolcott, *supra* note 11.
[87] Hiller et al., *supra* note 54, at 433.
[88] Anita Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 770 (2001); *see* discussion *infra* Part III.B.
[89] 15 U.S.C.A. § 6505(a) (2006) ("This chapter shall be enforced by the Commission under the Federal Trade Commission Act.").
[90] Press Release, FTC, FTC Announces Settlements with Web Sites That Collected Children's Personal Data Without Parental Permission (Apr. 19, 2001), *available at* http://www.ftc.gov/opa/2001/04/girlslife.shtm.

collectively ran the website Girlslife, a site targeted at girls ages nine to fourteen and offering pen pal opportunities, advice columns, online contests, and message boards.[91]

¶39 The FTC's enforcement against Girlslife focused on strict non-compliance with COPPA's provisions. The FTC found that the operators collected information from users under the age of twelve, such as their first and last names, e-mail addresses, and telephone numbers, without obtaining parental consent.[92] Further, site operators failed to provide notification of their collection practices, and sold the personal information of underage children to third parties without notice or obtaining parental consent.[93]

¶40 In the next wave of COPPA enforcement, websites that attempted to comply with COPPA were targeted for ineffectively implementing its provisions. In 2003, the FTC levied civil penalties of $100,000 and $85,000 against Mrs. Fields Cookies and Hershey's Foods, respectively, for COPPA violations.[94] The enforcement action against Hershey's marked the first time the FTC deemed a website's methods of obtaining parental consent insufficient, finding that Hershey's method of obtaining consent was not "reasonably calculated to ensure that the person providing consent was the child's parent."[95] Hershey's had instructed children under the age of thirteen to have their parents fill out an online consent form, but took no extra measures to verify that a parent had actually completed the form.[96]

¶41 In September 2006, the FTC settled with UMG Recordings for a civil penalty of $400,000 for collecting personal information on children under the age of thirteen, and additionally for failing to maintain an adequate privacy policy.[97] UMG requested users' birthdays before allowing them to enter the website, but did not take any steps to secure parental consent when users indicated they were under the age of thirteen.[98] UMG then collected personal information from users including full name, birthday, home address, and e-mail address despite having actual knowledge that some users were under thirteen and therefore entitled to COPPA protections.[99] The enforcements against Hershey's and UMG illustrate the difficulty for website providers in interpreting COPPA's vague statutory requirements as to what actually constitutes sufficient parental consent.

¶42 In recent years, the FTC has targeted social networking sites for COPPA violations. In September 2006, the FTC brought an enforcement action against the social networking

---

[91] *Id*.
[92] *Id*.
[93] *Id*. In 2001, enforcement actions were taken against Lisa Frank Inc., which collected addresses and phone numbers from girls under the age of twelve without parental consent, and against the website Jollytime, which collected e-mail addresses and home addresses from children under the age of thirteen and failed to obtain parental consent despite a stated privacy policy which claimed otherwise. Press Release, FTC, Web Site Targeting Girls Settles FTC Privacy Charges (Oct. 2, 2001), *available at* http://www.ftc.gov/opa/2001/10/lisafrank.shtm; Press Release, FTC, Popcorn Company Settles FTC Privacy Violation Charges (Feb. 14, 2002), *available at* http://www.ftc.gov/opa/2002/02/popcorn.shtm.
[94] Press Release, FTC, FTC Receives Largest COPPA Civil Penalties to Date in Settlements with Mrs. Fields Cookies and Hershey Foods (Feb. 27, 2007), *available at* www.ftc.gov/opa/2003/02/hersheyfield.shtm.
[95] *Id*.
[96] *Id*.
[97] Press Release, FTC, UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. to Pay $75,000 to Settle COPPA Civil Penalty Charges (Sept. 13, 2006), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm.
[98] *Id*.
[99] *Id*.

website Xanga for $1 million in civil penalties—the largest COPPA fine to date.[100] According to the FTC's complaint, Xanga allowed users under the age of thirteen to create profiles containing large amounts of personal information without first obtaining verifiable parental consent.[101] New users to Xanga seeking to create an account were prompted to check a box indicating whether or not they were over the age of thirteen.[102] Users under the age of thirteen received a message stating to "come back on your thirteenth birthday," while users who did not initially check the box received a message stating, "[y]ou must check the box below to certify you are at least thirteen years old."[103] An estimated 1.7 million users under the age of thirteen created user accounts on Xanga by checking the over thirteen box following this prompt.[104]

¶43 The FTC found Xanga in violation of COPPA for obtaining user information from these accounts without any efforts to obtain parental consent and for specifically using the information in underage accounts to tailor advertisements.[105] The FTC found Xanga's attempt to screen out underage users inadequate, and, therefore, many children under thirteen were allowed to submit personal information without parental consent.[106] In addition to the $1 million civil penalty, the FTC's enforcement action required Xanga to provide links to FTC consumer education materials and to publish FTC safety tips for social networking.[107]

¶44 In January 2008, the FTC charged the social networking site Imbee.com with COPPA violations.[108] Imbee was promoted as a social networking website specifically designed for kids ages eight to fourteen.[109] According to the FTC, Imbee enabled more than 10,500 children to create Imbee websites without properly obtaining parental consent.[110] The website collected a parent's e-mail address, and would not complete the registration of the children's profile without consent.[111] However, if the parent did not respond to the registration request, Imbee would not delete previously obtained children's information.[112] The FTC charged Imbee a $130,000 civil penalty for its COPPA infractions.[113]

---

[100] Press Release, FTC, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule (Sept. 7, 2006) [hereinafter FTC Xanga Enforcement], *available at* http://www.ftc.gov/opa/2006/09/xanga.shtm.
[101] Complaint of FTC at 5–6, United States v. Xanga.com, Inc., No. 06-6853 (S.D.N.Y. 2006), *available at* http://www.ftc.gov/os/caselist/0623073/060907xangacomplaint.pdf.
[102] *Id*.
[103] FTC Xanga Enforcement, *supra* note 100; Complaint of FTC at 6, United States v. Xanga.com, Inc., No. 06-6853 (S.D.N.Y. 2006), *available at* http://www.ftc.gov/os/caselist/0623073/060907xangacomplaint.pdf.
[104] *Id*.
[105] Complaint of FTC at 7–8, United States v. Xanga.com, Inc., No. 06-6853 (S.D.N.Y. 2006), *available at* http://www.ftc.gov/os/caselist/0623073/060907xangacomplaint.pdf.
[106] *Id*.
[107] *Id*.
[108] Press Release, FTC, Imbee.com Settles FTC Charges Social Networking Site for Kids Violated the Children's Online Privacy Protection Act; Settlement Includes $130,000 Civil Penalty (Jan. 8, 2008) [hereinafter Imbee Settlement], *available at* http://www.ftc.gov/opa/2008/01/imbee.shtm.
[109] *Id*.
[110] *Id*.
[111] *Id*.
[112] *Id*.
[113] *Id*.

¶45 The Imbee and Xanga enforcement actions prove the difficulty for a website to ensure complete COPPA compliance. The nature of these COPPA enforcements makes it even harder for websites to predict when measures to ensure age verification will be adequate under COPPA. Xanga's efforts to screen out users under the age of thirteen were deemed ineffective, and yet when Imbee attempted to create a social networking safe haven for children under the age of thirteen, rather than promote age falsification, its efforts were also condemned by the FTC. These enactments against social networking sites seemingly create a double-bind: a website who fails to verify users' ages will be held liable, while a website which seeks to embrace the challenges of age-verification, like Imbee, will also be held liable. Thus, the FTC's main enforcement actions against COPPA undermine confidence in the stability and predictability of its provisions rather than provide clear illustrations of when a violation has occurred.

