American Business Law Journal
Volume 45, Issue 3, 417–453, Fall 2008

POCKET Protection

Janine Hiller, France Belanger,** Michael Hsiao,*** and Jung-Min Park*****

I. INTRODUCTION

In December 2006 the online Web site Xanga.com was fined $1 million for failing to protect children's privacy as required under the Children's Online Privacy Protection Act (COPPA).[1] The Federal Trade Commission (FTC) estimated that 1.7 million accounts were created by underaged children without their parent's knowledge or consent.[2] Although the site asked for a person's age before completing registration, warning those under thirteen that they could not participate, nevertheless the system allowed those who subsequently entered birthdates indicating that they were under thirteen to simply continue the process of registration and to access and post information on the site.[3] Xanga also collected information from the children, including name, address, cell phone number, and instant messenger identification, which they posted in the child's online profile.

---

*Professor of Business Law, Virginia Tech, Blacksburg, Virginia. This research was supported, in part, by a grant from the National Science Foundation Cybertrust Program, #CNS-0524052. We would like to thank the participants in the 2007 Huber Hurst Research Seminar for their insightful comments and the University of Florida, Department of Management, for their sponsorship of the symposium.

**Professor, Accounting & Information Systems, Virginia Tech.

***Professor, Electrical & Computer Engineering, Virginia Tech.

****Assistant Professor, Electrical & Computer Engineering, Virginia Tech.

[1]Press Release, FTC, Xanga to Pay $1 Million to Violating Children's Online Privacy Protection Rule (Sept. 6, 2006), http://www.ftc.gov/opa/2006/09/xanga.shtm. COPPA is found at 15 U.S.C. §§ 6501–6506 (2000).

[2]*See* Press Release, *supra* note 1.

[3]*See id.*

The potential danger to young children was that this personally identifiable physical information was easily available online; the social networking site design encouraged communication and personal contact between registered users. Children could post profiles, pictures, and videos as well as communicate directly with other users.[4] The FTC fine against Xanga was the largest ever imposed under COPPA; the settlement of the complaint required Xanga to pay a $1 million fine, implement policies compliant with COPPA, file additional status reports, and submit to monitoring by the FTC.[5]

The Internet brings rich content to children and expands their horizons, but at the same time creates dangers and risks to their privacy and well-being. The recent massive and blatant failure of Xanga to follow COPPA is evidence that significant dangers to children still exist, despite the efforts of statutory protection. Protecting children's privacy today is essential because children are online at an increasingly younger age. A child's advanced technological sophistication that enables him to use the Internet does not match his worldly naïveté, and the dangers to children who share personal information are significant. Risks of harm can range from the threats of a child predator to the targeting and profiling of a commercial online marketer.

In Part II, this article describes the participation of children on the Internet, noting its exponential growth in recent years. Next, in Part III, the article examines the history of protecting children online. Part IV reviews the regulatory parameters of COPPA. COPPA was designed with the goal of interposing parental involvement in their child's electronic interactions by requiring parental consent for the collection of a child's personal information; ensuing regulations initially relied on the promise of emerging technologies to aid parents in this endeavor. The promise of a technological solution never materialized, however, and regulations setting standards for parental consent continue to be limited to the same methods as those available in 2000. Clearly, Internet and communications technology have progressed rapidly and significantly in over seven years, yet protection of children's privacy seems to have been left behind. Finally, in Part V, we propose a solution to this problem, providing evidence that the legal protections sought in COPPA can be implemented technically. This section

---

[4] *See id.*

[5] *Id.*

briefly describes POCKET (Parental Online Consent for Kids' Electronic Transactions), a technology concept we developed, under a National Science Foundation Cybertrust grant, to help protect children's privacy online.

A technological solution to protecting children online can be integrated into the legal framework, if parents, e-businesses, and regulators will take responsibility for its development, adoption, and use. We argue that it is possible, through the coordination of law and technology, to facilitate a parent's protection of his or her child in the online environment. The technology promise to protect children that seemed so near when COPPA was initially adopted should not be abandoned for less effective regulatory standards.

II. The Nature of Children Online

In 1997 14% of school-age children were online.[6] The FTC noted that the most prevalent activities for children online were "homework, informal learning, browsing, playing games, corresponding with electronic pen pals by e-mail, placing messages on electronic bulletin boards and participating in chat rooms."[7] Foreshadowing the future, the FTC commented in 1998 that the "most potentially serious safety concern is presented by the posting of personal identifying information by and about children . . . in interactive public areas . . . that are accessible to all online users."[8] A few short years later, 2003 statistics reported the number of children online by age: 19.9% between the ages of 3–4, 42.0% between the ages of 5–9, and 67.3% between the ages of 10–13.[9] The exponential increase in the numbers of children online, at increasingly younger ages, is an important reason to be concerned for their privacy.

Children participate in many activities online, accessing the Internet for information, help with homework, entertainment, and interaction.[10]

---

[6]FTC, Privacy Online: A Report to Congress 4 (1998) [hereinafter FTC 1998 Report].

[7]*Id.*

[8]*Id.* at 5.

[9]U.S. Dep't of Commerce, A Nation Online: Entering the Broadband Age, app. 2 (Sept. 2004), www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.pdf.

[10]Sonia Livingstone, *Children's Use of the Internet: Reflections on the Emerging Research Agenda*, 5 New Media & Soc'y 147, 149 (2003).

Even beneficial and benign uses by children can lead to or mask hidden dangers, however. For example, peer-to-peer (P2P) systems of communication, easily downloadable, can include bundled spyware that will collect information about children's online activities.[11] In addition, the expansion and popularity of social networking sites has created particular concern for parents.[12] Social networking sites are designed as online places where children can communicate with others with similar interests, a concept that can benefit children by increasing their knowledge, awareness, and personal communication skills, and simply being fun. Disney offers a new social networking site, for example, as it struggles to meet the popular demand for interactive features.[13] The site offers personalization for children, upgraded features for a fee, and retail sales. The inherent danger of social networking sites is that participation increases the chance that children will share personal information.

The gravest risk to children sharing information online is that it can allow predators to meet and harm them offline. It is estimated by the National Center for Missing and Exploited Children that one in seven children, ages ten to seventeen, are sexually solicited online.[14] Although parents may purchase and install filters to limit their children's online activities where a solicitation may be perceived as a greater threat, or where

---

[11]*See* Jessica Herdon, *Who's Watching the Kids—The Use of Peer-to-Peer Programs to Cyberstalk Children*, 1 OKLA. J.L. TECH. 12, 13–15 (2004).

[12]In December 2005 the popular site MySpace recorded more Web page views than Google and eBay combined. Michael Nutley, *Corporates Target Youth Market via Emerging Media*, NEW MEDIA AGE, Feb. 6, 2006, at 14 (citing ratings from the Netview monthly Internet survey). *See also* Sue Shellenbarger, *How Young Is Too Young When a Child Wants to Join the MySpace Set?*, WALL ST. J., Oct. 19, 2006, at D1 (discussing how to balance the benefits and dangers of new online social networking sites for young children). The American Medical Association has recently joined the discussion by adopting a policy that encourages physicians to engage and educate parents about the potential dangers to their children online. *AMA Adopts Plan to Help Protect Children From Online Harm*, U.S. NEWSWIRE, Nov. 14, 2006.

[13]http://disney.go.com/index (last visited June 1, 2008) (portal through which kids can enter contests, chat rooms, and more). A search for chatting reveals a statement that you can "Chat with your friends in Disney.com XD—the place to listen, watch, chat, and play all things Disney!" *See also* Merissa Marr, *Updated Disney.com Offers Networking for Kids*, WALL ST. J., Jan. 2, 2007, at B1.

[14]*See* Jessica E. Vascellaro & Anjali Athavaley, *Foley Scandal Turns Parents Into Web Sleuths; Sales of Software that Tracks Kids Online Activities Soar; Cyber-Safety as a Job Benefit,* WALL ST. J., Oct. 18, 2006, at D1.

sexually explicit material may be available,[15] it is the sharing of information without parental oversight, even on a children's site, that can pose the greatest risk.

Less sinister, yet undesirable, is the commercialization of a child's Internet use, where businesses collect personal information in order to create literal lifetime brand loyalty and target consumers. Children are not sophisticated enough to distinguish between advertising and unbiased content and can be convinced to share large amounts of personal information by the promise of a chance to win a small gift or the promotional antics of a cartoon character.[16] Also, marketing techniques can include creating profiles that can follow a child throughout his or her lifetime until adulthood and using those profiles to reach the parent through the child.[17] Hummerkids.com is a possible example of this trend. Although Hummers will obviously not be bought by children, www.hummer.com contains Hummer Kids, which includes coloring pages, a race where children choose their own Hummer, and a section where children can create their own Hummer. It is estimated that children under the age of fourteen influence 47% of family spending in the United States, representing $700 billion a year, perhaps explaining why more Internet sites that seem unrelated to children include children's pages.[18]

---

[15]*See id*.

