

NOTE

Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act

Joshua Warmund*

INTRODUCTION

Over recent years, Internet-based commerce has experienced considerable growth. Today, almost every business recognizes the need to incorporate the Internet into its business model. Beyond providing financial efficiency, the Internet serves as an unprecedented commercial tool for businesses to market and sell products.

Many of the businesses and commercial entities on the Internet contain websites with chat rooms, discussion boards, instant messaging capability, and forms of technology that collect registration and other information from site visitors. Further, because of the nature of their products, many sites target children as their customers. Other sites find curious children among their visitors, although the sites do not direct their content to children.

Indeed, children represent a large and rapidly growing segment of online consumers.¹ As of 1998, almost 10 million U.S. children had online access, with over 4 million using the Internet from

* Cornell University, B.A., 1996; Fordham University School of Law, J.D., 2000. The author thanks Andrew Goldner and Prof. Joel Reidenberg for their helpful comments. Many thanks to Thaddeus J. Tracy for his editorial assistance.

¹ See Interactive Consumers Research Report, Vol. 4, No. 5, at 1, 4 (1997) (discussing results of FIND/SVP's 1997 American Internet User Survey). Children use the Web for a wide variety of activities, including 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. *Id.*

school and 5.7 million from home.² Children are also avid consumers and represent a large and powerful segment of the marketplace.³ Their growing presence online, therefore, creates enormous opportunities for marketers to promote their products and services to an eager audience.⁴ Some commentators, however, submit that children under the age of thirteen do not have the developmental capacity to understand the nature of a website's request for information and its privacy implications.⁵ As a result, many commentators have advocated governmental regulation in an effort to safeguard children's privacy interests when they provide personal information over the Internet.⁶

² See *id.* at 1, 2 (noting that the number of children online increased nearly five-fold from Fall 1995 to Spring 1997).

³ See James U. McNeal, *Tapping the Three Kids' Markets*, AMERICAN DEMOGRAPHICS (Apr. 1998) (visited May 12, 2000) <http://www.demographics.com/Publications/AD/98_ad/9804_ad/ad980429.htm> (estimating that billions of dollars a year are spent in marketing to children to influence the expenditure of billions more). For example, in 1997 children aged 4 through 12 spent U.S. \$24.4 billion themselves and children aged 2 through 14 may have directly influenced spending by their parents in an amount as much as U.S. \$188 billion. *Id.*

⁴ See Robin Raskin, *What do Kids Want?*, FAMILY PC MAGAZINE, May 1998, at 17 (noting that most children's websites target children ages 8 to 11). Teens tend to visit the same sites that adults visit. *Id.*; see also *Pre-Teen Publishers Ponder Privacy and Payment Puzzles*, Min's New Media Report (Apr. 10, 2000) available in LEXIS, News Library, Philips File (reporting that pre-teen market represents "most wired and affluent generation in human history"). Pre-teens have not been able to buy online in the past and merchants have a chance to capture them as loyal customers by partnering with a website that permits online shopping. *Id.*

⁵ See Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,900 (noting American Psychological Association study); see also Lynn Burke, *A Chilling Wave Hits Schools*, Apr. 5, 2000, <<http://www.wired.com/news/print/0,1294,35299,00.html>> (reporting that children 12 years old and younger might fill out website information request forms in order to receive prizes without understanding that such prizes are obtainable without providing personal information). For instance, an 11-year old using the e-mail program of the Working Against Violence Everywhere program must provide his or her state, gender, age, and selected educational and vocational goals before receiving the fee e-mail feature. *Id.* Importantly, a child of this age may have no sense of when he or she should protect his or her identity. *Id.*

⁶ Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,889 (noting Federal Trade Commission ("FTC") comment period in response to creation of Children's Online Privacy Protection Act ("COPPA")). The FTC's comment period yielded 14 comments from different industry sources. *Id.*; see also *Consumer Privacy On The World Wide*

On October 21, 1998, President Clinton accordingly signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA" or the "Act").⁷ The intent of the Act is to regulate the collection and use of personally identifiable information from children under the age of thirteen ("children") via the Internet.⁸ The Act directs the Federal Trade Commission (the "FTC") to put rules into operation that effectuate the Act's mandates. The FTC issued its final rules (the "Rules") in October 1999 and the Act became effective on April 21, 2000.⁹

Web, Hearing Before The House Comm. on Commerce, Subcomm. on Telecommunications, Trade and Consumer Protection, July 21, 1998, 105th Congress (testimony of Robert Pitofsky, Commissioner of the FTC) (last visited Mar. 30, 2000) <<http://www.ftc.gov/os/1998/9807/privac98.htm#N7>> [hereinafter *Consumer Privacy*] (noting that consumers are especially concerned about collection of personal information from children). As Commissioner Pitofsky explained:

These practices raise especially troubling privacy and safety concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent. Indeed, consumers strongly favor limiting the collection and use of personal information from children online. A recent survey showed that 97% of parents whose children use the Internet believe Web sites should not sell or rent personal information relating to children, and 72% object to a Web site's requesting a child's name and address when the child registers at the site, even if such information is used only internally.

In sum, it is clear that consumers care deeply about the privacy and security of their own, and their children's, personal information in the online environment and are looking for greater protections. Until meaningful and effective consumer privacy protections are implemented in the online marketplace, consumers may remain wary of engaging in electronic commerce, and this new marketplace will fail to reach its full potential.

Id. (testimony of Robert Pitofsky, Commissioner of the FTC) (citations omitted).

⁷ 15 U.S.C.A. §§ 6501 - 6505 (1999).

⁸ See Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (1999) (implementing COPPA). This section prohibits "unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet." *Id.*

⁹ *Id.*; see also Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,889 (noting FTC's position in drafting final Rule).

For its part, the FTC has taken very seriously the concerns expressed about 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. The Commission believes that the final Rule strikes the

This Note examines the adequacy of COPPA's suggested parental consent measures in light of the Act's overall goal to protect children's privacy interests. Part I discusses the impetus and intent behind the creation of COPPA. This Part also outlines the structure of the Act and defines some of its key terms. Part II focuses on COPPA's parental consent measures, evaluating their content, form, and adequacy. Part III argues that the parental consent measures prescribed by the Act are impractical and inadequate methods to protect children's privacy interests. This Note concludes that COPPA ultimately fails as a form of federal regulation because it does not serve to improve commercial practices and activity—it serves drastically to impair them.

I. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998

A. *The Impetus to Create COPPA*

In May 1996, a consumer watchdog group known as the Center for Media Education petitioned the FTC to investigate the online website KidsCom.com (“KidsCom”) and bring an enforcement action against it, asserting that KidsCom's data collection practices violated section 5 of the Federal Trade Commission Act¹⁰ concerning unfair/deceptive trade practices.¹¹ In July 1997, the FTC completed its investigation and issued its findings in an enforcement letter (the “KidsCom Letter” or “Letter”).¹² The FTC

appropriate balance between these concerns and the Act's goals of protecting children's information in the online environment. It looks forward to continuing to work with industry, consumer groups, and parents to ensure widespread compliance in as efficient a manner as possible, to educate the public about online privacy protections, and to assess the Rule's effectiveness on a periodic basis.

Id.

¹⁰ 15 U.S.C. § 45(a)(1) (1994). Section 5(a) of the FTC Act provides that “unfair or deceptive acts or practices in or affecting commerce are declared unlawful.” *Id.*

¹¹ Parry Aftab & Nancy Savitt, *Children, Data and the Web; New Rules Stress Privacy, Safety*, N.Y.L.J., Nov. 15, 1999, at T4 (reporting that KidsCom collected information from children without accurately disclosing purpose, and that it failed to disclose that it was paid to endorse certain products).

¹² Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc., FTC Letter, (last visited Mar. 30, 2000)

determined in the letter that KidsCom's disclosure practices were inadequate and misleading.¹³ In issuing this ruling, the FTC publicly announced its guidelines for data collection from children on the Internet for the first time.¹⁴ Furthermore, after the FTC

<<http://www.ftc.gov/os/1997/9707/cenmed.htm>> [hereinafter *KidsCom Letter*]. In its letter, the FTC concluded that:

[I]t would likely be an unfair practice in violation of Section 5 to collect personally identifiable information, such as name, e-mail address, home address or phone number, from children and sell or otherwise disclose such identifiable information to third parties without providing parents with adequate notice . . . and an opportunity to control the collection and use of the information.

Id.

¹³ *Id.* The FTC noted that:

It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect.

Id.; see also Aftab & Savitt, *supra* note 11 (describing how FTC declined to take punitive action against KidsCom, however, since it had already changed its data collection practices and cooperated in the investigation).

¹⁴ See *KidsCom Letter*, *supra* note 12 (stating that KidsCom shared information collected from children at its website with third parties); see also Aftab & Savitt, *supra* note 11. The shared information was provided to third parties only in an anonymous, aggregate form. *KidsCom Letter*, *supra* note 12. In issuing its decision, The FTC relied on section 5 of the Federal Trade Commission Act (the "FTC Act"), that prohibits unfair and deceptive practices. *Id.* The FTC stated its four principles relating to data collection from children online. *Id.* The first principle was stated as follows:

It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect.

Id. The second principle stated that adequate notice must be given to a parent when collecting personally identifiable information from a child, because of the child's limited ability to understand the disclosure. *Id.* "Adequate notice" requires disclosure of (1) who is collecting the personally identifiable information; (2) what information is being used and for what purpose it is being used; (3) whether it will be disclosed to third parties, and if so, to whom and in what form; (4) how parents can prevent the "retention, use or disclosure" of that information. *Id.* The third principle generally concerns safety. *Id.* Section 5 of the FTC Act deems a practice unfair if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition. *Id.* This test applies to Internet child safety because the disclosure of a child's personal information introduces the risk

issued the KidsCom letter, it broadened its principles to include offline consent for children twelve years old and younger as well as any personal information shared online, in chat rooms, or in similar third-party communications.¹⁵

In March 1998, the FTC presented its Privacy On-Line Report to Congress, documenting the online collection of personal information from children.¹⁶ In its report, the FTC informed Congress of the need for parents to better understand the risks to their children's privacy on-line, as well as the need for parental consent concerning the collection and disclosure of their children's personal information.¹⁷ Congress enacted COPPA in October 1998 in response to this Report, and in light of the evidence of continued lack of industry compliance with the principles articulated in the KidsCom letter.¹⁸

B. COPPA's Mandates

Under the Act, operators of websites directed at children, or who knowingly collect personally identifiable information from

that a third party may harm the child. *Id.* The FTC's fourth principle criticized KidsCom's endorsement practices as misleading and deceptive. *Id.* Specifically, KidsCom failed to clearly and conspicuously disclose that the product information it displayed to children was in fact solicited from manufacturers and printed in exchange for in-kind payment. *Id.*

¹⁵ See Aftab & Savitt, *supra* note 11 (explaining that FTC jurisdiction extends to any site that collects and stores children's personal information, even an e-mail address).

¹⁶ See *Internet Privacy*, Hearing before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property, Mar. 26, 1998, 105th Congress (testimony of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, FTC) (last visited Mar. 30, 2000) <<http://www.ftc.gov/os/1998/9803/privacy.htm>> [hereinafter *Internet Privacy*] (reporting that collection of information from and about children who use the Internet deserves "special attention"); see also Aftab & Savitt, *supra* note 11 (noting FTC's concerns that collection of personal information from children under the age of 13 without informed parental consent would be deceptive trade practice). The FTC reported to Congress that even in chatrooms, children innocently and without request may reveal where they live or go to school or their real e-mail addresses. *Id.*

¹⁷ *Internet Privacy*, *supra* note 16 (testimony of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, FTC).

¹⁸ Aftab & Savitt, *supra* note 11; 15 U.S.C. §§ 6501 - 6505 (1999).

children, are required to (1) provide notice¹⁹ on their website of their information collection practices;²⁰ (2) obtain verifiable parental consent for the collection, use and/or disclosure of personal information from children;²¹ (3) provide a parent, upon request, with the ability to review the personal information collected from a child;²² (4) provide a parent, upon request, with

¹⁹ See Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4 (1999) (describing necessary notice practices under COPPA). Section 312.4 states that:

[A]n operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children.