B. Criticism & FTC Reviews

¶46 Following the passage of COPPA legislation and the implementation of the FTC's Rule, initial reactions to the law were optimistic and COPPA was hailed as a positive step towards protecting children's privacy interests online.[114] COPPA was praised for creating uniform legal standards for websites to adhere to and for bringing the concerns of children online to national attention.[115] In 2001, one commentator went so far as to proclaim: "[M]ost 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."[116]

¶47 Despite the optimistic outlook for COPPA, criticism began soon after the Rule was enacted. Smaller websites began to feel the increased burden of COPPA compliance, as separate costs were required to hire legal teams to write expansive privacy polices, and to enforce privacy requirements in chat rooms and message boards.[117] Given COPPA's virtual silence on the definition of a website "directed towards children," web operators had to judge for themselves whether or not they should comply with COPPA, or ignore its regulations and risk an enforcement action.[118] Some sites opted to cut out these services that could draw the attention of children, estimating that the total cost of COPPA compliance could reach upwards of $200,000 per year.[119] Some consumer protection and business leaders questioned the true effect of the COPPA age requirement. Jonathan Zuck, the president of the Association on Competitive Technology, a small business interest group, testified to Congress in early 2001 regarding COPPA's weaknesses, stating: "[W]e all agree with the goal of protecting kids, but that hasn't been the net

[114] Garber, *supra* note 56, at 165.
[115] *Id*.
[116] *Id*.
[117] Wolcott, *supra* note 11.
[118] *Id*. The challenges for websites in interpreting "directed towards children" as a statutory provision are highlighted even further by enforcement actions, such as those against UMG that illustrate how websites can be held liable for a misinterpretation of COPPA's language.
[119] Wolcott, *supra* note 11; *see also* Hiller et al., *supra* note 54, at 442. Initial criticisms of COPPA predicted that websites would close their doors to children under the age of thirteen because of the challenges of COPPA compliance, and the financial burden of obtaining parental consent. *Id*.

result. . . . Kids are just lying about their age on adult sites. I'm not sure that's a net positive."[120]

¶48 In addition to problems of age falsification, another persistent concern was whether or not such regulations would serve to restrict children's ability to use the Internet as an educational and functional tool.[121] A child's ability to freely explore online could be hampered by the need to obtain parental consent every time a website asked for personal information or preferences.[122] For example, resources like homework help, live chats, games, and educational materials tailored to personal preferences might be removed for a site seeking to achieve COPPA compliance. Conversely, websites had an incentive to remove content for children in order to avoid the financial burden of COPPA compliance.[123]

¶49 In the Children's Online Privacy Protection Act, Congress requires that the FTC conduct regular reviews of COPPA's implementation and compliance.[124] In 2002, the FTC concluded its first systematic review, finding that certain aspects of COPPA were initially more successful than others.[125] According to the review, COPPA had increased the number of children's websites providing privacy policies explaining to children and parents whether the site collected personal information, and how such information was used.[126] The FTC found that close to 90% of children's websites now made such policies available, as opposed to only 10% before COPPA's enactment—illustrating that the "notice" element of Fair Information Use practices had greatly improved.[127] Additionally, 45% of websites surveyed obtained a parent's e-mail address for purposes of consent, indicating a legitimate effort by websites to obtain verifiable parental consent through e-mail mechanisms, rather than an online consent form which is easier for children to forge.[128]

¶50 In this first report, the FTC admitted the limitations of its survey, noting that while some violations of COPPA can be ascertained from a surface view of the website, true compliance is best measured though an investigation of each site's individual practices.[129] Additionally, the FTC's first review only examined the practices of websites clearly "directed to children," but ignored websites which may not obviously target children, but that may nonetheless have collected personal information from children under the age of

---

[120] Wolcott, *supra* note 11.
[121] *See* Allen, *supra* note 88, at 769 (noting that the burden of parental consent may hinder children's ability to fully engage in the educational and entertainment aspects of the Internet).
[122] Leslie Harris, *MySpace Coming of Age for Age*, ABC NEWS ONLINE, Feb. 28, 2008, http://abcnews.go.com/Technology/Story?id=4355851&page=1.
[123] *Id*.
[124] 15 U.S.C.A. § 6506 (2006).
[125] FTC, STAFF REPORT, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 9 (Apr. 2002) [hereinafter FTC COPPA ONE YEAR REPORT], *available at* www.ftc.gov/os/2002/04/coppasurvey.pdf; *but see* Hiller et al., *supra* note 54, at 436 (describing that acceptance of verification technologies hindered the ability of COPPA to adequately protect children online).
[126] FTC COPPA ONE YEAR REPORT, *supra* note 125, at 9.
[127] *Id*.
[128] *Id*. at 4. However, the possibility remains that children might create false e-mail accounts and pretend to be their parents to grant consent. *See* BILL CARMODY, ONLINE PROMOTIONS: WINNING STRATEGIES AND TACTICS 104–05 (2001).
[129] FTC COPPA ONE YEAR REPORT, *supra* note 125, at 4.

twelve.[130] As discussed above, the statutory language of COPPA fails to clearly define what constitutes a website "directed to children." By studying only websites clearly for children, the FTC failed to consider the data collection practices of websites in the gray zone where COPPA violations could still occur.

¶51 The FTC's ever-changing attitude towards the "sliding scale" rule illustrates the difference between COPPA's requirements in theory and in practice. The sliding scale provision of COPPA was envisioned as a temporary guideline for obtaining parental consent until more secure electronic means were developed.[131] However, in the years following the passage of COPPA, the FTC's hope that the sliding scale would be replaced with more reliable electronic means of parental consent has been unrealized.[132] During a 2002 survey of COPPA compliance, the FTC requested comments from website operators and other interested parties on the issue of extending the duration of the sliding scale rule.[133] A wide range of interest groups—from advertising and marketing firms, to educational groups and internet services providers—took part in the comment, and generally all supported the extension of the sliding scale rule.[134] AOL Time Warner, arguing that the sliding scale not only be extended two years, but extended indefinitely, wrote of verification technology: "The promise of new digital signature technologies remains largely that—a promise."[135]

¶52 Other comments focused on the cost of eliminating the use of e-mail as acceptable parental consent, arguing that any alternative verification systems would be too expensive, and observing that even for adult websites, the use of digital verification technology is scarce.[136] Some commentators expressed an opposite view, worrying that by continuing to extend the sliding scale, organizations would not have the motivation to invest in technological advancements, and instead be content to rely on e-mail verification.[137] The FTC agreed with the majority of comments and approved a three-year extension of the sliding scale rule until its next review in 2005.[138]

¶53 Three years later, age verification technology still had not advanced in the manner envisioned by COPPA's drafters. During the required compliance review in 2005, the FTC concluded that COPPA was a generally successful mechanism for improving

---

[130] *Id.*

[131] *See* FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,908 (Nov. 3, 1999) (codified at 16 C.F.R. § 312).

[132] Hiller et al., *supra* note 54, at 436.

[133] *See* FTC, Children's Online Privacy Protection Rule, Public Comments Received 2002, http://www.ftc.gov/privacy/coppa2/comments/index.html [hereinafter Public Comments 2002] (last visted Sept. 1, 2010); *see also* Hiller et al., *supra* note 54, at 437.

[134] Public Comments 2002, *supra* note 133.

[135] Comments of AOL Time Warner et al., Children's Online Privacy Protection Rule Amendment—Comment P994504 (Nov. 30, 2000), *available at* http://www.ftc.gov/privacy/coppa2/comments/aol.htm.

[136] Letter from David Medine, Online Privacy Alliance, to Donald Clark, Secretary, FTC (Nov. 19, 2001), *available at* http://www.ftc.gov/privacy/coppa2/comments/opa.htm ("In many instances, the added burdens and costs imposed by the phase out of the sliding scale would cause some sites to cease interactions with children and possibly go out of business because the alternative verification mechanisms are too costly.").

[137] Letter from Rebecca Richards, TRUSTe, to Secretary, FTC (Nov. 30, 2001), *available at* http://www.ftc.gov/privacy/coppa2/comments/truste.htm ("Choosing to extend the compliance date every two years because new technological solutions have not been widely adopted, [sic] is likely to create a regulatory environment that does not place pressure or give incentive to companies to invest and use such systems.").

[138] Children's Online Privacy Protection Rule, 67 Fed. Reg. 18,818, 18,820 (Apr. 17, 2002), *available at* 2002 WL 560760 (F.R.).

children's privacy online.[139] However, in addressing the effectiveness of parental consent mechanisms, the FTC conceded that the views of most commentators were correct: "[S]ecure electronic mechanisms have not developed to the point where they are widely available and affordable."[140] The FTC decided to extend the sliding scale approach indefinitely, admitting that verification technology was still inadequate.[141] The full time adoption of the sliding scale rule illustrates that the other methods of parental consent contemplated by COPPA (print and mail forms, faxing signatures, and telephone hotlines) were not viable or cost effective options.