[16]The results of an Annenberg Public Policy Center survey in 1999 are summarized in Press Release, The Annenberg Public Policy Center of the University of Pennsylvania, Free Gifts Could Entice Children Into Revealing Personal Family Information Online (May 16, 2000). For further examination of the results of this survey and the implications, see Joseph Turow, *Family Boundaries, Commercialism, and the Internet: A Framework for Research*, 22 Applied Dev. Psychol. 73, 79–80 (2001) (the effect of information release and its commercialization raises concerns). For a discussion of the cognitive age limitations of children, see Elizabeth S. Moore, *Children and the Changing World of Advertising*, 52 J. Bus. Ethics 161, 163 (2004). The impact of interactive advertising techniques, including online advertising, on young children is discussed in ChildrenNow, Interactive Advertising and Children: Issues and Implications (2005), http://www.childrennow.org/assets/pdf/issues_media_iadbrief_2005.pdf.

[17]*See* Livingstone, *supra* note 10, at 45–46. *See also* Joseph Turow, *Family Boundaries, Commercialism and the Internet: A Framework for Research*, 22 Appl. Dev. Psych. 73, 78–81 (2001) (information collection impacts the family as well as the child and results in dangers to the family unit and parental control).

[18]*Marketing to Children: Trillion Dollar Kids,* Economist, Dec. 2, 2006, at 66 ("Children are hedonists, inclined to make impulse buys and less likely to make educated purchasing decisions.").

The concern for protecting children online did not begin with the increasing commercialization of the Internet and the serious dangers of social networking. The potential harms to children sharing personal information online were recognized by the FTC early in the 1990s.

III. Privacy Problems in the Pre-COPPA World

In the 1990s the Internet and the World Wide Web had only begun ascending to national and international communication and commercial prominence. Yet, one of the initial concerns of users remains an issue today: the nature of privacy in the online environment, where collection of information about persons and habits is easy and far from transparent. Studies and surveys have consistently shown that the lack of privacy is a concern for consumers,[19] affecting how they use the Internet.

The early days of Web site development did not initially include protection for the less sophisticated child participant. In 1997 KidsCom operated a Web site that included "KidsCash" and "Find a Key Pal" activities, requiring children to register and provide their "name, birth date, e-mail and home addresses, and product and activity preferences"[20] in order to participate. Not only did the site collect this information from children, it also shared identifiers with other third parties. The Center for Media Education filed a complaint with the FTC, alleging deceptive actions by the KidsCom Web site in this method of information collection from children and its subsequent sharing practices with third parties.[21] Although the FTC decided not to pursue an action against the Web site because it had modified its information collection practices, the FTC did provide a staff opinion letter in which it established important standards for commercial entities who deal with children online.[22] It stated that it was a deceptive

---

[19]*See, e.g.*, Tom Buchanan et al., *Development of Measures of Online Privacy Concern and Protection for Use on the Internet*, 58 J. Am. Soc. Info. Sci. & Tech. 157, 158–59 (2007) (reviewing studies that document widespread concern for online privacy).

[20]Press Release, FTC, FTC Sets Forth Principles for Online Information Collection from Children (July 16, 1997), http://www.ftc.gov/opa/1997/07/kidscom.htm.

[21]*Id.*

[22]Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, to Kathryn C. Montgomery, President, Center for Media Education, & Jeffrey A. Chester, Executive Director, Center for Media Education (July 15, 1997), http://www.ftc.gov/os/1997/07/cenmed.pdf.

practice to collect information from children for one reason yet use the information for another purpose and that it was "likely" to be an unfair practice to collect or release personally identifiable information from children without informed consent from a parent and the opportunity to restrict or prevent the collection and sharing of the child's information.[23]

A. The FTC's 1998 Privacy Study

The overall FTC approach to online privacy in the 1990s was to encourage Web sites to respect consumer privacy by voluntary self-regulation of information collection practices. In order to evaluate the effectiveness of the self regulatory approach, the FTC conducted a survey of Web site privacy practices in 1998, culminating in the report, "Privacy Online: A Report to Congress."[24] The FTC specifically addressed children's privacy concerns, and performed a separate study of children's Web sites in this survey.

The empirical results were striking: 89% of the Web sites studied collected personal information from children.[25] In order to entice children to share information, Web sites used offers of prizes, incentives of online chat rooms, and even the endorsement of imaginary characters in order to induce children to register and share personal information.[26] In fact, benefits were often available only upon registration.[27] Although the survey used a broad definition of a privacy policy, only 24% of the Web sites had such a policy, and only 8% of the sites stated that they informed parents of their information collection practices.[28] Forty-nine percent of the Web sites said they could share children's information with third parties.[29] A paltry three sites (of a sample of 212) required parental consent before information was collected from children.[30] The most common child protection

---

[23] *Id.*

[24] *See* FTC 1998 Report, *supra* note 6.

[25] *Id.* at 31.

[26] *Id.* at 33.

[27] *Id.*

[28] *Id.* at 34.

[29] *Id.* at 37.

[30] *Id.*

feature, followed by 23% of the sites, was simply to advise children that they should ask their parents before sharing information.[31]

To further evaluate the effectiveness of self-regulation, the FTC reviewed the two voluntary guidelines then available for businesses to use for standardized online child privacy practices. The Council of Better Business Bureaus' Children's Advertising Review Unit (CARU), and the Direct Marketing Association (DMA) each had established guidelines.[32] The CARU guidelines were acceptable to the FTC under the 1997 staff opinion letter, as they required notice and choice and providing parents with the opportunity to remove information about their children.[33] The CARU guidelines adopted a reasonableness standard to determine the acceptability of parental consent.[34] The FTC noted, however, that the CARU guidelines were not widely adopted by business.[35] The DMA guidelines were judged insufficient by the FTC as they were primarily aspirational in nature, without requiring fair information practices such as parental consent.[36]

The report gave guidance to Web sites for following effective privacy protection for children, listing notice/awareness, choice/consent, access/participation, and integrity/security.[37] Referencing the 1997 KidsCom staff opinion letter, the report emphasized that it is the *parent's* consent that is necessary, that adequate notice to the parent is a necessary precursor to collecting information from children, and that "actual or verifiable" parental consent is required when the information is to be shared with third parties.[38] Also relevant to future discussions of effectiveness, the report

---

[31]*Id*. at 34.

[32]*Id*. at 17.

[33]*Id*.

[34]*Id*.

[35]*Id*.

[36]*Id*. at 18.

[37]*Id*. at 12–14. These principles are broadly known for privacy protection, not just for children, and are widely recognized as Fair Information Practices. *See* Anita A. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 762 ("Fair information practices first promulgated in the 1970s are embodied in COPPA's requirements of notice, access, and security"); Jody Blanke, "*Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 70 (2000) (explaining that the FTC used the OECD Guidelines to identify five privacy principles, or "fair information practices").

[38]FTC 1998 REPORT, *supra* note 6, at 13.

noted that "online activities may be unique and unfamiliar to parents,"[39] and therefore notices to parents would need to be more robust. In this way, notices would "[empower] parents to monitor their children's interactions and . . . help protect their children from the risks of inappropriate online interactions."[40]

Not surprisingly, the FTC recommended that legislation be enacted requiring parental consent before commercial Web sites could collect information from children ages twelve and *under*.[41] The commission also recommended that parents of children *over* the age of twelve be notified of information collected and be given the opportunity to delete that information from a Web site database.[42] The FTC emphasized the role of parents and the necessity "of [legally] placing parents in control" of the information collected from their children.[43]

B. Early Child Privacy Cases Result in FTC Remediation

The FTC did not wait for the passage of legislation, but took the lead in addressing the conflict between privacy and the ease of electronic information collection from children in 1999. Under its Section 5 authority to prevent unfair and deceptive actions in commerce,[44] the FTC brought charges against two Web sites for collecting information in a deceptive manner.[45] In what the FTC calls the "First Internet Privacy Case,"[46] it filed a complaint against the Web site hosted by GeoCities. The GeoCities site contained individually created Web pages that were organized into "neighborhoods." Although the personal Web pages and areas of the site were free to users, GeoCities' business model was based on collecting information from consumers and selling that information to advertisers, who were

---

[39]*Id*.

[40]*Id*.

[41]*Id*. at 42.

[42]*Id*. at 42–43.

[43]*Id*. at 42.

[44]15 U.S.C. § 45(a)(1) (2000).

[45]*See* Allen, *supra* note 37, at 764–65.