16 C.F.R. § 312.4(b) (1999). The link to the notice must be conspicuous and it must clearly state that it concerns the online service's information practices regarding children. 16 C.F.R. § 312.4(1)(i)-(iii); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,894 (1999). The FTC has interpreted this to mean that the link must stand out and be noticeable to the website's visitors through, for example, a larger font size in a different color on a contrasting background. 64 Fed. Reg. at 59,894. Importantly, the FTC does not consider a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links as sufficient under this provision. *Id.* The content of the notice must state the "[t]he name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service." 16 C.F.R. § 312.4(2)(i).

Further, the notice must state the types of personal information collected, § 312.4(2)(ii), how it is to be used, § 312.4(2)(iii), and disclosure practices. § 312.4(2)(iv). Last, it is instructive to note that the FTC has applied a "reasonable consumer" standard in evaluating whether a notice is clearly and understandably written. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,894 n.91. Because the notices required by the Act are intended for parents, the Commission will look at whether they are written such that a reasonable parent can read and comprehend them. 64 Fed. Reg. at 59,894 n.91.

²⁰ See Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,894 n.95 (noting that several commentators supported use of other mechanisms for providing notice, such as pop-up or interstitial pages, which typically appear temporarily when visitors move from one part of a website to another). Pop-up or interstitial pages, however, will only satisfy the notice requirements if they are clear, prominent, and easily accessible to users, *i.e.*, they do not disappear after the initial viewing or users can re-access them through a clear and prominent link on the home page. *Id.*

²¹ See 16 C.F.R. § 312.5(a)(1) (stating that the website provider must obtain verifiable parental consent "before any collection, use, and/or disclosure of personal information from children"). Parental consent is also necessary for any material changes to the collection, use, or disclosure practices that occur thereafter. *Id.* See *infra*, Part II and III for a more detailed analysis of this section.

²² See 16 C.F.R. § 312.6(a) (stating that the operator of a website or online service

the opportunity to prevent the use or maintenance of personal information that was collected on or after April 21, 2000, or the future collection of personal information from that child;²³ (5) limit collection of personal information required for a child's participation in an online game, prize offer, or other activity to information that is reasonably necessary for the activity;²⁴ and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children.²⁵ Importantly, the Act establishes a "reasonableness" standard as the proper measure of compliance.²⁶

C. Key Definitions of COPPA

The mandates of the Act only apply to operators of websites or online services that are either directed to or that collect personal information from children. Importantly, website operators must

must provide a child's personal information to parent for parent's review). Upon request of the parent, the online service operator must provide "[a] description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities" 16 C.F.R. § 312.6(a)(1).

Furthermore, the online service operator must ensure that the person requesting the information is, in fact, the parent of the child, § 312.6(a)(3)(i), and that the means employed to carry out this provision are not unduly burdensome. *Id.*

²³ 16 C.F.R. § 312.6(a)(2) (noting that parent must be provided "[t]he opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information"). Furthermore, "an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information." 16 C.F.R. § 312.6(c).

²⁴ See 16 C.F.R. § 312.7 (stating that "[a]n operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.").

²⁵ See 16 C.F.R. § 312.8 (entitled "Confidentiality, security, and integrity of personal information collected from children").

²⁶ See 16 C.F.R. § 312.2 (requiring website operators to make a "reasonable" effort to obtain verifiable parental consent); 16 C.F.R. § 312.4(c) (providing that website operators must make "reasonable" efforts to ensure that parents receive notice of the website's practices concerning the collection, use, or disclosure of children's personal information); 16 C.F.R. § 312.6(b) (providing safeharbor for website operators who follow "reasonable" procedures in disclosing personal information for parental review).

adequately secure their site in order to ensure the integrity and confidentiality of the child's online information. The exact meaning of COPPA's provisions, however, is best understood in light of their definitions.

1. "Operator"

To be an operator, the website must be used for commercial purposes, and must collect or maintain personal information from or about its users.²⁷ The Rules broadly define an operator to include all persons who operate a website, as well as those on whose behalf such a website is hosted and/or maintained.²⁸ Where more than one party has access to, or control over information collected, all are jointly and severally responsible for satisfying the mandates of the Rules.²⁹

2. "Directed at Children"

The FTC considers a number of different factors when

²⁷ See 16 C.F.R. § 312.2 (stating that "collecting" information concerns gathering "any personal information from a child by any means"). The means by which information can be collected includes requesting that the child submit personal information. *Id.* Other means include "[e]nabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records"

Id. Utilizing cookies to identify the child also falls under this definition. *Id.*

²⁸ *Id.* Operator is defined as:

[A]ny person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce.

Id. But see Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 59,891 (1999) (noting that entities which merely provide access to the Internet, without providing content or collecting information from children, are not considered operators). Thus, ISPs and cable operators that offer Internet access are not "operators" under the Rule. 64 Fed. Reg. at 59,891 n.52. One wonders whether online auctioneers fall under this definition.

²⁹ 16 C.F.R. § 312.2. An operator can include any "individual, partnership, corporation, trust, estate, cooperative, association, or other entity." *Id.*

determining whether a website or online service, or any portion thereof, is directed at children.³⁰ While none are dispositive, the FTC will consider (1) whether a designated children's area exists;³¹ (2) the subject matter, visual or audio content, age of model, if any, language or other similar characteristics;³² and (3) whether games, puppets, animated characters or other child-oriented activities and incentives are used.³³

An operator of a general interest website or online service that is partially directed to children is required to satisfy the mandates of the Rules for only that portion of the site which is directed at children.³⁴ If the website or online service is not directed at children, the operator will, nonetheless, be subject to the mandates of the Act if the operator knows that particular users are under the age of thirteen.³⁵

³⁰ See *id.* (explaining that a “[w]ebsite or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children”). A commercial website or online service, however, is not subject to this provision “solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.” *Id.*

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ See *id.* (modifying the scope of its provisions to commercial websites, online services, or “portions thereof”); Children’s Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,893 (1999) (stating that “if a general audience site has a distinct children’s ‘portion’ or ‘area,’ then the operator would be required to provide the protections of the Rule for visitors to that portion of the site”).