¶54 In 2007, the most recent review of COPPA, the FTC concluded that the Act and Rule were "effective in helping protect the privacy and safety of young children online[,]" and did not recommend any changes to the core of COPPA's framework.[142] While remaining optimistic about the general workings of COPPA, the 2007 report did concede several significant weaknesses.[143] For instance, the FTC acknowledged the limitation inherent in COPPA's application only to websites "directed to children," expressing concern that general audience websites may still be collecting information from children under the age of thirteen.[144]

¶55 The 2007 report continued to acknowledge the lack of technology providing a plausible means of age verification.[145] As one commentator noted, "[T]here is no conceivable way, short of locking a child in a closet and not letting him out until adulthood, to absolutely prevent a child from viewing age inappropriate websites."[146] With respects to age verification, there is similarly no absolute way of ensuring that children will not lie on registration forms to certain websites.[147] Instead, the FTC advised websites to check for age information "in a way that does not bias the result," such as not

---

[139] *See* Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247, 13,258 (Mar. 15, 2006) (concluding that COPPA would be left unmodified). For a list of the organizations who participated in the comment period, highlighting the breadth of commentary on the issue, see FTC, Children's Online Privacy Protection Rule, Public Comments Received 2005, http://www.ftc.gov/os/comments/COPPARuleAmmend/Index.htm (last visited Aug. 9, 2010).

[140] Children's Online Privacy Protection Rule, 71 Fed. Reg. at 13,255.

[141] Children's Online Privacy Protection Rule, 71 Fed. Reg. at 13,255.

[142] FTC, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS 1 (Feb. 2007) [hereinafter FTC COPPA 2007 REPORT], *available at* www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[143] *Id*.

[144] *Id*. at 12.

[145] *Id.*; *see also* Letter from Daniel Popeo et al., Wash. Legal Found., to Secretary, FTC 5 (June 27, 2006) [hereinafter Washington Legal Foundation Letter], *available at* http://www.ftc.gov/os/comments/COPPArulereview/516296-00027.pdf (noting how children can simply use the "back" button on browsers to re-enter ages if they are denied initial access).

[146] Washington Legal Foundation Letter, *supra* note 145.

[147] In the area of pornography, perhaps the one area of the Internet where age verification is effective, children are kept off websites because of a requirement that the user enter valid credit card information. The assumption is that anyone old enough to hold a credit card is likely old enough to view pornography. In the realm of children online, however, the use of credit cards for age verification is likely too burdensome to be effective. While it is not a burden for an adult seeking pornography to use his or her credit card to access a single site, using credit cards for COPPA verification would require parents to constantly verify their children's Internet usage on a myriad of websites. The alternative—that children would simply lie about their age in order to avoid this burden—would be the likely outcome of this approach. *See* Amit Asaravala, *Why Online Age Checks Don't Work*, WIRED ONLINE, Oct. 10, 2002, http://www.wired.com/politics/law/ news/2002/10/55338.

making it clear on a log-in page that thirteen is the permitted age and ensuring that drop down menus for birthdays cover all ages rather than just thirteen and up.[148]

¶56 In 2007, the FTC recognized the challenges faced with the rise of social networking sites—a move which was significant, but long overdue. Recognizing the growing popularity of social networking, the report states:

> While social networking websites offer the potential for online communication, camaraderie, and a sense of community among teens and tweens, they also pose substantial risks because the information that children post on their online journals or blogs may be accessed by other Internet users, social networking websites have become a matter of public concern.[149]

¶57 The FTC has additionally responded to the concerns of social networking sites by posting best practice educational materials on its website to inform children, teens, and parents of the possible privacy risks of using such sites.[150] The FTC also emphasized that COPPA still applies to such websites that knowingly collect information from children under the age of thirteen. The FTC highlighted the 2006 enforcement action against Xanga as sending a strong message to social networking sites to ensure COPPA compliance.[151]

C. COPPA Today

¶58 While the FTC praises the few, but important, benefits of COPPA, it ignores growing online dangers to children's privacy posed by social networking. Ten years after COPPA's passage, and bearing in mind the changed landscape of the Internet among teens and adolescents, many critics do not share this sense of optimism. The permanent extension of the sliding scale rule indicates that technological advancements have not evolved in the manner originally envisioned by COPPA.[152] As such, e-mail remains the only viable means for parental consent, which is highly vulnerable to circumvention.[153]

¶59 Furthermore, the line between a website "directed towards children" and a general audience website has blurred. One of the practical effects of COPPA has been that websites now often use age-screening methods to prohibit users under the age of

---

[148] FTC COPPA 2007 REPORT, *supra* note 142, at 26 (encouraging websites to use "cookies", a tracking device, to prevent children from going back one page to change their birthday once they realize a website is blocked).
[149] *Id.* at 25.
[150] Hiller et al., *supra* note 54, at 440.
[151] FTC Xanga Enforcement, *supra* note 100; *see also* FTC COPPA 2007 REPORT, *supra* note 142, at 29–20 (explaining that the FTC also explored the emerging issue of the Internet on mobile devices, noting that COPPA compliance is still required as marketers anticipate that mobile Internet access for children is expected to rise).
[152] Hiller et al., *supra* note 54, at 438.
[153] *Id.* at 444 ("If COPPA is to protect children online by means of parental involvement, then new tools are needed to assist them, technical methods that will empower parents to assert control over Web site practices, and even their own, technically sophisticated children."); *see also* DAN ALBAN, COMPETITIVE ENTERPRISE INST., A FREE-MARKET GUIDE TO NAVIGATING TECH ISSUES IN THE 107TH CONGRESS: COPPA AND ON-LINE PRIVACY FOR CHILDREN 73 (2002), *available at* http://cei.org/PDFs/COPA_and_Internet_Content_Regulation.pdf.

twelve.[154] These screening methods are technologically ineffective, as computer-savvy children often know how to circumvent these attempted roadblocks.[155] The ease of age falsification leads to a situation where children may share personal information on a website which seeks to operate outside of COPPA restrictions because it "officially" doesn't allow underage users.

¶60 The FTC has recognized the problems with age verification and the technological weakness of electronic parental consent. In this view, COPPA does not operate as the most effective mechanism to protect children's online privacy rights, but rather encourages websites to limit the Internet resources available to young persons by imposing largely unenforceable age restrictions on websites.[156] The FTC recognizes that the rise of social networking sites is the changing Internet landscape, but admits that nothing but inadequate age screening mechanisms serve to prevent children from registering on such sites.[157]

¶61 When the FTC addressed the rise of social networking sites as an emerging issue, the Commission only skimmed the surface of the possible privacy challenges that lie ahead. Given the popularity of social networking sites and their potential privacy risks, advocacy groups have recently begun to call for an overhaul of COPPA. In an April 2008 letter to the FTC, advocacy groups including the American Academy of Pediatrics, Children Now, and the Center for Digital Democracy called upon the FTC to expand privacy rights to a class they believe COPPA ignores—the thirteen to seventeen age demographic.[158] Aside from COPPA, there are no other Internet-specific privacy laws, and ignorance of the adolescent demographic is gaining support as one of the biggest weaknesses of COPPA.[159]

¶62 Before a meaningful recommendation of revisions to COPPA can be addressed, it is necessary to review how the collection and use of personal information online has changed and grown in the ten years since the FTC first addressed privacy challenges of children. Specifically, it is important to discuss the privacy threats to adolescents and the rise of social networking sites.

IV. CURRENT INTERNET PRIVACY CONCERNS

A. The Use of Personal Information Online: Then & Now

¶63 The opportunities for individuals to share personal information over the Internet have expanded exponentially in the years since Congress passed COPPA. In 1997, the

---

[154] Wolcott, *supra* note 11.
[155] *See* FTC Xanga Enforcement, *supra* note 100 (finding Xanga's age screening attempts insufficient under COPPA).
[156] Joshua Warmun, Note, *Can Coppa Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, 216 (2000) ("Although well-meaning, COPPA raises too many problems to be a truly effective mechanism to protect children's online privacy interests.").
[157] *Id*.
[158] Children's Group COPPA Letter 2008, *supra* note 17; *see also* Stefanie Olsen, Group calls for teen privacy protections on Facebook, MySpace, http://news.cnet.com/8301-10784_3-9915769-7.html (Apr. 9, 2008, 17:44 PDT). In 2008, New Jersey legislatures introduced bills to extend the privacy protections of COPPA to children between the ages of thirteen and eighteen. *See* Jane Coviello, *Internet Safety: Legislative Initiatives for our Protection*, N.J. LAW. MAG., Dec. 2008, at 57.
[159] Hotaling, *supra* note 22, at 560.