[46]Press Release, FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Information in Agency's First Internet Privacy Case (Aug.13, 1998), http://www.ftc.gov/opa/1998/08/geocitie.shtm.

then able to send targeted messages and ads to certain interest groups based on the identifying information.[47] The GeoCities site was hugely popular at the time of the complaint, with 1.8 million members and a listing in the top ten most visited Web sites.[48] Included in the numbers of members were approximately 200,000 children under the age of fifteen.[49] The site included the "Enchanted Forest" neighborhood and the "GeoKids Club" for children and required that children provide information including name, age, e-mail address, and gender, without any requirement of parental supervision or consent in order to participate.[50] These neighborhoods were maintained by third parties, although it would seem to users that they were GeoCities sites.[51] The GeoCities privacy policy stated that the information collected was never sold or shared, even though it regularly used the personal information for commercial gain. The FTC alleged that the privacy policy and practices were deceptive, and GeoCities subsequently entered into a consent decree to settle the charges.[52] The consent decree specifically addressed the online collection of information from children by requiring GeoCities to abstain from collecting personally identifying information from children ages twelve and under when it had "actual knowledge" that the child did not have parental consent to share the information.[53] It required a procedure to obtain express parental consent.[54]

The FTC brought a second complaint under its general authority in 1999 against Liberty Financial Companies for the practices on its younginvestor.com site.[55] The site required children to complete a survey in

---

[47]Complaint, FTC v. GeoCities, No. C-3850 (Feb. 5, 1999), http://www.ftc.gov/os/1999/02/9823015cmp.htm.

[48]*See id.*

[49]*Id.*

[50]*Id.*

[51]*See id.*

[52]Decision and Order, FTC v. GeoCities, No. C-3850 (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015.do.htm.

[53]*See id.*

[54]*See id.*

[55]Complaint, FTC v. Liberty Fin. Cos, No. C-3891 (Aug. 12, 1999), *available at* http://www.ftc.gov/os/1999/08/libertycmp.pdf.

order to receive a newsletter and to be eligible to win prizes. The survey asked for personally identifiable information such as name and addresses and also asked for financial information such as the child's weekly allowance and the types of investments that their family owned.[56] Although Liberty stated that the information would be anonymous, they held the identifiable information in a database. Adding further injury, the Web site never sent the newsletter or awarded the prizes.[57] The consent decree entered into by Liberty Financial defined "child" as someone under the age of thirteen, however, the order applied to those under the age of seventeen.[58] In addition, the order contained details regarding parental consent.[59]

These two consent decrees, entered into within months of each other, illustrated the challenge of designing an effective yet cost-efficient methodology for ensuring that parents are involved in protecting their children. The GeoCities decree defined acceptable methods of obtaining express parental consent as: (1) mail or fax, (2) an e-mail that included an electronically verifiable signature, (3) a secure credit card transaction, (4) any procedure authorized by law or regulation, or (5) "such other procedure that ensures verified parental consent and ensures the identity of the parent, such as the use of a reliable certifying authority."[60] It defined an electronically verifiable signature as "a digital signature or other electronic means that ensures a valid consent" by including authentication, integrity and nonrepudiation.[61] Furthermore, the decree allowed a Web site to adopt a screening procedure that sent an e-mail to the parent in order to obtain consent for the information collection.[62] The Liberty Financial decree adopted the same definition of an electronically verifiable signature, but substantially changed the definition of verifiable parental consent. In addition to the five methods described in the GeoCities settlement, the FTC included any "reasonable effort (taking into consideration available

---

[56]*See id*. at 1.

[57]*See id*. at 3.

[58]Decision and Order, FTC v. Liberty Fin. Cos., No. C-3891, at p. 3 (Aug. 12, 1999), *available at* http://www.ftc.gov/os/1999/08/libertydo.pdf.

[59]*Id*. at 4–5.

[60]*See GeoCities*, No. C-3850, *supra* note 52.

[61]*Id*.

[62]*Id*.

technology),'' as an accepted method of obtaining consent.[63] Clearly, the advent and application of new and effective methodologies was anticipated by the commission with their reference to available technology.[64]

IV. COPPA'S PRIVACY FRAMEWORK

Within months of the 1998 Report, Congress passed COPPA.[65] The swift enactment of the legislation was due in large part to the groundwork laid by the 1998 Report and the work of the FTC.[66] However, the legislation was proposed during a time of Internet regulation that included an Internet tax moratorium[67] and the limitation of children's access to pornography,[68] thereby overshadowing discussion of the comparably less controversial COPPA. The Congressional Record contains pages of debate about whether to limit children's access to harmful content and almost no legislative history to explain or supplement COPPA's statutory language. Comments summarily introduced by its cosponsor provide the most background.[69] The summary notes four goals:

> The goals of this legislation are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[70]

---

[63]*See* Liberty Fin., *supra* note 55.

[64]*Id.*

[65]Pub. L. No. 105-277, 112 Stat. 2681-2728 (1998) (codified as amended at 15 U.S.C. §§ 6501–6506 (2000)).

[66]*See* 144 Cong. Rec. E1861-01 (1998) (remarks of Rep. Edward J. Markey introducing the House version of the bill).

[67]Internet Tax Freedom Act, Pub. L. No. 105-277, 112 Stat. 2681-719 (1998) (codified as amended at 47 U.S.C. § 151 (2000)).

[68]Child Online Protection Act of 1998, 47 U.S.C. § 231 (1998).

[69]144 Cong. Rec. S12741-04 (1998) (remarks of Sen. Bryan, explaining that the bill went forward on voice vote from committee and no committee report was filed).

[70]*Id.*

Only the third goal, providing security for the information collected, a responsibility obviously associated with the collecting Web site, did not contain an element of parental involvement.

COPPA's focus on parental involvement is consistent with precedent; as a parent's participation in a child's education, health, and contracts is either legally sanctioned, permitted, or provided incentives in order to protect children in these important areas.[71] The following section focuses on the role of parental consent within the statutory framework of COPPA.

A. COPPA Definitions and Scope: Parental Consent Highlighted

Although the FTC suggested that the law apply in stages to children younger than seventeen, the law only protects a child under the age of thirteen.[72] Commercial online entities engaged in interstate commerce that collect information for themselves or on behalf of others are covered by COPPA.[73] The Web site operator must either direct its Web site or a part thereof toward children, or actually know that the information it collected was from a child,[74] in order for certain provisions to apply. The mere inclusion of a link to a different site that is targeted to children will not trigger the application of the statute.[75]

Personal information is defined as "individually identifiable information about an individual collected online"[76] and includes data that would allow the child to be individually contacted, either online or offline.[77] Thus, the online information that is personally identifiable specifically includes an e-mail address.[78] Name (first and last), address, telephone number, and Social Security number are also considered personally identifiable

---

[71]*See* Allen, *supra* note 37, at 772 (placing parents as gatekeepers is "arguably suitable" and is consistent with the Family Educational Privacy Act, for example); Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 151 (2001).

[72]Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2000).

[73]*Id.* § 6501(2) (definition of "operator").

[74]*Id.* § 6501(10)(A).

[75]*Id.* § 6501(10)(B).

[76]*Id.* § 6501(8).

[77]*Id.* § 6501(8)(F).

[78]*Id.* § 6501(8)(C).

information.[79] In addition, information aggregated about a child, *or their parents*, that is collected and matched with this identifying information, is also covered.[80]

Verifiable parental consent for the collection of a child's information may be obtained by "any reasonable effort (taking into consideration available technology)"[81] that results in parents receiving notice of the information collection, its use, and the site's privacy practices, together with the parent's consent to such use before information is collected from the child. The statute makes it clear that the parent may consent to future information collection as well as current collection.[82] In the summary of the law as it was presented for adoption, it was noted that parental consent

> should be interpreted flexibly, encompassing "reasonable effort" and "taking into consideration available technology." Obtaining written parental consent is only one type of reasonable effort authorized by this legislation. "Available technology" can encompass other online and electronic methods of obtaining parental consent. Reasonable efforts other than obtaining written parental consent can satisfy the standard. For example, digital signatures hold significant promise for securing consent in the future, as does the World Wide Web Consortium's Platform for Privacy Preferences.[83]

Disclosure of information occurs in one of two ways, either by the release of information in identifiable form, which would include sharing of information for marketing purposes, for example, and by making the personally identifiable information available publicly.[84] The statute lists the actions of publicly posting the information on the Internet, on a home page, or through pen pals, e-mail, message boards, or chat rooms, as disclosure.[85] Comments in the House of Representatives noted that "the public posting of children's identifying information in chat rooms and other online forums may pose safety concerns, and the bill simply protects against those things happening."[86]

---

[79]*Id.* § 6501(8)(A), (B), (D), & (E) (respectively).

[80]*Id.* § 6501(8)(G).

[81]*Id.* § 6501(9).

[82]*See id.* ("and the subsequent use of that information").

[83]144 Cong. Rec. S12741-04 (1998).