³⁵ See 16 C.F.R. § 312.2 (noting that the Commission considers as “competent and reliable empirical evidence” the intended audience of the website); see also Children’s Online Privacy Protection Rule, 64 Fed. Reg. at 59,893 (describing one commentator’s concern that operators should not be able to construct “veil of ignorance” where operator can determine through questions whether visitor is a child without specifically asking for visitor’s age). The FTC has responded, however, that it will closely examine such sites to determine whether they have actual knowledge that they are collecting information from children. 64 Fed. Reg. at 59,894. Similarly, issues arise for websites that ask for age ranges that include both children and teens (*e.g.*, a “15 and under” category). *Id.* Since website operators can easily craft a “12 and under” age range, the FTC has vowed to closely inspect those websites that do not offer such a range if it appears that their operators are trying to avoid compliance with the Rule. *Id.*

3. “Personal Information”

The Act enumerates several forms of individually identifiable information that qualify as “personal information.”³⁶ Furthermore, the Act authorizes the FTC to expand the definition to include other identifiers that permit physical or online contacting of a specific individual. Specifically, the Rules list (1) a first and last name;³⁷ (2) a home or other physical address including street name and name of a city or town;³⁸ (3) an e-mail address;³⁹ (4) a telephone number;⁴⁰ (5) a Social Security number;⁴¹ (6) any persistent identifier associated with personal identifiable information;⁴² or (7) information concerning the child or the parents of that child that the operator collects online from the child and combines with a persistent identifier.⁴³

³⁶ See 16 C.F.R. § 312.2 (describing personal information as “individually identifiable information about any information collected online”). Conversely, operators are not required to provide parental notice or seek parental consent for collection of non-individually identifiable information that is not and will not be associated with an identifier. *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ See *id.* (identifying personal information as an “e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual’s e-mail address”).

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² See *id.* (stating that a persistent identifier includes cookies). The Act identifies personal information as “[a] persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical online contracting. . . .” 16 C.F.R. § 312.2. This provision has raised the question of whether operators must ensure that a screen name chosen by a child does not contain individually identifiable information. Children’s Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,892 n.66 (1999). The FTC has stated that website operators do not have a specific duty to investigate whether a screen name contains such information. 64 Fed. Reg. at 59,892 n.66. However, an operator could give children warnings about including such information in screen names, especially those screen names that will be disclosed in a public forum such as a chat room. *Id.*

⁴³ 16 C.F.R. § 312.2; see also Children’s Online Privacy Protection Rule, 64 Fed. Reg. at 59,892 (noting that non-individually identifiable information, e.g., information about a child’s hobbies or toys, can be associated with an identifier and, thus, fall under this provision). Some child advocacy groups have suggested that the FTC remove the

4. Confidentiality, Security, and Integrity of Personal Information

The Rules require an operator to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.⁴⁴ More specifically, operators must maintain adequate policies and procedures for protecting children's personal information from loss, misuse, unauthorized access, or disclosure.⁴⁵ Such protections may include (1) designating an individual in the organization to be responsible for maintaining and monitoring the security of the information;⁴⁶ (2) requiring passwords to access the personal information;⁴⁷ (3) installing firewalls;⁴⁸ (4) utilizing encryption;⁴⁹ (5) implementing access-control procedures in addition to passwords;⁵⁰ and/or (6) storing the information on a

phrase "collected online" from this provision in order to cover information that is submitted to an operator offline, then posted online by the operator. 64 Fed. Reg. at 59,893 n.71. While cognizant of the risks posed by such practices, the FTC declined to expand COPPA to information submitted to an operator offline. *Id.*

⁴⁴ 16 C.F.R. § 312.8.

⁴⁵ Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,906.

⁴⁶ *Id.*; see also 16 C.F.R. § 312.4 (stating that in order for notice to be complete, a website operator must provide information concerning all operators collecting or maintaining personal information from children through his/her website). Alternatively, the website operator may:

[L]ist the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice.

16 C.F.R. § 312.4(b)(2)(i). *But see* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,895 (noting that data-sharing relationships in online world change rapidly, and that this provision therefore causes undue burden on website operators to revise their parental notices with each change). During the comment period, the FTC agreed with those commentators that believed that it would be burdensome for website operators to send numerous updated notices to parents. 64 Fed. Reg. at 59,895. Therefore, the FTC modified this provision to require a new notice to the parent only where there would be a material change in the collection, use, and/or disclosure of personal information from the child. *Id.*

⁴⁷ Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,906 n.284.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

secure server that is not accessible from the Internet.⁵¹ Adherence to the Act's "reasonableness" standard⁵² would dictate using at least the customary form of such protection, not an out-of-date version or level of protection.

II. A CLOSER LOOK: METHODS OF PARENTAL CONSENT SUGGESTED IN COPPA

Because of particular interest among commentators concerning how to obtain verifiable parental consent under the Rule, the FTC conducted a public workshop on July 20, 1999 in order to obtain additional information and learn more about the views expressed.⁵³ The thirty-two panelists at the workshop included representatives from the Internet industry (including website operators and technology companies), as well as privacy advocates, consumer groups, and representatives of other government agencies.⁵⁴ Approximately 100 other parties also attended the workshop.⁵⁵ Panelists discussed methods of obtaining verifiable parental consent that are currently in use, whether and how e-mail could be used to obtain verifiable parental consent, and technologies or methods that are under development that could be used in the future to obtain verifiable parental consent.⁵⁶

⁵¹ *Id.*

⁵² *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.8 (1999) (stating that a website operator's security measures must be "reasonable").

⁵³ *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 34595 (announcing public workshop).

⁵⁴ The transcript and all of the comments received in the course of the proceeding appear on the FTC's website at <www.ftc.gov>. References to the workshop transcript are cited as "Speaker/affiliation (Workshop Tr. at—)" followed by the appropriate page designation. Initial references to the comments are cited as "Name of Commentator (Comment or Workshop comment number) at (page number)."

⁵⁵ Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,888.

⁵⁶ *See id.* (stating that workshop comment period, which ended on July 30, 1999, yielded 14 comments).

A. Verifiable Parental Consent

Under the Rules, an operator must obtain verifiable parental consent⁵⁷ before any collection, use, and/or disclosure of personal information from children.⁵⁸ Furthermore, where an operator materially changes its information collection and use practices, it must obtain verifiable parental consent to the new practice(s) before using the previously collected personal information.⁵⁹ In addition, an operator must allow parents to consent to collect and use the child's information while agreeing not to disclose such information to third parties.⁶⁰ The Rules, however, specifically

⁵⁷ See 16 C.F.R. § 312.2 (defining "obtaining verifiable consent" as "making any reasonable effort (taking into account available technology) to ensure that before personal information is collected from a child, a parent of the child: (a) receives notice of the operator's personal information collection, use, and disclosure practices; and (b) authorizes any collection, use, and/or disclosure of the personal information").