FTC mostly concerned itself with the risks of children voluntarily submitting their personal information to website operators, chat rooms, and message boards.[160] During the past thirteen years, however, website operators have significantly increased their use of passive methods of data collection. More websites now use cookies or similar technologies to store user preferences and argue that such practices help consumers by making Internet use more convenient and efficient.[161]

¶64 Today, one of the most prevalent uses of personal information online is a web operator's ability to create effective and targeted advertising.[162] Online advertising has grown to a nearly ten billion dollar industry in recent years.[163] By using personal information gathered online, marketers can effectively target audiences based on interests, demographics, and any other factor about a person that can be ascertained from web history and online behavior.[164]

¶65 Known as "behavioral targeting," online advertisers target consumers by analyzing information collected through cookies, clickstream data, and voluntary information submission to create web advertisements that best match an individual web user's interests.[165] This highly effective mechanism is certainly beneficial for web operators and advertisers, and arguably for consumers as well (individuals likely prefer marketing for goods and services that they have an interest in).[166] The largest commercial companies online utilize behavioral targeting methods in their advertising—in 2007, Internet companies invested over $575 million in behavioral targeting.[167] Some privacy advocates question if the FTC enforces COPPA aggressively enough when it comes to behavioral targeting practices.[168]

¶66 A large percent of Americans remain largely ignorant of the extent that behavioral targeting occurs online. According to as study by the Consumer Reports National Research Center, fifty-seven percent of Web users "mistakenly believe that before monitoring their online browsing, companies are legally required to identify themselves, spell out why they're collecting data and who they intend to share it with."[169] Sixty-one percent of those surveyed believe that online activities are "private and not shared without their permission."[170] Forty-three percent of users incorrectly believe that a court order is required to monitor Web-browsing activities.[171] These statistics demonstrate the ignorance of information collection practices, not just among children and adolescents, but the population on the whole.

---

[160] *See* discussion *supra* Part I.B.
[161] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 565 (2008).
[162] Hotaling, *supra* note 22, at 537.
[163] *See 100 Leading National Advertisers*, ADVERTISING AGE, June 25, 2007, *available at* http://adage.com/images/random/lna2007.pdf (see pie chart on page 7 describing $150 billion in spending by type of advertising media).
[164] Hotaling, *supra* note 22, at 537.
[165] *Id*.
[166] Ciocchetti, *supra* note 161, at 568.
[167] *Id*. at 569–70.
[168] Heather Osborn Ng, *Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware*, 31 HASTINGS COMM. & ENT. L.J. 369, 380–81 (2009).
[169] Andy Greenburg, *Not as Private as You Think*, FORBES ONLINE, Sept. 25, 2008, http://www.forbes.com/2008/09/25/online-privacy-protection-tech-security-cx_ag_0925privacy.html.
[170] *Id*.
[171] *Id*.

¶67 Internet providers and website operators argue that personal information for the use of behavioral targeting ads is a necessary predicate to useful, free Internet services.[172] Websites generate profits and cover costs of operation through such advertisements, and as such are able to operate such sites free of cost.[173] Surveys have shown that consumers enjoy the value of the benefits of free sites (Facebook and MySpace are free to users, as are other interactive sites like YouTube and Wikipedia), and are willing to allow the use of personal information as the "price" of such use.[174] The flaw in this reasoning, however, is that consumers are unaware of the broad and sweeping control that a website may have over their personal information.[175] Under ideal circumstances, Internet users of free websites would be fully informed of the extent to which their personal information is being used. With this full knowledge would come the appropriate consent to accept this use as the "price" of a free Internet. Without such meaningful consent, however, websites are able to exploit the ignorance under a guise of "it's the cost of doing business." Bearing in mind the FTC's four principles of fair information use—notice, choice, access, and security—meaningful consent cannot be achieved without first providing consumers with meaningful notice.

B. Privacy Concerns Specific to Teens

¶68 As COPPA protections only extend to children under the age of thirteen, websites that are directed towards adolescents are not subject to the rigors of COPPA enforcement. As the FTC stated back in 1997, children do not possess the cognitive powers to distinguish commercial speech or possess the ability to meaningfully consent to the distribution and use of their personal information.[176] A key goal of COPPA from the onset sought to return this power of consent to parents rather than children.[177]

¶69 However, teenagers are vulnerable to information misuse, sometimes even more so than young children. Teenagers face peer pressures to join social networking sites, and therefore such websites have increasingly become part of an adolescent's social identity.[178] As such, teenagers like to interact online and share personal information through social networking sites.[179] As more adolescents seek out identity formation on the Internet, it becomes incredibly difficult for them to resist the peer pressure to interact online and divulge personal information.[180]

¶70 Additionally, adolescents are typically viewed as prone to experimentation and risk-taking, which makes it difficult for parents, educators, and website operators to help teens remain aware of the potential misuse of personal information that they share online.[181] Especially with regard to behavioral targeting, commentators argue that

---

[172] Ciocchetti, *supra* note 161, at 571 ("These beneficial services do come at a cost, however, as companies tend to predicate participation upon an exchange for an individual's [personal information].").
[173] *Id*. at 570–71.
[174] *Id*.
[175] *See* discussion *infra* Part IV.D (describing how Facebook users waged a "Quit Facebook" campaign in the Spring of 2010 upon learning of privacy rights violations).
[176] *See supra* Part II.B.
[177] *See supra* Part II.B.
[178] Children's Group COPPA Letter 2008, *supra* note 17, at 6–8.
[179] *Id*.
[180] *Id*.
[181] *Id*.

teenagers are "less likely than adults to understand the long term consequences of sharing personal information online for tracking."[182] Additionally, some argue that teens might be "more susceptible to targeted advertisements that are tailored to their psychological weaknesses."[183]

¶71 Furthermore, a discussion of the risks of data collection online would be incomplete without touching upon the many safety considerations that are raised when children and teens share too much of their personal life online. The many unfortunate examples of teenagers manipulated into disclosing personal information to strangers online, and subsequently suffering harm, provide further support for frequent teenager ignorance of the dangers of providing personal information online.[184] Concerns over sexual predators, online harassment, and cyber bullying can arise when teenagers allow the collection of their personal data online without regard to the possible consequences.[185] While revised COPPA provisions would not even attempt to directly resolve all these sensitive problems, new provisions requiring more adequate notice and better informed consent to the dissemination of personal information may make adolescents more cognizant of the risks online.

C. Illustrating the Need for Change: Facebook

¶72 As previously mentioned, outside of COPPA regulations, the only mechanism to protect Internet users from misuse of personal information online is section 5 of the FTC regulation against "unfair or deceptive acts or practices in or affecting commerce."[186] Therefore, websites that are not "directed towards children" (an ambiguous term at best) are not required to follow specific practices regarding the collection and dissemination of personal information.

¶73 However, as the FTC's enforcement action against Xanga and Imbee.com prove, social networking websites are considered "directed towards children" under the age of thirteen in addition to teenage and adult demographics.[187] The ease of age falsification online and the vulnerabilities of children and adolescents to personal information misuse warrant an examination of such websites' privacy practices.