[84]COPPA, 15 U.S.C. § 6501(4) (2000).

[85]*Id.* § 6501(4)(b).

[86]144 Cong. Rec. H9902-01 (1998).

As we know years later, protecting children in online forums is a worthwhile and necessary goal, yet a simple implementation has not been found.

B. Unfair and Deceptive Practices Defined in COPPA

COPPA makes it unlawful for businesses (an unfair and deceptive practice) to collect information from children in a way that conflicts with the statute and any regulations adopted by the FTC in its furtherance.[87] COPPA requires businesses to:

1. Provide notice of information collection practices, including use and disclosure practices,[88]
2. Obtain prior verifiable parental consent for the collection, use, or disclosure of the information,[89]
3. Facilitate parental access to information collected, the right to delete the information, and the ability to prohibit further collection,[90]
4. Refrain from conditioning a child's participation in online activities on disclosing information unless it is reasonably necessary,[91] and
5. Protect and maintain the accuracy and security of the information collected.[92]

Exceptions to the requirements are based on the limited use of that information and include a one-time response to a child when that information is not retained by the business and the child is not recontacted by the business.[93] In addition, the information may be collected without parental consent when it is used to contact the parent to obtain consent, for the safety of the child, for the secure operation of the site, or other legally authorized reasons.[94]

---

[87]COPPA, 15 U.S.C. § 6502(c) (2000).

[88]*Id.* § 6502(b)(1)(A)(i).

[89]*Id* § 6502(b)(1)(A)(ii).

[90]*Id.* § 6502(b)(1)(B).

[91]*Id.* § 6502(b)(1)(C).

[92]*Id.* § 6502(b)(1)(D).

[93]*Id.* § 6502(b)(2).

[94]*Id.* § 6502(b)(2)(D).

COPPA includes a provision for the establishment of safe harbors "issued by representatives of the marketing or online industries,"[95] when approved by the FTC, as "incentives for self regulation."[96] Participation in and meeting the expectations of an approved safe harbor program is deemed to be compliance with the statute. At the present time there are four safe harbor programs approved by the FTC.[97]

The FTC[98] and state Attorneys General have enforcement power,[99] and the FTC was directed to adopt regulations regarding these practices.[100] Regulations to implement COPPA, and the approval of safe harbors, are discussed in the following sections.

C. The Protracted Development of COPPA Regulations

The FTC proposed rules to enforce COPPA in 1999.[101] Because of particular interest in the application of "verifiable parental consent," the FTC held an additional workshop focused on this provision.[102] The final rules, and the temporary rule for obtaining verifiable consent, were made effective as of April 2000.[103] This article focuses on those aspects of the regulations affecting the nature of parental consent and the potential for using technology for obtaining that consent. In that regard, the history of the development of the standards, the comments of industry, and the expectations expressed as the rule developed, are relevant.

---

[95]*Id.* §6503(1) (or other entities).

[96]*Id.* § 6503(b)(1).

[97]*Id.* § 6503(b)(2). The four approved safe harbor programs are: The Children's Advertising Review Unit, Entertainment Software Rating Board, TRUSTe, and PRIVO. *See* FTC Safe Harbor Program, http://ftc.gov/privacy/privacyinitiatives/childrens_shp.html (last visited Mar. 21, 2008).

[98]COPPA, 15 U.S.C. § 6505(a) (2000) (various other financial agencies have authority to enforce the provisions under subsequent subsections of § 6505).

[99]*Id.* § 6504.

[100]*Id.* § 6506.

[101]Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750 (proposed Apr. 27, 1999) (to be codified at 16 C.F.R. § 312).

[102]Press Release, FTC, FTC to Hold Public Workshop on Appropriate Methods to Obtain Parental Consent in Conjunction with Rulemaking on Children's Online Privacy Protection Act (June 23, 1999), http://www.ftc.gov/opa/1999/06/kidswork.htm.

[103]Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2008).

Parental consent must be informed; the standard proposed by the FTC was that notice must be reasonably designed based on available technology.[104] Possible methods for providing notice included "sending the notice by postal mail, sending the notice to the parent's e-mail address, or having the child print out a form to give to the parent."[105]

The proposed regulation pertaining to the method of parental consent, itself, was linked to the available technology, following the language in COPPA. In developing the regulations more fully, the FTC took the position that it could not at that time adopt a particular technology and requested input regarding the "feasibility, costs and benefits" of different technical methods.[106] Possible methods noted by the commission included a physically produced and mailed consent form signed and returned by the parent (mail or fax), the use of a credit card transaction, a toll free number for parents to call, and a digitally signed e-mail.[107] At that point, the commission also asked for comments about the use of e-mail for other limited types of consent.[108]

A substantial number of comments focused on the potential for technology to assist businesses in obtaining parental consent; however, no clear consensus emerged from this input.[109] One group of commentators agreed that the old-fashioned physical consent form was the most dependable and verifiable; the American Psychological Association (APA) advocated the use of this method based on a "particular concern" that "[c]hildren under the age of 13 do not have the developmental capacity to understand the nature of the request for information that is being made by a Web site and may, unknowingly, pass along information not intended for distribution or collection by their parents."[110] Although this method would slow the process of obtaining consent, it would provide an oppor-

---

[104]Children's Online Privacy Protection Rule, 64 Fed. Reg. at 22753 (explaining proposed rule § 312.4(2)(c)).

[105]*Id*.

[106]*Id*. at 22756.

[107]*Id*.

[108]*Id*.

[109]*See id*. at 59888 & 59899 (Nov. 3, 1999) (to be codified at 16 C.F.R. § 312) (final rule).

[110]Letter from Jeff McIntyre, Legislative & Fed. Affairs Officer, Am. Psychological Ass'n., to Donald S. Clark, Sec'y, FTC (June 11, 1999), http://www.ftc.gov/privacy/comments/apa.htm.

tunity for parents to increase their involvement, providing an opportunity to educate children about the online environment. Interestingly, the APA's comments recognized the potential burden of requiring a signed, physical, writing for consent, but argued that this would provide an incentive for business to develop "secure, affordable technology using digital signatures."[111]

The use of e-mail to obtain parental consent was seen by commentators as problematic. This method was identified as the easiest and least costly for businesses, but was also recognized as having the greatest potential for abuse.[112] Several commentators provided information that parents and children at that time used the same e-mail address and that easily obtainable e-mail addresses would lead to falsification of consent by the child.[113] The use of a credit card transaction to identify the person as a parent was viewed in a similar light; comments noted that not all parents used credit cards, and one credit card company emphasized that credit cards should not be used for identification.[114]

1. 2000 Temporary Final Rule

Adopting the final rule, the FTC stated the goals of "maintaining children's access to the Internet, preserving the interactivity of the medium, and minimizing the potential burdens of compliance on companies, parents, and children."[115] It sought to balance these goals with the protection of children online[116] by making its final rule temporary, based on a "sliding scale" method of consent "until secure electronic methods [became] more available and affordable."[117]

The final temporary rule adopted a standard for consent as follows:

> An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any consent must be rea-

---

[111] *Id.*

[112] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59900.

[113] *Id.*

[114] *See id.* at 59900–01.

[115] *Id.* at 59889.

[116] *See id.*

[117] *Id.* at 59901.

> sonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.[118]

The rule then specified the following methods to meet this standard: a signed consent form that is mailed or faxed, use of a credit card in a transaction, a toll-free number to be called by a parent that is staffed with trained personnel, digital signature using public key cryptography, or an e-mail utilizing a password or personal identification number (PIN).[119] Importantly, the final rule also included a provision that allowed businesses to adopt a less rigorous standard until April 21, 2001. The less stringent standard allowed the use of an e-mail consent method if (1) the information collected is not shared with third parties, (2) the e-mail is accompanied by additional steps to determine the parent's identity (specifically mentioned were an e-mail, mail, or telephone confirmation), and (3) the parent is given notification that they may revoke previous consent.[120] This method has come to be known as the "e-mail plus" method of obtaining parental consent.[121] While the methodology became known as a "sliding scale," the rule actually encompasses a two-tier standard, based primarily on whether the information is shared externally. Noting the number of technologies already identified in the comments, the FTC believed that the sliding scale was only necessary in the short term, as "with advances in technology, companies will soon be able to use more reliable verifiable electronic methods in all of their transactions."[122] In the meantime, the sliding scale "[provided] operators with cost-effective options until more reliable electronic methods [became] available and affordable, while providing parents with the means to protect their children."[123]

---

[118]16 C.F.R. § 312.5(b) (2008).

[119]*Id.* § 312.5(b)(2).

[120]*Id.*

[121]*See* Garber, *supra* note 71, at 184 n.255.

[122]Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59902 ("Comments and testimony at the workshop showed that digital signatures and other reliable electronic methods are likely to be widely available and affordable within approximately a year . . . ample time for these mechanisms to develop and become widely available").