⁵⁸ 16 C.F.R. § 312.2; *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,898 (reporting that because the Act requires parental consent *prior to any* collection, use, *and/or* disclosure, the parental consent requirement applies to subsequent use or disclosure of information in an operator's possession before the effective date of the Rule that is combined with the information gathered after the effective date of the Rule). The FTC has made clear that:

[N]otwithstanding any prior relationship that an operator has with the child, any collection of "personal information" by the operator after the effective date is covered by the Rule. Thus, for example, if an operator collected a child's name and e-mail address before the effective date, but sought information regarding the child's street address after the effective date, the later collection would trigger the Rule's requirements. Similarly, if after the effective date, an operator continued to offer activities involving the ongoing collection and disclosure of personal information from children (*e.g.*, a chatroom or message board), or began offering such activities for the first time, notice and consent would be required for all participating children regardless of whether they had previously registered or participated at the site.

Id.

⁵⁹ See 16 C.F.R. § 312.5(a)(1) (noting that consent must also be obtained for any material change in the collection, use, and/or disclosure practices to which the parent has previously consented); Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,899. Originally, many commentators objected that gaining new parental consent for any changes to the collection, use, and/or disclosure practices would be extremely burdensome, especially in light of constant changes taking place in the online world, and unnecessary to achieve the purposes of the COPPA. 64 Fed. Reg. at 59,899. The FTC responded to these complaints by requiring new parental consent only if there is a *material* change in the operator's collection, use, and/or disclosure practices. *Id.*

⁶⁰ See 16 C.F.R. § 312.5(a)(2) (mandating that "[a]n operator must give the parent the

exclude from these requirements any personally identifiable information collected by an operator prior to April 21, 2000.⁶¹

The Rules provide operators with some flexibility to comply with these requirements. Because the potential dangers to children's data privacy vary according to how the collected

option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties"). *But see* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,899 (noting that this provision interferes with an operator's right to terminate service to a child whose parent refuses to permit further use, maintenance, or collection of data). The FTC nevertheless made no changes to this provision. After considering many comments, the FTC concluded that:

[G]iving parents a choice about whether information can be disclosed to third parties implements the clear goals of the COPPA to give parents more control over their children's personal information, limit the unnecessary collection and dissemination of that information, and preserve children's access to the online medium. The Act requires consent for the collection, use, or disclosure of information, thus expressing the intent that parents be able to control all of these practices. Although the Act does not explicitly grant parents a separate right to control disclosures to third parties, the Commission believes that this is a reasonable and appropriate construction of the Act, particularly in light of the rulemaking record and other considerations.

Indeed, the record shows that disclosures to third parties are among the most sensitive and potentially risky uses of children's personal information. This is especially true in light of the fact that children lose even the protections of the Act once their information is disclosed to third parties. The Commission believes that these risks warrant providing parents with the ability to prevent disclosures to third parties without foreclosing their children from participating in online activities. In addition, the Act prohibits collecting more information than is reasonably necessary to participate in an activity, showing Congressional intent to limit information practices (such as disclosures to third parties) that do not facilitate a child's experience at the site. Finally, the Commission believes that allowing parents to limit disclosures to third parties will increase the likelihood that they will grant consent for other activities and therefore preserve children's access to the medium.

64 Fed. Reg. at 59,899 (citations omitted).

⁶¹ Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,898. Several commentators have argued that, by requiring parental consent for future use of information collected before the effective date of the Rule, the FTC attempted to apply the Act retroactively. *Id.* Furthermore, many noted that it would be extremely costly and burdensome to obtain consent for information collected years ago, especially in instances where the website operator was unaware of a child's past or current age or had no information on how to contact the parents. *Id.* The FTC, in response to these criticisms, eliminated the Act's requirement that website operators provide notice and consent for information collected prior to the Rule's effective date. *Id.*

information is used and/or disseminated, the FTC adopted a sliding scale approach for obtaining verifiable parental consent.⁶² Among other possibilities, an operator could (1) provide a consent form to be signed by the parent and returned to the operator by postal mail⁶³ or facsimile;⁶⁴ (2) require a parent to use a credit card in connection with a transaction;⁶⁵ (3) have a parent call a toll-free telephone number;⁶⁶ or (4) accept an e-mail accompanied by a valid digital signature.⁶⁷

In addition, the Rules provide several exceptions to the parental consent requirement.⁶⁸ The first, and most obvious, of these exceptions permits an operator to collect the name or online contact information of a child for the sole purpose of obtaining parental consent or to satisfy the notice provisions of the Act.⁶⁹ Similarly, an operator is also permitted to collect the information

⁶² See 16 C.F.R. § 312.5(b)(1) (stating that “[a]n operator must make reasonable efforts to obtain parental consent, taking into consideration available technology”). Further, any method contemplated by the website operator “to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.” *Id.*; see also Children’s Online Privacy Protection Rule, 64 Fed. Reg. at 59,901 (describing “sliding scale” standard in which consent mechanism required depends upon how operator intends to use information). The sliding scale approach permits website operators to obtain consent at a reasonable cost until secure electronic mechanisms become more widely available and affordable. 64 Fed. Reg. at 59,901. Under this scheme, e-mail—in conjunction with additional verifying procedures—suffices for purposes of consenting to an operator’s *internal* use of information, such as an operator’s marketing to a child based on the child’s preferences. *Id.* A more stringent method of consent, such as use of a credit card or print-and-send form, satisfies for purposes of consenting to activities that present greater risks to children, such as public postings (*e.g.*, in chat rooms and on bulletin boards), as well as disclosures of information to third parties. *Id.*; *How to Comply With The Children’s Online Privacy Protection Rule*, (last visited March 30, 2000) <<http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>>.

⁶³ 16 C.F.R. § 312.5(b)(2) (1999).

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ 16 C.F.R. § 312.5(c); Children’s Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,902 (1999) (explaining that exceptions were intended to “facilitate compliance with the Rule, allow for seamless interactivity in a wide variety of circumstances, and enable operators to respond to safety concerns”).