¶74 Facebook's privacy practices provide a useful example of online networking practices both because of the sites immense popularity and because its practices have been both praised and criticized.[188] Launched in 2004, Facebook.com has over 500

---

[182] Ng, *supra* note 168, at 380–81.
[183] *Id.*
[184] *See, e.g.*, Christopher Maag, *When the Bullies Turned Faceless*, N.Y. TIMES, Dec. 16, 2007, at 9 (describing the case of teenaged girl who committed suicide after a Myspace acquaintance engaged in online bullying and manipulation).
[185] BERKMAN CTR. INTERNET & SOC'Y, HARVARD UNIV., ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES 4–5 (2008), *available at* http://cyber.law.harvard.edu/pubrelease/isttf/.
[186] 15 U.S.C. § 45(a)(1) (2006).
[187] FTC Xanga Enforcement, *supra* note 100.
[188] Ciocchetti, *supra* note 161, at 601; *compare id., with* Kevin Bankston, Facebook's New Privacy Improvements are a Positive Step, But There is Still More Work to be Done (May, 26 2010), http://www.eff.org/deeplinks/2010/05/facebooks-new-privacy-improvements-are-positive ("All of the new settings are positive steps towards giving Facebook users more control over the privacy of their data."), *and* Letter from Philippa Lawson, Director, Can. Internet Pol'y & Pub. Interest Clinic, to Commissioner Stoddart, Privacy Comm'r Can. 1 (May 30, 2008) [hereinafter Canada Facebook Complaint], *available at* www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf ("[Facebook is] failing to: identify all

million active users as of August 2010.[189] Initially limited to college users, Facebook eventually opened up to any users thirteen and older.[190] Facebook is currently the second most popular website in the world, second only to Google.[191] Facebook offers opportunities to voluntarily share personal information through user profiles. Users on Facebook share a wide range of personal information, including e-mail address, interests, geographic location, information about acquaintances, favorite websites, music, phone numbers, and photographs.[192] In fact, more than 3.5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared on Facebook each week.[193]

¶75 Like most social networking websites, Facebook uses advertising to generate revenues. According to estimates, Facebook generated $500 million in advertising revenues in 2009.[194] Facebook "Social Ads" target specific demographics based on the information in user profiles.[195] While users on Facebook have great control as to the degree of personal information they wish to share with other Facebook users, Facebook's privacy mechanisms don't allow users control over the use of their information by advertisers. Facebook does not permit users to opt-out of advertisements completely.[196] Such a decision may reflect the theory that the behavioral targeting methods employed by Facebook are part of the "cost" of getting the benefits of Facebook.

¶76 Facebook maintains a privacy policy as a component of its Terms of Service agreement (TOS), which seeks to give notice to users regarding such advertising practices. The policy is comprehensive, and can be found by following the "Privacy" link located on the bottom of a users' page. Concerning sharing personal information, the policy states:

> We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are . . . . Even though we do not

---

the purposes for which it collect's user's personal information . . . [a]llow Users to use its service without consenting to supply unnecessary personal information . . . [b]e upfront about its advertisers.").

[189] Munkutla-Parker, *supra* note 21, at 634–637; Facebook.com, Facebook.com Statistics, http://www.facebook.com/press/info.php?statistics [hereinafter Facebook Statistics] (last visited Aug. 26, 2010); *see generally* Facebook.com, Facebook's Privacy Policy, http://www.facebook.com/policy.php [hereinafter Facebook Privacy Policy] (last visited Aug. 9, 2010).

[190] Facebook Privacy Policy, *supra* note 189.

[191] Alexa.com, The Top Five Websites in the World, http://www.alexa.com/topsites (last visited Aug. 9, 2010) (listing the top five websites in terms of web traffic as follows: (1) Google, (2) Facebook, (3) YouTube, (4) Yahoo!, and (5) Windows Live).

[192] Canada Facebook Complaint, *supra* note 188; Facebook Privacy Policy, *supra* note 189 (recommending those over the age of thirteen to "ask their parents for permission before sending any information about themselves to anyone over the Internet").

[193] Facebook Statistics, *supra* note 189.

[194] Kaila Krayewski, U.S. Internet Advertising Sees Record Earnings This Quarter (May 14, 2010), http://isedb.com/20100514-3607.php.

[195] Facebook Privacy Policy, *supra* note 189.

[196] *Id*.

> share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.[197]

¶77 The policy outlines several other instances in which Facebook may use a users' personal information, including managing the service, contacting users, or developing social ads.[198]

¶78 Turning first to the positive aspects of Facebook's privacy policy, critics have praised Facebook's statement about its privacy practices, noting that it is written in clear, plain English.[199] Facebook discloses the fact that they use information in profiles to solicit third party advertisements, and does not attempt to hide this practice behind confusing legalese.[200]

¶79 However, others note that Facebook's privacy policy is extremely lengthy, accessible only from a small link towards the bottom of the page, and thus users may not be likely to make the effort to seek out, fully read, or comprehend its often vaguely worded provisions.[201] In 2004, a study measured the required reading levels for the top fifty U.S. websites' privacy policies, and found that the average policy required a college education to fully comprehend, while over half contained language "beyond the grasp of 56.6 percent of the Internet population."

¶80 Facebook fails to straightforwardly communicate the full scope of its privacy policy with respect to third party advertisers. Facebook's main privacy page states in bold print, "We never share your personal information with our advertisers," but states later that sharing is done but on an anonymous basis.[202] This vague language is only moderately clarified in the privacy subsection found on a smaller link. COPPA notice requirements mandate privacy policies be placed in a "clear and prominent" place on a site, and include sufficient detail on how such information is used and *with whom* it is shared.[203] Under such an analysis, Facebook would be required to detail its use of personal information in behavioral targeting in more detail than described in its current policy, and disclose *all* third parties with whom information is shared, including advertisers.[204]

---

[197] *Id.* This language is current in Facebook's privacy policy as of May 31, 2010. Facebook's terms of use have been heavily modified since its inception in 2004 and have recently undergone changes in response to recent privacy debates. For an interesting perspective on the evolution of Facebook's privacy language, see Kurt Opshal, Facebook's Eroding Privacy Policy: A Timeline (Apr. 26, 2010), http://www.eff.org/deeplinks/2010/04/facebook-timeline/. Facebook's policy has visibly shifted to contain more ambiguous language over the years. *Id*.

[198] Opshal, *supra* note 197. Social Ads pair Facebook advertisements with relevant user information about a user or the users' friends "to make advertisements more interesting and more tailored." *Id.* For instance, if a user becomes a fan of a page, Facebook may display the users' name a photo next to an advertisement for that page. *Id.*

[199] Ciocchetti, *supra* note 161, at 602.

[200] *Id.*; Facebook Privacy Policy, *supra* note 189.

[201] *See* Facebook Privacy Policy, *supra* note 189.

[202] Facebook.com, Facebook Privacy Policy Explanation, http://www.facebook.com/privacy/explanation.php [hereinafter Facebook Privacy Policy Explained] (last visited May 31, 2010).

[203] Children's Group COPPA Letter 2008, *supra* note 17.

[204] The website Inside Facebook compiled a list of companies that advertise on Facebook.com. As of

¶81 Another key feature on Facebook is the use of Facebook Platform applications. Facebook Platform allows third party developers to create applications that Facebook users may add to their profiles to enhance their Facebook experience.[205] Applications include games (e.g., *Farmville* or *Mafia Wars*), quizzes (e.g., "Which *Twilight* Character are You?"), entertainment (e.g., "iLike," "Bumper Sticker," "My Year in Statuses") and many more.[206] Facebook currently hosts over 550,000 active applications on the Facebook Platform.[207] Every month, more than 70% of Facebook users engage with Platform applications.[208]

¶82 Facebook's Platform applications are created and operated by third party developers.[209] As Facebook's privacy policy clearly states, "We do not own or operate the applications that you use through Facebook Platform (such as games and utilities)."[210] The policy continues, "That means that when you use those applications and websites you are making your Facebook information available to someone other than Facebook."[211] Facebook distances itself completely from third party application and claims it has no control or responsibility for how third-parties use the information provided to them by users. One must look beyond Facebook's privacy policy to learn more about how these third party applications might access your information.[212] A separate policy about Platform applications (located in a different link, thus illustrating again Facebook's lack of straightforward notice) states, "When you use an application, your content and information is shared with the application."[213]

¶83 The range of users' personal information third party application developers may access without individual consent is vast.[214] The privacy concerns raised by such

---

January 2010, this list included over 21,000 companies. InsideFacebook.com, Complete List of 21,655 Companies on Facebook, http://www.insidefacebook.com/complete-list-of-21655-companies-on-facebook/ (last visited Jan. 10, 2010).

[205] Facebook.com, Facebook Platform Principles & Policies, http://developers.facebook.com/policy/ [hereinafter Facebook Platform] (last visited July 10, 2010).

[206] *See generally* Facebook.com, Facebook Application Directory, http://www.facebook.com/apps/directory.php#/apps/directory.php?app_type=0&category=0 (last visited Jan. 10, 2010).

[207] Facebook Statistics, *supra* note 189.

[208] *Id*.

[209] Facebook Privacy Policy, *supra* note 189.