[123]*Id.*

2. 2001 Review

In 2001 the FTC undertook an empirical study of the privacy policies of Web sites targeted to children[124] and also requested comments to review the temporary sliding scale for obtaining parental consent, soon slated to expire. Although the study of Web sites focused on the privacy policies of the sites, it also collected information about the use of parental consent mechanisms referenced in the privacy policy. Of those sites that disclosed their practices in the policy, the study found that half of the Web sites utilized the print and confirm procedure, and half used e-mails to parents. Seventeen percent used telephone verification, and 31% used some other method.[125] The number of Web sites collecting personal information from children dropped from 89% in 1998, to 72% in 2001.[126]

In response to its request for comments, the FTC received twenty-one submissions concerning whether the sliding scale should be extended or made permanent.[127] Although the comments varied considerably, most commentators stated the opinion that the sliding scale should be extended because the predicted advance in available technology had not occurred.[128] In contrast to the FTC's optimistic assumptions two years earlier, comments described the technology as "nascent,"[129] warning that "no widely and economically feasible verification technology even appears to be on the near horizon."[130]

Slow acceptance and adoption of technology by consumers and parents was cited as one reason for the lack of progress toward a technical solution to protecting children online.[131] The Entertainment Software

---

[124]*See* FTC, Protecting Children's Privacy Under COPPA: A Survey on Compliance (2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf [hereinafter FTC 2002 Report].

[125]*Id.* at 12.

[126]*Id.* at 3.

[127]*See* Children's Online Privacy Protection Rule: Public Comments Received, http://www.ftc.gov/privacy/coppa2/comments/index.html (last visited Mar. 21, 2008).

[128]Children's Online Privacy Protection Rule, 67 Fed. Reg. 18818, 18820 (Apr. 17, 2002).

[129]Letter from Jill Luckett, Vice President, Nat'l Cable & Telecomm, Ass'n., to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/ncta.htm.

[130]Letter from Magazine Publishers of America to FTC, http://www.ftc.gov/privacy/coppa2/comments/mpa.htm (last visited Mar. 27, 2008).

[131]*See* Luckett, *supra* note 129.

Ratings Board, certified as a safe harbor, noted that they were open to adopting more technically sophisticated measures such as digital signatures, but that "such mechanisms have been of limited utility since few parents are familiar with the technology, and those few have found the technology difficult to use. Thus, from a parent's perspective, the use of digital technology tools has been unattractive and impractical."[132]

Several commentators advised against extending the sliding scale, however, and one well-known trust organization warned that "[c]hoosing to extend the compliance date every two years because new technological solutions have not been widely adopted, is likely to create a regulatory environment that does not place pressure or give incentive to companies to invest and use such systems."[133] Other comments emphasized that the online environment was no less dangerous for children than in the previous two years, and the need to protect children was even more pressing, especially with regard to the availability of public information in places such as chat rooms.[134]

In support of maintaining the flexibility of the sliding scale, especially the e-mail-plus method, principals of Cyberangels, an online safety organization, said:

> Parents have been slow to respond to requests for consent. From busy soccer moms and dads to corporate workers and executives, parents have overwhelming demands on their time. The easier the consent process is, the better the response rates will be—always keeping in mind the need to have the consent "verified."[135]

The FTC temporarily extended the sliding scale for another three years, until April 2005, noting that "[s]ecure electronic mechanisms and/or infomediary services for obtaining verifiable parental consent are not yet widely available at a reasonable cost."[136]

---

[132]Letter from Marc E. Szafran, Vice President, Entertainment Software Rating Board, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/esrb.htm.

[133]Letter from Rebecca J. Richards, Director, TRUSTe, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/truste.htm.

[134]*See* Letter from Jorian Clarke, President, Circle 1, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/caru.htm (citing increasing number of children online, increasing pornography, and decreasing choices).

[135]Letter from Parry Aftab, Esq. & Nancy L. Savitt, Esq., to FTC, http://www.ftc.gov/privacy/coppa2/comments/aftab.htm (last visited Mar. 27, 2008).

[136]Children's Online Privacy Protection Rule, 67 Fed. Reg. 18818, 18819 (Apr. 17, 2002).

3. 2005 Review

In 2005 the FTC undertook a second review of COPPA rules and proposed making the sliding scale rule permanent.[137] Comments were solicited about the availability of technical methods for obtaining parental consent in both a general review and specific sliding scale requests for comments. Specific technologies mentioned included digital signatures, digital certificates, digital credentialing, P3P, and infomediaries.[138] Twenty-five comments were submitted about COPPA in general, and ninety-one comments were submitted specifically concerning the sliding scale.[139]

The FTC distinguished between form-based and non-form comments in assessing the input. Forty-eight comments opposing consent by e-mail were discounted, as the FTC explained that the rule did not allow bare e-mail consent, but required the e-mail-plus method.[140] The majority of non-form comments favored retaining the sliding scale rule, with or without some modification.[141]

The FTC once again noted the general concurrence that electronic verification technology was neither widespread nor cost effective and that the future of these technologies was unpredictable.[142] The technologies mentioned included digital signatures, public key infrastructure, P3P, and infomediaries.[143] Digital signature technology uses a mathematical formula to encrypt a message from a person that can only be decrypted with a unique formula. Thus, one may be sure that the person who sends the message, or in the case of COPPA the person who grants parental consent,

---

[137]*See* Children's Online Privacy Protection Rule, 71 Fed. Reg. 13247 (Mar. 15, 2006).

[138]*See id* at 13255.

[139]*Id*. at 13247.

[140]*Id*. at 13248–49.

[141]*See id*.

[142]*Id*. at 13255.

[143]A more detailed description of these technologies is beyond the scope of this article. For more detailed information on privacy-enhancing technologies such as those mentioned, particularly P3P, see generally Noushin Ashrafi & Jean-Pierre Kuilboer, *Privacy Protection Via Technology: Platform for Privacy Preferences (P3P)*, 1 Int'l J. E-Bus. Res. 56 (2005); Kimberly Rose Goldberg, *Platform for Privacy Preferences (P3P): Finding Consumer Assent to Electronic Privacy Policies*, 14 Fordham Intell. Prop. Media & Ent. L.J. 262 (2003).

is identified and the message is authentic. Public key infrastructure supports encryption; it is a method by which the mathematical scrambling known as encryption may be matched with the person sending the message. P3P, or Platform for Privacy, is a system of privacy setting standards that operationalizes privacy policies of participating Web sites into a format that can be read by a computer automatically and compared with preferences set by a user; if the policy does not meet the privacy preferences set by the user, then a notification message is displayed. An infomediary, as used in this context, is an entity that serves the function of certifying trustworthiness between two parties by acting as a middleman for the negotiation of whether or not to share information.[144] The conclusion reached after reviewing these choices was that no single technology was universally cost effective, available, and effective for obtaining parental consent.[145]

One group of comments predicted that a permanent rule would actually promote the development of more secure methods of parental consent, as the temporary nature of the rule discouraged investment because of regulatory uncertainty.[146] Commentators generally agreed that the internal use of personal information by Web sites posed the least danger for children and that less costly parental consent mechanisms for this type of information collection and use served to preserve content for children on the Internet.[147] Furthermore, it was stated that the sliding scale responded to the increased risk of public disclosure or sharing of children's information by imposing more secure parental consent mechanisms for these uses.[148]

Thus, in March 2006 the FTC retained the sliding scale for obtaining parental consent, stating that, "[in]n light of the unpredictability of tech-

---

[144]An "infomediary" is not defined by the FTC and is sometimes called an information intermediary in other disciplines. *See* Robert Garfinkel et al., *Secure Electronic Markets for Private Information*, 36 IEEE Transactions Sys., Man & Cybernetics 461, 462 (2006) (trusted information intermediary).

[145]P3P lacked an identity function and was not designed to obtain parental consent for children's information; digital signatures and infomediaries were not widely available or cost effective.

[146]*See* Children's Online Privacy Protection Rule, 71 Fed. Reg. at 13256–57.

[147]*See id.*

[148]*Id.* at 13257.

nological advancement and the benefits of decreasing regulatory uncertainty, the Commission has determined to retain the sliding scale indefinitely while it continues to evaluate developments."[149] In conclusion, the FTC noted that it maintained the right to modify the rule in response to future developments.[150]

4. 2007 Report

In February 2007 the FTC reported to Congress as required by COPPA and concluded that the administrative rules provided a "workable system" for providing online privacy and safety to children.[151] The report relied on the 2006 comments and review, described earlier, but noted additional future challenges.