⁶⁹ 16 C.F.R. § 312.5(c)(1).

without prior parental consent to the extent necessary to protect the security or integrity of its website or online business, as well as other precautions aimed at avoiding liability.⁷⁰

Further, an operator may collect online contact information from a child without prior parental consent for the sole purpose of responding directly, on a one-time basis, to a specific request from the child, (e.g., to provide one-time homework help or to send a document).⁷¹ When an operator intends to use the information to respond directly to a specific request from a child more than once, and not to re-contact the child beyond the scope of that request, it must make reasonable efforts (taking into consideration available technology) to ensure that a parent receives notice and has the opportunity to request that the operator make no further use of the information.⁷² Last, the website operator is permitted to collect, without parental consent, the name and online contact information of the child to the extent reasonably necessary to protect the safety of a child participating on the website.⁷³

⁷⁰ 16 C.F.R. § 312.5 (c)(5); *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,903, n.225 (permitting website operators to collect limited information in order to protect security of website, for example, from hackers).

⁷¹ *See* C.F.R. § 312.5(c)(2) (explaining that this exception also requires that operator not use information to re-contact a child and that an operator delete information from its records); Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,902 n.221. If the website wishes to retain the child's e-mail address for future homework assistance, then it would fall into the scope of the exception in section 312.5(c)(3) and require parental notice and "opt-out". 64 Fed. Reg. at 59,902 n.221. Moreover, if the operator wishes to use the information, then he/she must follow the notice and consent requirements of the Rule. *Id.*

⁷² 16 C.F.R. § 312(c)(3); Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,902, n.222 (noting that sending electronic postcard where website retains online contact information until postcard is opened falls under this exception). However, where the operator's postcard system sends the requested postcard without maintaining the online contact information, this collection would fall under section 312.5(c)(2). 64 Fed. Reg. at 59,902, n.222.

⁷³ 16 C.F.R. § 312.5(c)(4); *see* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,902, n.224 (observing that operators may collect online contact information from children participating in their chat rooms in order to report to authorities the child's claim that he or she is being abused).

B. *Methods of Obtaining Parental Consent*

While most commentators generally support the concept of prior parental consent, they differ on what constitutes a satisfactory verification mechanism under this provision.⁷⁴ A significant number of commentators contend that e-mail alone is sufficient to satisfy the Act, noting that Congress intended e-mail to be used for consent purposes precisely because the Act permits online contact information to be collected in order to gain parental consent.⁷⁵ Indeed, many commentators have stated that, in their experience, parents prefer to use e-mail to grant consent.⁷⁶ Meanwhile, others suggest that “print-and-send” is the method least subject to falsification and the easiest to implement.⁷⁷ Still other commentators support the use of credit cards in obtaining parental consent on the grounds that few, if any, children under the age of thirteen have access to credit cards.⁷⁸

Many have suggested that, with proper training, employees can learn to differentiate between children and adult phone callers, and

⁷⁴ See Children’s Online Privacy Protection Rule, 64 Fed. Reg. at 59,899 (noting the debate over whether e-mail based mechanisms can provide adequate assurance that a person providing consent is the child’s parent). Because of concerns that a child using e-mail could pretend to be a parent and thereby bypass the consent process, some commentators favored methods that would provide additional confirmation of the parent’s identity. 64 Fed. Reg. at 59,900.

⁷⁵ See *id.* (noting that Cartoon Network, Disney, and Time Warner, among others, advocated this position).

⁷⁶ See *id.* (listing Bagwell/MTV Networks Online and a child advocacy group led by Parry Aftab as supporters of this position).

⁷⁷ See *id.* (naming Council of Better Business Bureaus, Inc. (“CBBB”), Children’s Advertising Review Unit of the Council of Better Business Bureaus (“CARU”), National Association of Elementary School Principals (“NAESP”), Douglas L. Brown, and Don and Annette Huston as supporters of print-and-send method to ensure that operators are obtaining parental permission in certain circumstances—for example, when obtaining consent to publish child’s art work or letter, or to send contest winner prize). Additionally, because it is used by schools, most parents are familiar with the print-and-send method. *Id.*

⁷⁸ See *id.* (referring to commentators such as America Online (“AOL”), iCanBuy.com, Mars, Inc., KidsOnLine.com, and Talk City, submitting that credit cards can be used to erect parental “master account” with e-mail address to be used exclusively by parent).

that parents prefer this method.⁷⁹ Yet other commentators support the use of digital signatures to obtain consent, pointing to their effectiveness, reliability, and veracity.⁸⁰ Finally, there are a number of other electronic products and services that are available, or under development, that could be used to confirm a parent's identity and obtain consent. These include services that would provide a parent with a digital signature, password, PIN number, or other unique identifier after determining that the person seeking the identifier is an adult.⁸¹

⁷⁹ See Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,900. (listing CARU, Center for Media Education, Consumer Federation of America, American Academy of Child and Adolescent Psychiatry, American Academy of Pediatrics, Junkbusters Corp., National Alliance for Non-Violent Programming, National Association of Elementary School Principals, National Consumers League, National Education Association, Privacy Times and Public Advocacy for Kids ("CME/CFA *et al.*"), and Aftab).

⁸⁰ See *id.* (mentioning commentators such as Brandt/VeriSign, Teicher/CyberSmart!, Lucas/PrivaSeek, Hill/ZeroKnowledge, and Johnson/Equifax Secure, Inc).

⁸¹ See *id.*, n.186 (describing newly developing service which employs schools to assist in issuing digital certificates to children after obtaining parental consents). Other developments include:

- an e-mail authentication system that verifies the age or profession of a person, and then assigns that person an e-mail address associated with his age or status, e.g., *John.doe@validadult.com*; *Mary.teacher@validteacher.com*. *Id.*;
- a permission-based info-mediary service that enables consumers to set their preferences as to how their information may be disclosed online. *Id.* Under this service, a parent is assigned a password or digital signature following initial verification. *Id.* The charge to participating websites is anticipated to be \$0.10-.20 per name. *Id.*;
- a system wherein digital credentials (a certificate, PIN, or password) are assigned to consumers after authenticating their identity. *Id.* The estimated cost for sites to use this service is \$3-4 per customer. *Id.*;
- a service that enables children to make purchases, with a parent's permission, at participating websites. *Id.* Parents use a credit or debit card to establish an account and then authorize the sites to be accessed and the amounts to be spent. *Id.*;
- a free verification service that uses both credit and bank cards in conjunction with algorithms to verify the validity of the card numbers. *Id.* The card number is checked at the consumer's browser and is not collected or transferred over the Internet, addressing some consumers' concerns about using credit cards online. *Id.* Parents without online access will be able to obtain verification by telephone. *Id.*;
- a system wherein parents and children are provided with digital pseudonyms that, following initial verification using a digital signature, can be used to verify