[210] *Id*.

[211] *Id*.

[212] *See* Facebook.com, Facebook Statement of Rights and Responsibilities, http://www.facebook.com/terms.php (last visited Aug. 26, 2010).

[213] *Id*.

[214] "Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile." Facebook.com, Facebook is Selling your Personal Information, http://www.facebook.com/group.php?gid=2208625477 (last visited Aug. 26, 2010) (the above language is from an older version of Facebook's privacy policy and is found in

applications are serious, but not well understood. As one commentator notes, "[Applications] are given access to far more personal data than they need to in order to run. . . . Not only does Facebook enable this, but it does little to warn users that it is even happening, and of the risk that a rogue application developer can pose."[215]

D. Facebook Privacy Controversies

¶84 Facebook has been the subject of several high-profile privacy controversies in recent years. In August 2008, Facebook user plaintiffs filed a class action suit against Facebook's Beacon ad technology (Beacon).[216] Beacon ads used cookie technology to track a user's activity on outside websites, and then report this information back to Facebook on user profiles to advertise products or services.[217] With the Beacon technology, if a user were logged into Facebook, their activities on partner websites would be posted on that users' Facebook wall (for example, if a user purchased movie tickets on Fandango.com a story would appear). The suit alleged Facebook and its affiliates did not give users adequate notice and choice about Beacon and the collection and use of users' personal information.[218] Plaintiffs and Facebook settled the suit in late 2009.[219] Under the settlement terms, Facebook terminated Beacon and provided $9.5 million to establish an independent nonprofit foundation that will identify and fund projects and initiatives that promote the cause of online privacy, safety, and security.[220]

¶85 In February 2009, Facebook was hit with a wave of public criticism after the consumer blog *The Consumerist* published a critical report on Facebook's Terms of Service (TOS).[221] The report focused on a key provision in the TOS agreement granting Facebook an irrevocable and non-exclusive right to any and all user content.[222] As summarized by the report, the provision essentially stated that "anything you upload to Facebook can be used by Facebook in any way they deem fit."[223] *The Consumerist* focused on a recent change in the policy that appeared to extend Facebook's right to all of a user's information indefinitely—even if the user terminated his or her account.[224]

---

a Facebook group protesting its information collection policies).

[215] Chris Soghoian, *Exclusive: The Next Facebook Privacy Scandal*, CNET NEWS, Jan. 23, 2008, http://news.cnet.com/8301-13739_3-9854409-46.html.

[216] Lane et al. v. Facebook et al., Frequently Asked Questions, http://www.beaconclasssettlement.com/FAQs.htm [hereinafter Beacon Class Action] (last visited Jan. 10, 2010).

[217] *See* Facebook Privacy Policy, *supra* note 189.

[218] Beacon Class Action, *supra* note 216.

[219] *See id*.

[220] *Id*.; *see also* Caroline McCarthy, *Facebook Notifies Members About Beacon Settlement*, CNET NEWS, Dec. 3, 2009, http://news.cnet.com/8301-13577_3-10409034-36.html.

[221] Chris Walters, Facebook's New Terms of Service: "We Can Do Anything We Want With Your Content. Forever.", http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever (Feb. 15, 2009, 23:14 EST).

[222] *Id*. As of February 15th, the TOS policy stated: "You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof." *Id.* (internal citation omitted).

[223] *Id*.

[224] *Id*. The language, "You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge

¶86 An intense public backlash arose in the wake of the report. Commentators across the Internet—from the *New York Times* to blogger Perez Hilton—expressed concerns over the seemingly limitless control Facebook was claiming to exert over users' personal information.[225] After several prominent privacy advocacy groups threaten to file a complaint with the FTC, Facebook backtracked on its policy changes and agreed to reinstate the original policy, and asked users to help contribute to a new "Bill of Rights and Responsibilities" to cover privacy concerns.[226]

¶87 On December 9, 2009, Facebook again made headlines by announcing new privacy settings that promised improved simplicity and greater user control over content.[227] Upon logging in, all Facebook users were prompted with a pop-up message informing users of a new privacy page.[228] All Facebook users were then connected to their privacy setting page, and given the option to either keep their old privacy settings, or to create new ones.[229] The change in Facebook's policy was intended to raise awareness to online privacy concerns. As Facebook spokesman Simon Axten stated, "As far as we know, it's the first time in the history of the Internet that so many people have been required to make affirmative decisions about their privacy."[230]

¶88 However, while the Facebook policy changes made it possible for users to exert more control over who can view their content, certain user information *must* remain public and visible to all users including name, profile picture, current city, networks, friends list, and pages.[231] Thus, while the policy changes offer additional privacy controls they simultaneously limit your ability to control access to key personal information. Many privacy advocates responded negatively to these changes, including the ACLU, Center for Digital Democracy, and Electronic Frontier Foundation.[232] As one commentator notes, "[T]he 'privacy' changes are all about encouraging [users] to share more stuff publicly. It's great that Facebook is making all users think about privacy, but we are concerned that the transition tool and other changes actually discourage or eliminate some privacy protections that Facebook users currently employ."[233] In December 2009, the Electronic Privacy Information Center, along with several other online privacy groups, filed a formal complaint with the FTC, alleging that the new

---

that the Company may retain archived copies of your User Content," was removed and replaced with the statement, "The following sections will survive any termination of your use of the Facebook Service . . . [including] User Content." *Id*.

[225] Brian Stelter, *Facebook's Users Ask Who Owns Information*, N.Y. TIMES, Feb. 16, 2009, at B3; Perez Hilton, Boycott Facebook! Here's Why, http://perezhilton.com/2009-02-16-boycott-facebook-heres-why (Feb. 16, 2009, 13:45 PST) ("So what does this mean? Basically, Facebook can do whatever the hell they want with YOUR STUFF.").

[226] *The Facebook Uprising*, CHI. TRIB., Feb. 20, 2009, at C34, *available at* http://www.chicagotribune.com/news/op inion/chi-0220edit2feb20,0,1966013.story.

[227] Larry Magid, Facebook Details New Privacy Settings, CNET NEWS, Dec. 9, 2009, http://news.cnet.com/8301-19518_3-10411418-238.html.

[228] *Id*.

[229] *Id*.

[230] *Id*.

[231] Complaint of Electronic Privacy Information Center, *In re* Facebook, Inc. 8 (FTC Dec. 17, 2009), *available at* http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[232] For an overview of these critiques, see Adam Ostrow, *Facebook's New Privacy Push Concerns Experts*, MASHABLE, Dec. 12, 2009, http://mashable.com/2009/12/10/facebook-privacy-experts/.

[233] *Id*.

privacy controls "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[234]

¶89 Another serious privacy controversy emerged in spring 2010, directly involving Facebook's data collection practices and third party advertisers. The *Wall Street Journal* reported that although Facebook claimed that it "doesn't share information with advertisers," on several occasions it shared the user name of Facebook users with advertisers.[235] The direct contradiction with Facebook's privacy policy has caused politicians to call for regulatory action and caused over a dozen privacy groups to file complaints with the FTC for deceptive trade practices.[236] The controversy caused Facebook to yet again publicly promise to review its privacy policies, yet the spring 2010 incident has caused Facebook users themselves to react strongly to the violation of trust.[237] The website QuitFacebookDay.com was launched urging Facebook users "sick of Facebook's lack of respect for . . . data" to quit the site once and for all.[238] While Facebook has promised to roll out new controls in response to the controversy, it is unclear how if at all these controls will related to a user's ability to control third party access to their personal data.[239]

¶90 A final—although less public—controversy surrounding Facebook is the growing number of users under the age of thirteen, in direct violation of COPPA's provisions. Statistics as to underage Facebook usage are difficult to come by given the ease of age falsification on Facebook.[240] A study in the United Kingdom found that more than a quarter of eight to eleven year olds online have a profile on a social networking website.[241] Another study found that a quarter of children ages eight to twelve have a social networking profile on Facebook, Bebo, or Myspace.[242] It is clear that privacy concerns on Facebook extend beyond just teens to children COPPA set out to protect.

¶91 With the provisions of COPPA in mind, the string of recent Facebook controversies illustrate two important points. First, the typical Facebook user remains largely ignorant

---

[234] Complaint of Electronic Privacy Information Center, *In re* Facebook, Inc. (FTC Dec. 17, 2009), *available at* http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; *see also* Caroline McCarthy, *F.T.C. May Enter Latest Facebook Privacy Debate*, CNET ONLINE, Dec. 17, 2009, http://news.cnet.com/8301-13577_3-10417934-36.html.