First, the emergence and popularity of social networking sites was noted as a particularly risky development, enabling child predators to identify and contact children.[152] The Xanga case prosecution was discussed in this light, and the FTC expressed the opinion that the significant penalty imposed would act to guide other social networking sites to protect children and deter them from making similar mistakes. As Xanga involved children falsifying their ages to register and gain access to the Web site, it is interesting that other sections of the report commented about the ease of age falsification when low-technology methods are used. In contrast, the Commission noted that "[c]ontinued concerns about children's online safety may prompt the more rapid development of age verification technology. The Commission will monitor closely any such developments, and will update its business guidance accordingly if and when such technology becomes more widespread."[153]

The report also identified the convergence of technologies as a future area of concern. Growing access to the Internet by mobile devices will increase the difficulty for parents to supervise their children's activities on-

---

[149]*See id.*

[150]*See id.*

[151]FTC, Implementing the Children's Online Privacy Protection Act 28 (2007), *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[152]*Id.* at 25–27.

[153]*Id.* at 13.

line.[154] The FTC promised to monitor these developments. Lastly, the FTC concluded that the "failure to develop more secure electronic mechanisms or infomediaries to verify parental consent poses an additional technological challenge."[155]

V. Improving the Effectiveness of Parental Consent in COPPA

Parental consent is the lynchpin of COPPA; rather than adopt a draconian law that prohibited information collection from children, Congress relied upon a flexible approach to obtaining parental consent. Yet, the parental consent formulation of the law has been criticized for being unrealistic, costly,[156] and more beneficial to businesses than to parents.[157] Although several studies subsequently reviewed Web site privacy policy compliance with COPPA requirements,[158] the important issue of parental consent methodologies and effectiveness has not been similarly studied or analyzed. Instead, the FTC anticipated the evolution of a technological solution to more powerfully and effectively support this element of the law, a means that never developed. The following sections review concerns and challenges and describe a possible solution.

A. Initial Concerns Regarding Complexity and Evasion

Debate about the efficacy of COPPA arose soon after its adoption.[159] Criticisms included the cost to businesses, the lack of parental ability to mon-

---

[154]*Id.* at 27.

[155]*Id.* at 29.

[156]Joshua Warmund, *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, 208–11 (2000).

[157]Joseph A. Zavaletta, *COPPA Kids, Cookies & Chat Rooms: We're From the Government and We're Here to Protect Your Children*, 17 Santa Clara Computer & High Tech. L.J. 249, 270–72 (2001).

[158]*See generally* FTC 1998 Report, *supra* note 6; FTC 2002 Report, *supra* note 124. *See also* Tess Koleczek, *Children's Section On Children's Privacy on the Internet*, 6 U.C. Davis J. Juv. L. & Pol'y 79, 85–90 (2001) (containing a short study, including measures, for obtaining parental consent).

[159]*See, e.g.*, Mark. D. Robins, *Coping with COPPA: Privacy, Children, and the Internet*, 17 Computer Law. 17, 17 (2000) (noting that the regulations "represent a highly complex labyrinth of tests, required procedures, exceptions, safe harbors, and traps for the unwary").

itor, and the ease with which children could manipulate consent mechanisms.[160] Dire consequences were predicted; Web sites would simply close their online doors to children under age thirteen because it would be too difficult to comply with the burdensome regulations and too expensive to obtain parental consent.[161] Amid the initial confusion, Disney announced that it would bar children under age thirteen from its chat rooms.[162] From the consumer side, there was concern that the law primarily protected businesses while giving parents, on behalf of their children, neither the tools of control nor the power of enforcement.[163] At this early date, at least one commentator concluded that the parental consent measures were impractical, inadequate, and constitutionally suspect.[164] In contrast, the emphasis on parental involvement led others to believe that the law could be an effective legislative tool to protect children.[165] A period of time after COPPA's effective date however, commentators continued to question whether the consent methods were effective, restating concerns that children would be able to easily enter false ages to avoid restrictive Web sites and that parental involvement was problematic because continuous monitoring was too onerous and burdensome.[166]

B. Current Environment in Light of COPPA

Clearly, Web sites have generally become more careful about collecting information from children after the passage of COPPA. However, the failure to develop a robust technical means to protect children has thwarted

---

[160]*See* Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 547 (2007) (discussing the difficulty of parental monitoring); Warmund, *supra* note 156, at 207–10 (detailing the cost and ease of child manipulation).

[161]*See* Melanie L. Hersh, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831, 1855–68 (2001).

[162]*Id.* at 1866.

[163]*See* Zavaletta, *supra* note 157, at 270–72.

[164]*See* Warmund, *supra* note 156, at 213–16.

[165]*See* Garber, *supra* note 71, at 186–87 ("COPPA serves to increase children's safety online and to protect their privacy in the most effective way that the Internet currently affords").

[166]*See* Allen, *supra* note 37, at 768–69; Rachael Malkin, *How the Children's Online Privacy Protection Act Affects Online Businesses and Consumers of Today and Tomorrow*, 14 LOY. CONSUMER L. REV. 153, 167–68 (2002).

the goal of COPPA regulations regarding parental consent. Children are accessing the Internet more frequently and are visiting a wider variety of Web sites, not all of which are directed at children. Therefore, those Web sites may not employ strong methods of age verification. Businesses are building on the fact that children can affect the purchasing decisions of their family, and are increasingly offering child-oriented activities to general-audience Web sites. In addition, Web sites seem to have overcome their initial misgivings about compliance and the regulatory burden, perhaps in light of the potential commercial value of young consumers. Disney, having initially decided to limit the offerings of its Web sites to children under age thirteen, recently announced the launch of a new site that incorporates new interactivity and increased opportunities for personalization.[167]

In light of the trend for Web sites to become increasingly interactive in order to attract young consumers, one might expect that parallel technologies to protect children and enable parents to control their online activities would also emerge. Such has not been the case. Today, Web sites may have learned from the Xanga case that they should not allow a visitor to go back and reenter a different age, thereby bypassing the verification process, but they have taken few steps beyond the simple use of cookies to prevent this practice. The technical sophistication of children continues to trump these basic techniques,[168] as the basic knowledge of how to clear the cache will allow a child under age thirteen to circumvent the age falsification preventive method of using cookies.

While children become more adept technically, parents seem to fall behind.[169] They are uncomfortable with even basic technical measures, such as using the history browser button to see which sites their child has visited. Parents most often use nontechnical means to monitor their child's Internet usage, such as placing the computer in a common room in the house. Parents are almost completely unaware of the four self-regulatory (safe harbor) programs approved by the FTC. There is little indication that

---

[167]Marr, *supra* note13, at B1.

[168]Although this evidence is purely anecdotal, we have been informed on numerous occasions by students that any ten-year-old boy knows how to clear the browser history button and the cookie file.

[169]Our focus group studies indicated that parents have not heard of the safe harbor groups. *See* Robert Crossler et al., *Parents and the Internet: Privacy Awareness, Practices, and Control*, 2007 Proc. Am.'s Conf. Info. Sys. 3 (on file with authors).

the self-regulatory programs can create any trust by parents who are unaware of their existence.[170] The goal of parental involvement is therefore unassisted by technology or self-regulatory groups. Lastly, parents have no mechanism to individually enforce any deficiencies by Web sites that they might discover. Although the FTC has sought enforcement against high-profile and serious violators, it has limited resources, and has brought only eleven cases in seven years.[171]

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. The regulations anticipated this technical development, and it is essential that these tools develop if COPPA is to become truly effective in protecting children in today's online environment.

C. Conceptualizing Parental Verification and Consent

Conceptualizing the implementation of parental consent is an important step toward determining how to increase the effectiveness of COPPA regulations in order to meet the goal of protecting children online. The operation of Web sites today, under COPPA, can be expressed by the illustration in Figure 1, showing that the Web site and the child are the primary parties in direct communication.

As the illustration shows, the Web site is responsible for obtaining consent from the parent. The means of obtaining parental consent puts the Web site in the middle of the process, between the parent and the child, quite different from the original intent under COPPA that anticipated that the involvement of the parent with the child would act as an educational and monitoring function. Figure 1 also shows that the Web site is in charge of the communications. The parent could communicate with the Web site and grant or deny consent and the child may never be directly involved with the parent. Of course, the parent will know of the child's interest and will have the opportunity to discuss the decision and the online activities

---

[170] *Id.*

[171] The FTC Web site has a list of these cases. FTC Privacy Initiatives, http://ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Mar. 21, 2008).