C. Criticisms of the Parental Consent Measures

Many commentators have criticized some of these methods for the costs and burdens they are likely to impose.⁸² For instance, some oppose the use of e-mail on the grounds that children can easily disguise their identities using this medium.⁸³ Accordingly, many of the commentators who support the use of e-mail acknowledge that additional steps would be necessary to increase the likelihood that the parent, and not the child, properly submitted the consent.⁸⁴

Other methods are equally challenging. The print-and-send method has been estimated to cost U.S. \$2.81 per child in order to process mailed or faxed parental consent forms, a cost that gains significance when one considers how many parental consents would be needed to conform with the Act.⁸⁵ Another commentator

identity. *Id.*

⁸² See Dorothy A. Hertzell, Note: *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, 441 (2000) (noting that obtaining verifiable parental consent can be costly); Matthew Rothenberg, *COPPA Kicks Up Controversy: TalkBack Readers Mull Whether A New Law Limiting Access To Information From Preteens Will Help Kids Or Harm The Web*, (last updated Apr. 24, 2000) <<http://news.excite.com/news/zd/000424/20/coppa-kicks-up>> (reporting that the Act creates unnecessary hurdles for commercial websites).

⁸³ Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,899; Rothenberg, *supra* note 82. One consumer explained that "[t]rying to stop pre-teens from using the Web is like trying to nail Jell-O to the wall . . . Each of them has a sister, a brother, a friend who has legit access . . . As is the case with all adult material, preteens can find it. Another piece of bureaucratic insanity. Enforcement should be fun on this one!" Rothenberg, *supra*.

⁸⁴ See Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,901 (listing steps such as use of PIN numbers or passwords, sending follow-up e-mails to a parent to increase the likelihood that the parent will receive a request for consent, or allowing e-mail consent only if the parent and child have different e-mail addresses). Children, however, can easily obtain multiple e-mail addresses from free e-mail services. *Id.* Still others recommend including questions in the e-mail to which the child would be unlikely to know the answer. *Id.* Yet, the FTC has noted with respect to this last suggestion that it could pose problems if it requires operators to verify the "answer" to the questions, or if the child is reasonably sophisticated. *Id.*

⁸⁵ See Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,900, n.187 (noting that the cost to open and sort written consent forms is about U.S. \$0.08-0.31 per child). The cost per consent by fax and mail, including overhead, has been estimated at U.S. \$0.94 and U.S. \$0.89, respectively. *Id.*

noted that online subscriptions to a magazine publication declined by eighty percent when the magazine switched from an online subscription model to a form that required downloading and mailing.⁸⁶ And, of course, there is no way to fully ensure the veracity of an electronically authenticated signature.⁸⁷

Concerning the use of credit cards, commentators have complained that operators will be charged a fee for each transaction,⁸⁸ and that many parents prefer not to use credit cards online out of fear for their own privacy.⁸⁹ Using telephone verification may be problematic because it requires operators to hire personnel just to answer phones, and would therefore be costly.⁹⁰ Finally, a number of commentators contend that while digital signatures and other electronic methods may be promising alternatives, they are not yet widely available, rendering them impracticable as current methods of compliance.⁹¹ Thus, websites

⁸⁶ See *id.* (stating that other offline methods might be too inconvenient or labor-intensive for parents).

⁸⁷ *Id.*

⁸⁸ See *id.*, n.190 (explaining that credit cards could cost up to \$3.00 per verification to process). One company that has attempted to verify its credit card purchases experienced costs ranging from \$2.00 – 3.00 per verification. *Id.*

⁸⁹ See Rothenberg, *supra* note 82 (noting consumer fears that the use of credit cards is just “another excuse for companies like Disney to compile a list of credit-card numbers”). One consumer commented that “credit cards were never meant to be used as identification and doing so increases the risk of credit card and identity theft.” *Id.*; Children’s Online Privacy Protection Rule, 64 Fed. Reg. at 59,900, n.191 (noting that consumers might be troubled by privacy implications of divulging personal information for the purpose of granting consent). Indeed, credit card companies oppose this method as well because it could foster unauthorized use and undermine systems used to detect fraud. 64 Fed. Reg. at 59,901. Besides, not every parent owns a credit card. *Id.* Despite the risks in using credit cards for this purpose, the FTC has noted that this method is already being used for similar purposes—for example, to verify that a person is over 18 in order to obtain access to adult materials online. *Id.*

⁹⁰ See *id.*, n.194 (revealing that the cost for telephone consents would be \$0.97 for an automated answering system, the tapes of which would then need to be manually swept to weed out children and enter data into a system). Some commentators have estimated the cost of a live operator at \$55 per hour plus training costs. *Id.*

⁹¹ *Id.*; see also Daniel B. Phythyon, *Consumer Privacy Issues to Dominate Wireless Internet Policy Agenda*, RADIO COMM. REPORT, Feb. 28, 2000, at 36 available in 2000 WL 9540239 (explaining that applicability of COPPA to Internet-capable wireless services are also unclear). Since COPPA was enacted before the wireless Internet emerged, it does not yet address concepts peculiar to that industry, such as location issues

seeking to continue collecting, using, and/or disclosing children's personal information will need to set up reliable systems for notifying parents and obtaining non-e-mail parental consent.⁹² Implementation of these systems, including legal and programming costs, will be expensive, providing a special problem for small or start-up sites⁹³ who will find their ability to compete severely restricted.⁹⁴

More significant was the reaction of the online industry as the April 21, 2000 deadline approached.⁹⁵ Rather than wade through the Act's proscriptions, some companies decided that the best, most cost-effective answer was simply to cancel all the accounts they had with children under the age of thirteen.⁹⁶ Other

inherent in targeted advertising. *Id.*

⁹² See Brian Ross, *Web Sites Must Heed Privacy for Children*, NAT'L L.J., Dec. 20, 1999, <http://test01.ljextra.com/na.archive.html/99/12/1999_1211_56.html> (last visited Apr. 15, 2000) (noting that preparatory steps to comply with COPPA will be expensive).