[235] Elinor Mills & Declan McCullagh, *Facebook Sent Some User Data to Advertisers*, CNET ONLINE, May 20, 2010, http://news.cnet.com/8301-27080_3-20005574-245.html?tag=newsLeadStoriesArea.1. The disclosure occurs through the use of a cookie technology referred to as "the Referer," which can send your Facebook name to advertisers when you click on certain links while logged into Facebook. *Id*.

[236] *Id*.

[237] Should Government Take on Facebook?, http://roomfordebate.blogs.nytimes.com/2010/05/25/should-government-take-on-facebook/ (May 26, 2010, 19:09 EST).

[238] QuitFacebookDay.com, We're Quitting Facebook, http://www.quitfacebookday.com/ (last visited May 31, 2010).

[239] Jodie O'Dell, *How Facebook's New Privacy Controls Work*, MASHABLE, May 26, 2010, http://mashable.com/2010/05/26/new-facebook-privacy-controls/.

[240] A user seeking to create a Facebook profile must enter his or her date of birth. If that user is under the age of thirteen, Facebook will not permit that user to create a profile. The user then simply deletes the cookies stored in the Internet browser, and then simply registers again, this time with a falsified date of birth.

[241] Darren Waters, *Children Flock to Social Networks*, BBC ONLINE, Apr. 2, 2008, http://news.bbc.co.uk/2/hI/technology/7325 019.stm.

[242] Children Signing Up for Under-Age Social Networking Profiles, http://www.ofcom.org.uk/consumer/2010/03/children-signing-up-for-under-age-social-networking-profiles/ (last visited Aug. 9, 2010).

of his or her privacy rights. For instance, many of the offending provisions at issue in the report and subsequent response have always been in the Facebook TOS—it took the report from *The Consumerist* and the third party privacy breach of spring 2010 to shed light on these vague provisions. Notice and consent under Facebook's current policy fails to adequately inform users of their rights. The recent "Quit Facebook" campaign demonstrates that users have not fully comprehended their rights under the current policies, and that change is needed to more effectively communicate Facebook's policies to its users.

¶92 Secondly, the controversies are important because they foster an open discussion of online privacy concerns.[243] Facebook users—including millions of adolescents and even children—are increasingly mindful of the power and control Facebook and third parties have over their personal information. As such, there exists today a valuable opportunity for Congress to consider revisions to its online privacy policies.

V. A NEW CHILDREN'S ONLINE PRIVACY PROTECTION ACT

A. Suggestions from Advocacy Groups and Critics

¶93 COPPA is in need of reform due to the changing Internet landscape and the threats posed to children and adolescents online. While Facebook's practices affect all its users, not just children and teens, framing the issue through the lens of Facebook's most vulnerable users is likely to create a stronger incentive to meaningful change. Legislators must strike a balance between the need to protect the private information of children and teens and the need to permit social networking sites to continue to use a legitimate business model which relies on advertising revenues to support their products. While the original objective of COPPA intended for parents and website operators to share the burden of protecting children's information online, this goal has not been met due to the ease of age falsification and the absence of an effective means for granting parental consent. A higher burden must be placed on web operators themselves to fulfill the principles of fair information use—better notice, clearer consent, and easier access to information policies and security.

¶94 In April 2008, several consumer and privacy advocacy groups called upon the FTC to consider revisions to COPPA. These proposals addressed the challenges of targeted marketing efforts and criticized COPPA regulations as an ineffective means of ensuring the protection of personal information online.[244] Organizations called upon the FTC to create a special task force to examine new threats to children and teenagers, including the role of behavioral targeting and profiling and to open up an inquiry into the data collection and target-marketing practices of social networks, including Facebook and MySpace.[245]

---

[243] *The Facebook Uprising*, CHI. TRIB., Feb. 20, 2009, http://articles.chicagotribune.com/2009-02-20/news/0902190493_1_facebook-online-privacy-users ("It was encouraging to witness a victory for consumer vigilance because that's the way many of the rules are being written in the evolving sphere of electronic communication.").

[244] *See* Children's Group COPPA Letter 2008, *supra* note 17 ("We know that teenagers use the Internet to seek help for their personal problems and to deal with difficult issues in their lives. These activities give marketers unprecedented opportunities for massive data collection and behavioral targeting. . . . The loss of privacy is too high a price for reaping the benefits of the digital age.").

[245] *Id.*

¶95 Some commentators have suggested that an overhaul of COPPA that eliminates age distinctions and parental consent requirements would be the most effective means of revision, arguing instead for a new policy that places a higher burden on the website operators themselves to regulate the use of personal information.[246] These advocates have called on the FTC or Congress to eliminate parental consent entirely and require website operators to obtain consent directly from the individual whose information is being collected.[247] However, while a revision to COPPA eliminating all age barriers would address the problematic concept of parental consent, it ignores the particular vulnerabilities of children and adolescents and, as such, would push aside the original legislative intent of COPPA regulations.

¶96 In 2008, a Canadian public interest group charged Facebook with several violations of Canadian privacy laws.[248] According to the complaint, Facebook fails to identify all the purposes for which it collects users' personal information, fails to obtain informed consent from users regarding the dissemination of their personal information to third parties, fails to disclose its advertisers' use of personal information and the level of users' control over their privacy settings, and fails to provide adequate notice regarding the range of personal information that is disclosed to third party advertisers and application developers.[249] Canada's approach suggests that revised privacy laws should include stricter notice and consent requirements, with stronger emphasis on disclosure of *all* third parties with access to an individual's personal information. The complaint is even more poignant and compelling given recent controversies over Facebook's use of private information.[250]

¶97 Another proposed change to COPPA would require mandatory opt-in policies.[251] Websites with an "opt-out" mechanism require users to take an affirmative step to protect personal information; for example, checking "accept" to a statement allowing for the disclosure of private information to third parties.[252] Opt-in policies, on the contrary, mandate that as a default option, personal information cannot be shared or disseminated with third parties *unless* a user affirmatively grants permission.[253] For example, a Facebook user wishing to share their personal information for the purposes of advertising would have to affirmatively agree to such use via a consent agreement. In a recent forum on behavioral targeting, FTC Commissioner John Leibowitz expressed his support for these policies, stating that "[t]he current 'don't ask, don't tell' in online tracking and profiling has to end."[254] In the wake of the spring 2010 Facebook controversy, consumer groups have advocated an opt-in model with minimal data collection, in particular given the use of Facebook by children and teens.[255]

---

[246] *See, e.g.*, Hotaling, *supra* note 22, at 560.
[247] *Id*.
[248] Canada Facebook Complaint, *supra* note 188.
[249] *Id*.
[250] *See* discussion *supra* Part IV.D.
[251] Hotaling, *supra* note 22, at 558.
[252] *Id*.
[253] *Id*.
[254] Louise Story, *F.T.C. Member Vows Tighter Controls of Online Ads*, N.Y. TIMES, Nov. 2, 2007, http://www.nytimes.com/2007/11/02/technology/02adco.html.
[255] Chloe Albanesius, *Facebook Should be Opt-in or Bust, Watchdogs Say*, P.C. WORLD, May 27, 2010, http://www.pcmag.com/article2/0,2817,2364262,00.asp.

¶98 However, a mandatory shift to opt-in only information sharing would likely be heavily opposed by Facebook and other social networking websites. Facebook creator Marc Zuckerberg has recently commented that an "opt" policy defeats the purposes of Facebook—the sharing of information with others.[256] Speaking directly to opt-in policies, Zuckerburg noted, "people use [Facebook] because they love sharing information."[257] Further, blanket opt-in policies are an unnecessary step if Facebook were to provide meaningful notice and consent to its users in the first place. As noted above, Internet providers argue that, from a policy perspective, consent to some data sharing with advertisers is the implicit cost to a free Internet.[258] If a website is providing adequate notice to its users of its information practices, then users can decide whether or not to continue using that website. As the "Quit Facebook" campaign demonstrates, users are willing to turn away from the site when educated with the full extent of data practices.[259] Therefore, regulations should focus on ways to equip vulnerable Internet users—children and teens—with the information necessary to make this determination.