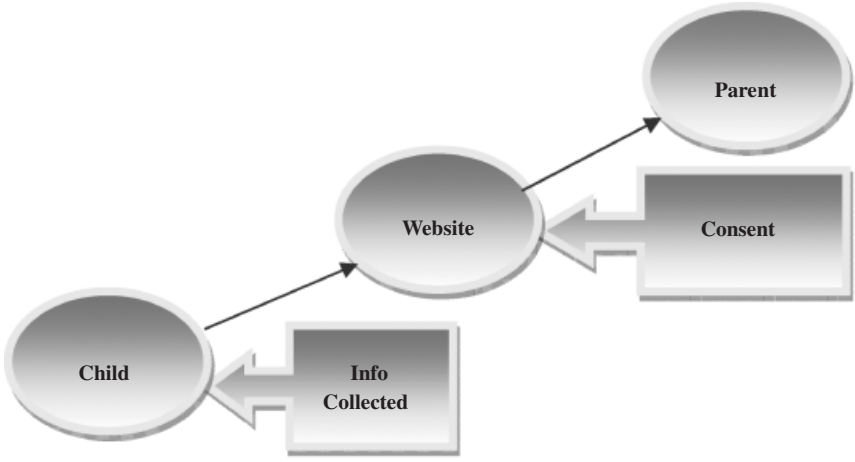

Figure 1. Present Consent Mechanism

with the child later. And, as the Xanga case shows, if COPPA compliance fails, the parent will be unaware of the violation and unable to provide a buffer between the Web site and the child to prevent the information collection.

However, consider the rearrangement of the process shown in Figure 2, which would change the dynamics of the interaction between child, parent, and Web site.

Obviously, if the parent could be involved with the transaction between the child and the Web site, providing a mature and protective influence, then it would satisfy the intent of COPPA and provide protection for the child. The reality is however, that parents cannot always be present, mediating every Web interaction, when their child is online.

If technology could provide a means for mediation, it could act as an automatic predetermined proxy for the mature decision making of the parent regarding information collection.

The conceptual illustration shown in Figure 3 proposes that it would be possible for technology to allow a parent to control the child's ability to share information by software installed on the computer, blocking access to the Web site unless the Web site meets the requirements preset by the parent. If the child wishes to access the site, then he/she will need to ask the parent to unblock the site, thereby instigating the communication between

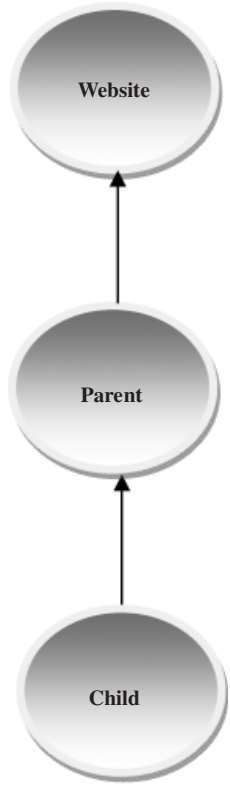

Figure 2. Parental-Mediated Consent

parent and child about online activities. The heavier arrow between the Web site and the computer indicates that the information collected by the Web site is only that allowed by the parent, and the Web site collects no information directly from the child.[172]

---

[172]The technology of P3P is a related example of this concept; however, it does not include exchange of specific, user-generated information between the user and the Web site in the transaction. The weakness of P3P is that it does not account for the necessary authentication and security when information may be exchanged on an open network. For a basic description of P3P, see Mary Anne Patton & Audun Josan, *Technologies for Trust in Electronic Commerce*, 4 Elec. Com. Res. 9, 12–13 (2004).

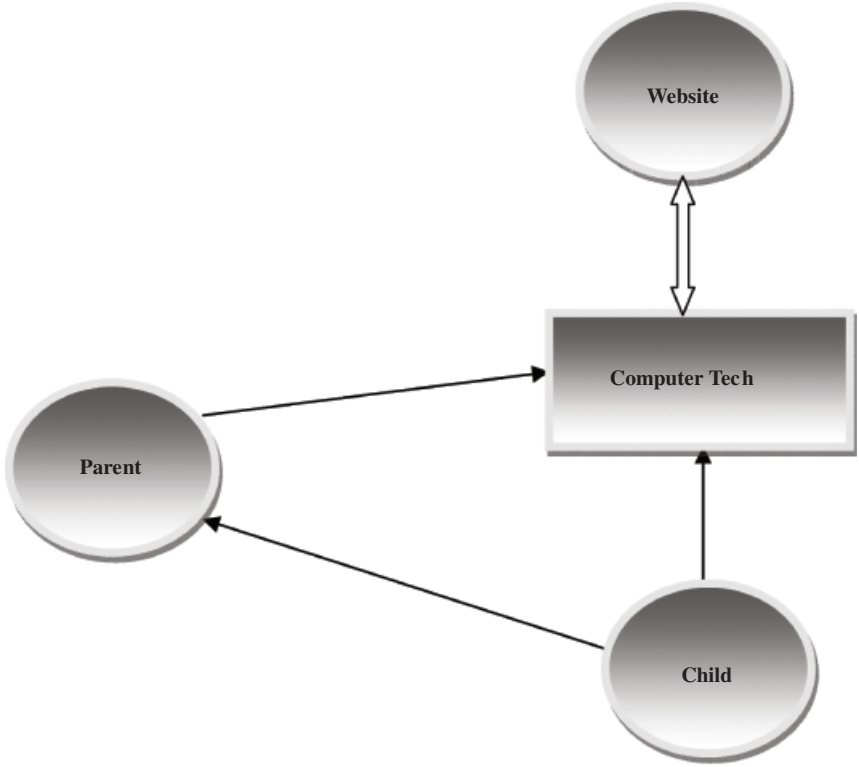

Figure 3. Technology-Aided Consent

D. A New Technical Concept: POCKET

POCKET is a proof-of-concept[173] system we developed that would allow for the implementation of the concept described above in a more sophisticated and robust manner. POCKET is a technical solution to obtaining parental consent. In the following section, the system is described briefly, in a nontechnical manner, to show how it would meet the conceptual needs of COPPA, obtain parental consent, and protect children. The benefit of the POCKET system is that it puts control back in the hands of the parent, making the parent the focal point of child protection, as originally envisioned in COPPA.

---

[173]A proof of concept is not a fully developed product; it functions in the lab environment to show that it is technically possible to achieve the result.

POCKET is composed of two parts, the parent/child side and the Web site side, and consists of two stages, the registration stage and transaction stage. In the registration stage the parent must first obtain and install the software on the home computer that is used by the child. The software will work through the browser on the home computer to implement the system. When the parent obtains the software he or she must provide identification and register, creating a password that will be used in any future interactions. The merchant installs similar POCKET software, thereby allowing automatic communication between the two parties (by computer interactions). During the registration process, the parent enters specific choices about what information about the child may be collected and whether the information may be shared. The Web site also specifies its information collection and sharing practices during its registration process.

In the transaction phase, when a child visits a Web site, the parent/child POCKET software interacts automatically and transparently with the merchant POCKET software, identifying that there is a user under the age of thirteen[174] and implementing preset instructions about what personally identifiable information, if any, can be given to the Web site and whether the information can be shared. If the Web site requests information through POCKET that does not match the choices made by the parent on behalf of the child, then POCKET automatically blocks the Web site. If the Web site collection and parent preferences match, then POCKET automatically transfers the child's information from the child's computer to the Web site. A log is kept on the parent/child's computer so that the parent can check at any point in time to determine where the child has visited and what information has been shared. The system is illustrated conceptually in Figure 4.

---

[174]In addition, POCKET also addresses the issue of security and trustworthiness between the parent/child and Web site computers. POCKET incorporates transparent authentication protocols so that the Web site can be assured that the information that is transferred from the child's computer is authentic and secure. As the parent/child's computer transfers information to the Web site, the POCKET system acts as the trusted third party, the certificate authority, to incorporate a digital signature based on public key encryption to identify the sender. This is important because the Internet, being a public and open architecture, is not a secure environment. Others may intercept and change the communication, potentially attacking the Web site and endangering the child's information, unless security measures are taken. The use of a "ticket," the combination of the digital signature attached to the message, is a process that ensures the integrity of the message and provides for nonrepudiation. Importantly, the use of the ticket is automated and requires no additional action by the parent.

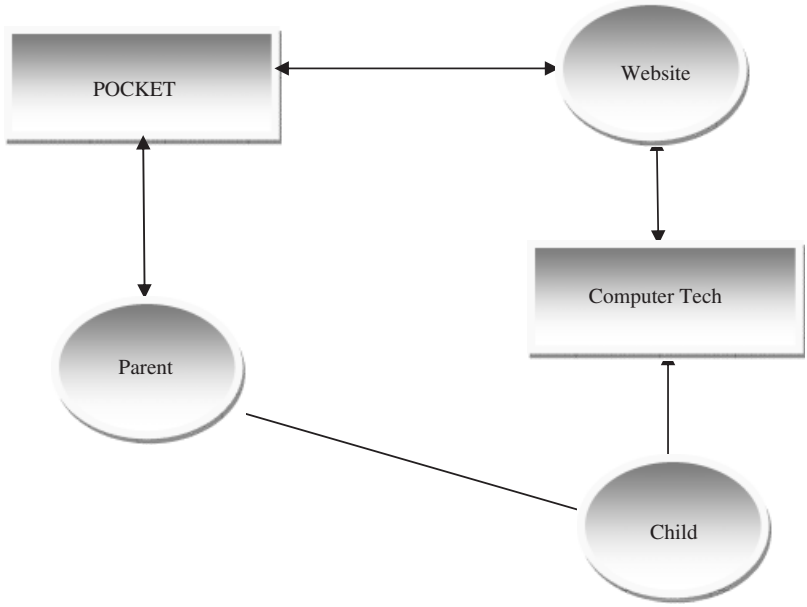

Figure 4. Robust POCKET-Aided Consent

As noted by the FTC, falsification of age by children is a problem that needs attention. Although the conceptual POCKET system does not address the issue directly, it is an example of an effective approach. Because the child's computer queries the Web site with POCKET, it indirectly communicates that a child under the age of thirteen is seeking to visit that site. Thus, the thorny problem of how to prevent a child from circumventing age verification procedures is solved by giving parents a method for signaling that the Web site visitor is a young child. POCKET's password system prevents the child from circumventing the technology of control.[175]

Lastly, identification of a parent, for purposes of consent, is important. Although POCKET does not incorporate a particular form of identification technology, it is designed to utilize a more secure method of identification upon the parent's registration. The present methods used by

[175]Many Web sites use cookies to prevent the child from reentering a site and trying to register at an older age. Children are adept at knowing how to clear the cookies file and circumventing this basic technology. Similarly, sometimes the age identification process can be fooled by simply reloading the Web page.

most Web sites are rather simplistic and do not rely on sophisticated methods of identification. In fact, it would be cost prohibitive to require these methods of identification for every time a child visited each individual Web site. POCKET allows for a more sophisticated method of identification to be used once, when the parent registers, and from that time forward the parent's choices are implemented by the software. Future changes are instituted only with the parent's password. No individual Web site is required to obtain direct parental identification. This accomplishes two goals: it implements a more secure parental consent mechanism and it is cost efficient for the Web site.

POCKET helps a parent to limit information sharing by a child by automating the decision and consent process. It gives a parent a way to be technically present when he or she is unable to be physically present. In sum, this proof of concept shows that presently available technology *can* be implemented to achieve a strong parental consent mechanism and to protect children.

E. Possible Approaches to Strengthening COPPA

The history of the adoption of COPPA, and the subsequent regulatory review of parental consent mechanisms, contains evidence of compromise and a deference to market mechanisms. From the beginning, the Senate cosponsor of the bill described the process as "consensus" building and noted the "participation of the marketing and online industries, the Federal Trade Commission, privacy groups, and First Amendment organizations."[176] The consensus led to the first constitutional privacy protection law for children online, and to changes in Web site operation that gave notice to parents and limited information collection from children. These accomplishments are significant and should not be minimized. Subsequent years without progress toward a technical solution for protecting children, however, reveal the inherent weakness in COPPA's lack of standards. Senator Bryan unsuccessfully proposed privacy legislation at the same time as COPPA, describing the approach: "[If] technological tools don't exist, or where a particular industry refuses to embrace this code . . . then the gov-

---

[176]*See* 144 Cong. Rec. S12741-04 (1998) (remarks of Sen. Bryan introducing the Senate version of the bill).

ernment is obliged to step in and reinforce protection of privacy rights."[177] The POCKET proof of concept shows that presently available technology exists to help parents protect their children's personal information, however, market incentives to implement technology improvements are lacking. As we approach a decade of study, legislation, and regulations to protect children's privacy, it may be time to address these technical failures with renewed regulatory guidance.

The FTC applies a test of reasonableness to whether a technical system should be required for obtaining parental consent; in order to be required, the system must be widely available and cost efficient.[178] If the FTC continues to rely only on the private sector to develop technology that meets this test, it is unlikely that there will be progress toward a technical solution, in part because there is no incentive for businesses to develop a technology while the FTC continues to accept the minimalist sliding-scale approach. Under the present regulatory regime, only FTC enforcement actions provide an incentive for businesses to develop a more sophisticated technical means of compliance. While businesses incur an economic risk by violating the regulations, as illustrated by the $1 million fine against Xanga, the risk is minimized because the FTC has limited resources to monitor Web sites for compliance, and parents have no individual right of action for a violation of the law. The Xanga site violations, although eventually uncovered, occurred over a five-year period. This case of delayed discovery illustrates that enforcement is significantly limited, and therefore, consequently, the incentive for business to adopt new technology is weak.[179]

The FTC should consider multiple, additional methods for spurring the adoption of technology to protect children online. Regulations that utilize technology to protect consumers, or gain efficiency, already exist in

---

[177] *Id.*

[178] Standardized technology would likely require a "massive educational effort . . . [and would need to be] compatible with most Internet sites, relatively easy for consumers to use, and difficult for data seekers to evade." *See* James P. Neff, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 60 (2003).

[179] It is worth considering whether parents, with a natural incentive to protect their children, might champion the development of the technology for their benefit. Although parents are more sophisticated and knowledgeable than their children in general matters, they are usually less proficient in the use of computers and technology. It is unlikely that parents could effect the change necessary for technical solutions. In fact, the potential adoptability of any technology will depend on an interface that is very easy for parents to use. *See* Crossler, *supra* note 169.

other technology-related areas. The FTC's do-not-call registry for phone solicitations is a successful example of a governmental, centrally operated solution. The majority of citizens have chosen to opt out of telephone solicitations[180] by joining a list that is maintained by the FTC.[181] A business must register with the National Do Not Call Registry, pay fees based on the number of area codes used, and download a list of telephone numbers from which it may not solicit by phone.[182] The business is free internally to choose the technology that will work best with the opt-out list. Other examples of government-supported technical solutions abound. Television broadcasters are required to provide closed captioning in order to provide access to viewers who are deaf.[183] In a more complex environment, individuals and businesses may file electronically with the Internal Revenue Service (IRS), through a system known as the Electronic Federal Tax Payment System.[184] The system for participating in the electronic filing is free and made available by the U.S. Treasury. More options for electronic payment are available through commercial software that may have additional enterprise benefits, but that software must meet technical standards established by the IRS.[185]

The FTC could make parental consent technology freely available or, in the example of POCKET, operate the server necessary for the process and allowing the business to design technology that will work best internally. Similarly, one or more safe harbor programs could also provide this service. However, the safe harbors do not have the same recognition by the public as the FTC, nor do they have the established consumer trust that made the FTC do-not-call regulation effective. The safe harbor programs do, however, have connections with children's Web sites and accountability

---

[180]*See* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 Notre Dame L. Rev. 583, 612 (2006).

[181]The FTC list can be found at the National Do Not Call Registry, *available at* https://telemarketing.donotcall.gov (last visited Mar. 27, 2008).

[182]The process is described on the "Create a Profile" page of the National Do Not Call Registry, https://telemarketing.donotcall.gov/profile/create.aspx (last visited Mar. 27, 2008).

[183]*See* Kesan & Shah, *supra* note 180, at 628–29.

[184]*See* Electronic Federal Tax Payment System, http://www.irs.gov/efile/article/0,,id=98005,00.html (last visited Mar. 27, 2008).

[185]The options available are listed on IRS e-file, http://www.irs.gov/efile/index.html (last visited Mar. 27, 2008).

mechanisms. A combination of FTC sponsorship or standard setting, and safe harbor requirements for business members, could prove to be the most effective and cost-efficient approach.

VI. Conclusion

Children are online at an increasingly young age, and they are subject to increasing dangers because of the evolving online environment of interactivity and social networking. MySpace exceeded the page views of Google and eBay years ago, and the AMA advises doctors to warn parents about potential Internet dangers.[186] Although the Internet brings rich content to children and expands their horizons, at the same time it also creates dangers and risks to their privacy and well-being. For the better part of a decade, the FTC championed the protection of children's privacy online. The FTC predicted since its COPPA regulations in 2000 that technology would provide the answer to protecting children online, yet no technology solution emerged. Clearly, Internet and communications technology have progressed rapidly and significantly in over seven years, yet protection of children's privacy seems to have been left behind. The goals of COPPA, to encourage the participation of parents in the online activities and decisions of their children and to facilitate the method of obtaining verifiable parental consent, can be accomplished with the aid of presently available technology, as illustrated by the POCKET proof of concept. POCKET shows that technology can empower parents to protect their children, yet incentives are lacking for businesses to develop similar, commercially available technology. Revised regulations could provide the incentives needed to spur the market to develop technology to protect children, technology that seemed so near when COPPA was initially adopted. Millions of children are online every day; protecting the richness of that experience while providing for the safety of their interaction is a parental goal that should be supported by the intersection of effective regulation and available technology.

---

[186] *See supra* note 12.