B. Recommended Changes

¶99 Judge Frank Easterbrook's earlier quoted comment on internet law can help guide the reform of COPPA: "Let us not struggle to match an imperfect legal system to an evolving world . . . . Let us do what is essential to permit the participants in this evolving world to make their own decisions."[260] Revisions to legislation that seek to regulate the Internet must provide users themselves with the tools to make informed, complete decisions with regard to their privacy rights online.

¶100 Policy makers charged with amending COPPA legislation should consider the following three revisions: (1) extending protections to adolescents ages thirteen to seventeen; (2) increasing opt-in information sharing policies in lieu of parental consent; and (3) providing more comprehensive notice and consent requirements consistent with principles of fair information use.

¶101 When considering the following arguments, bear in mind the challenges of drafting effective legislation to regulate the Internet, especially given its expansive nature. These recommendations should serve as a starting point for continued discussion as policy makers continue to seek the most effective solutions to protect the privacy of children and adolescents online.

1. Extending Protections to Teens

¶102 While the FTC argues that children under the age of thirteen are particularly vulnerable and in need of special protections online, the expanded abuse of young people's personal information, along with other dangers from over-sharing online since COPPA's enactment, have proven that such vulnerabilities are not limited to young people under thirteen. Given the social pressures teens face to interact online, and the prevalence of social networking sites as a means of communication, it is no longer

[256] *Id*.
[257] *Id*.
[258] *See* discussion *supra* Part IV.A.
[259] QuitFacebookDay.com, *supra* note 238.
[260] Easterbrook, *supra* note 1, at 215–16.

accurate to assume that teenagers are protected from the risks of dissemination of personal information online.[261]

¶103 Teenagers, like children, may not be able to grant meaningful consent to the use of their personal information online under the current framework. When COPPA created protections only to users under the age of thirteen, website operators adopted age screening mechanisms to purportedly ban underage users from their sites. The practical effect of this measure caused smaller websites to reduce services offered to children and encouraged age falsification. Thus, a revision to COPPA should seek to address the underlying issue of fair information collection and use, rather than impose ineffective and unenforceable age restrictions.

2. Limited Opt-In Requirements

¶104 The parental consent requirement has never functioned in the manner envisioned by the drafters of COPPA. In implementing COPPA, the FTC argued for measures that would return parents to their traditional role as gatekeepers of what information children access and what information others access about their children.[262] The FTC sought to meet this objective by requiring websites to obtain parental consent. However, technological advancements to verify parental consent have remained largely ineffective, and given their practical and economic impracticability, it is difficult to believe that consent methods like faxing in signatures or age verification hotlines are the best solution. Identifiers such as social security or driver's license numbers could be used to verify age; however, the issue then becomes whether or not these extra verification measures pose an even greater risk to privacy, as websites would then be required to maintain large databases of children, teenagers', and their parents' most sensitive information.[263]

¶105 In lieu of the parental consent requirement, policy makers should consider adopting a balancing test between opt-in requirements and age. Blanket opt-in policies for all Internet users, as argued above, are unlikely to find policy support and are unnecessary for non-children and teen users where consent is possible. Under a balancing test, however, the degree to which e-advertisers and web operators could share a users' personal information would relate to that child or teen's stated age. For example, children under the age of thirteen would have mandatory opt-in policies (no information can be shared with advertisers without the user explicitly agreeing), and users over eighteen would have default opt-out policies (information shared with advertisers automatically unless the user expresses otherwise), with varying degrees of information sharing permitted within the teenage demographic. Further, such a rule might actually promote honest age representations when using Facebook, as children and teen users would not have to lie to gain access to the website and would be afforded more distinct opportunities for privacy than those over eighteen. On Facebook, opt-in policies could be mandatory with regard to third party applications. Using such a rule, regulators could seek a balance between the interests of e-advertisers and web operators and the privacy needs of children and adolescents.

---

[261] Allen, *supra* note 88, at 759–60.
[262] *See* discussion *supra* Part I.B.
[263] Harris, *supra* note 122.

3. Improving Notice & Consent

¶106 In order for an limited opt-in/opt-out system to function properly, the new COPPA policy must impose a burden upon websites to require more comprehensive notice and consent procedures. Rather than demanding "verifiable parental consent," policy makers could revise COPPA to include a new consent requirement applicable to both children and adolescents who share personal information online. Such a policy would require the recognition by policy makers that children and teens' ability to consent differs from adults. Rather than trying to bypass these age groups by faulty parental consent mechanisms, such a reform would require websites to educate children and teens directly. For example, a new COPPA could require "informed notice and consent in a manner that ensures maximum possible comprehension before any collection, use and/or disclosure of personal information."[264]

¶107 The methods for ensuring "maximum possible comprehension" would place the burden of fair information practices to the websites themselves, and encourage creative and effective solutions for educating children and teens about sharing information online. Under this standard, the FTC would focus enforcement actions against websites providing inadequate forms of notice and consent, and against websites failing to provide *any* form of notice and consent. Websites would adopt baseline notice and consent mechanisms and procedures based on whether or not they are directed towards young children, adolescents, or both.

¶108 For very young Internet users, such as a four-year-old child who visits the website NickJr.com to play games, informed notice and consent to the sharing of personal information may be limited given developmental capacities. Website operators would be encouraged to adopt creative mechanisms to teach children about privacy online (such as playing a video of a popular cartoon character talking to kids about giving their e-mail to strangers online) in order to provide proper notice of risks online. Under the language proposed above, such methods would be targeted to ensure "maximum possible comprehension" among younger Internet users (rather than placing the burden on parents through ineffective means of consent) and instill judicious browsing habits from an early age.[265]

¶109 For the seventeen-year-old Facebook user, maximum possible comprehension of notice and consent could take on a different form. Currently, when a user registers on Facebook, they consent to all terms and policies automatically by simply signing up.[266] Rather, Facebook could use progressive click through agreements to educate users about

---

[264] This statutory language is found in some informed consent statutes in the medical context. *See, e.g.*, ALA. STAT. § 47.30.837 (2010).

[265] To be sure, a gray area exists in targeting children directly—can a minor legally grant consent, or comprehend their rights? These suggested revisions to COPPA challenge this notion. Websites may wish to continue reaching out to parents in an attempt to obtain "maximum possible comprehension" of rights, especially when personal information is submitted by very young children. Under a new standard, websites would be applauded for taking this extra step, but not required to like under COPPA today. Further, baseline notice and consent requirements would be imposed upon websites so that even if children try to bypass parental consent, or if a child is on a website that is age inappropriate, a mechanism still exists to inform them of their rights.

[266] A user seeking to join Facebook acknowledges: "By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy." Facebook.com, Sign Up Screen, http://facebook.com (last visited Jan. 10, 2009).

its information use policies in a clear and straightforward matter.[267] Users would not be able to register until clicking through several pages of privacy rights materials. In order to comply with "maximum possible comprehension," Facebook would be required to disclose all third party advertisers with whom they share information, and clearly outline Facebook's rights to users' personal information. Similarly, Facebook could require users to watch an online video explaining Facebook's information use procedures before allowing registration. These creative solutions would foster "maximum possible comprehension" of users' rights, and ensure proper notice and consent to usage terms among all users, but especially the vulnerable children and teen demographics.

VI. CONCLUSION

¶110 While COPPA legislation was originally intended to better protect the privacy interests of children online, its practical effect has been to hamper children's access to certain online resources, and encourage age falsification. COPPA legislation, despite only having been in effect for eleven years, is already outdated. Congress and the FTC should act to revise COPPA to include teenagers and to require opt-in policies and stricter notice and consent requirements. As the recent high-profile privacy controversies surround Facebook suggest, privacy concerns on social networking sites, especially with regard to teenagers, are sure to dominate privacy law debates for years to come. As the Internet by its nature is a fluid, dynamic, and ever-changing medium, new COPPA laws are needed to provide flexible, yet comprehensive, regulations to guarantee that the privacy and safety of children and adolescents are protected now and in the future.

[267] For a general discussion of progressive click through agreements (also known as "click-wrap" agreements), see Francis M. Bruno & Jonathan A. Friedman, *Maximizing the Enforceability of Click-Wrap Agreements*, 4 J. TECH. L. & POL'Y 3 (1999), *available at* http://grove.ufl.edu/~techlaw/citation.html.