⁹³ *Id.*; see also Hertzler, *supra* note 82, at 441 (concluding that costs of implementing parental consent measures will effectively wipe out small to medium-size web providers).

⁹⁴ Ross, *supra* note 92.

⁹⁵ See Lynn Burke, *Time Running Out on Kid Email*, <<http://www.wired.com/news/print/0,1294,34453,00.html>> (last modified Feb. 29, 2000) (reporting that companies that provide free e-mail services are scrambling to determine how to bring those e-mail accounts held by children into compliance with COPPA).

⁹⁶ See *id.* (noting that compliance with the Act will cost anywhere from U.S. \$60,000-\$100,000). Snap.com and email.com, for instance, have destroyed the files and accounts of customers under 13 years old, rather than deal with the Act. *Id.*; see also Ross, *supra* note 92 (illustrating problems small businesses will encounter under the Act). Ross posited the following hypothetical:

[I]magine a small start-up Web site directed to children, called www.earthdayforkids.com (EDFK). EDFK offers ecology stories, chat rooms, bulletin boards, e-commerce links and a feature allowing kids to e-mail "Mother Nature" and receive a personalized response. EDFK wants to comply with the rule, but implementing a system of parental notice and consent would be far too costly. Therefore, under the rule, whenever a child e-mails "Mother Nature," the operator may only keep the child's name and e-mail address long enough to send one response, then the operator must delete the personal information. If EDFK wants to use "cookies," then the operator must keep children's identifying codes carefully segregated from any personal information. If the codes are commingled with that information, then the codes become "personal" information, too, and must be deleted.

To avoid future liability, EDFK would like to maintain a database of "Mother Nature" transactions, to prove that it has only responded once to any request from a child under 13 and that it has automatically deleted all personal

companies, willing to satisfy the Act, devised elaborate plans to ensure that they obtain verifiable parental consent.⁹⁷ Unfortunately, some found these compliance methods difficult to implement and in fact, in some cases, the solutions exacerbated the problem.⁹⁸

Furthermore, until parental-consent systems are in place, many online businesses may opt to be cautious and err on the side of overcompliance, which adversely impacts free speech, privacy, and

information afterward. Paradoxically, maintaining such a database to avoid liability would constitute the very same act that gives rise to the liability in the first place. These conundrums may confound online companies as they try to determine how best to comply with the rule and protect themselves from liability in the coming year.

.....
EDFK, under the hypothetical, faces additional compliance issues. If EDFK shares children's personal information with any third party, such as an order-fulfillment house, EDFK must ensure that the party agrees to take adequate steps to protect personal information. Further, EDFK will likely need to audit its own internal security measures and redraft its privacy policy to address the rule. EDFK will probably have to close its chat rooms and bulletin boards because it cannot afford the cost of hiring someone to monitor them.

Ross, *supra*.

⁹⁷ See Burke, *supra* note 95 (describing Hotmail's Kids Passport Online Parental Consent Service). This service will give parents options to permit varying degrees of access to their children. *Id.* Another e-mail service provider, Surfmonkey, permits children to sign up for their own e-mail accounts, but only after registering a request with his/her first name and an e-mail address for one of his/her parents. *Id.* If Surfmonkey is satisfied with the response, the parent is prompted to fill out and execute a registration form, and mail or fax it to the company. *Id.*

⁹⁸ See Lynn Burke, *Oops: A Barrel of Kids' Emails*, Mar. 2, 2000, (visited Mar. 15, 2000) <<http://www.wired.com/news/print/0,1294,34679.00.html>> (reporting that in Surfmonkey's attempt to obtain parental consent, it released complete lists of e-mail addresses for thousands of children registered with company). Surfmonkey's error illustrates the extreme difficulty websites face in bringing their services into compliance with COPPA. *Id.* Indeed, other industry experts, including David Steer, spokesperson for TRUSTe, have admitted that efforts to comply with COPPA will be "messy." *Id.* As Mr. Steer divulged, "I think we're seeing the tip of the iceberg." *Id.* Thus, despite a company's, such as Surfmonkey, best intentions, compliance can lead to greater problems. *Id.*; see also *Pre-Teen Publishers*, *supra* note 4 (concluding that "there seems to be substantial disconnect among formal government policy, generally positive parental attitudes toward youngsters going online, and acceptance of digital methods for letting kids e-shop").

commerce.⁹⁹ And, despite the acrobatics some online companies are performing to satisfy the Act, many in the business feel that the Act still does not afford adequate protection for children.¹⁰⁰

COPPA's parental consent measures, additionally, place undue burdens upon the constitutional right to commercial free speech. In *American Civil Liberties Union v. Reno* ("ACLU"),¹⁰¹ the U.S. District Court for the Eastern District of Pennsylvania ruled that the economic costs imposed on website operators, including out-of-pocket costs to implement mechanisms that satisfy the Child Online Protection Act ("COPA"), potential loss of revenue and closure of websites, and the ability of website operators to shoulder these economic burdens incrementally justified preliminarily enjoining COPA's enforcement.¹⁰² Similarly, COPPA's parental consent methods impose economic and technological burdens which may destroy small or developing commercial websites and which will surely impact the business practices of those who are more established. Indeed, in formulating its opinion, the *Reno* court noted the significant loss of both users and revenues incurred by verification schemes substantially similar to those imposed upon website operators under COPPA, such as credit card verification procedures and PIN numbers.¹⁰³ In both the COPA

⁹⁹ See Ross, *supra* note 92 (reporting that rather than paying someone to monitor chat rooms and message boards, sites may simply close them down, thus choking off forums for speech). Sites distributing online newsletters that are unsure whether they are child-directed or not might inform every parent that their child has signed up for a newsletter, infringing on older minors' access to information and privacy. *Id.*

¹⁰⁰ See Hertz, *supra* note 82, at 443 (explaining that "[d]espite the thoughtful drafting by the FTC, the COPPA is not a panacea to the problem of a child's privacy online"); see also Burke, *supra* note 95 (explaining that while e-mail options may be acceptable under COPPA, some fear it is too weak to protect children's privacy interests). Telephone and e-mail confirmations are inherently dangerous. Burke, *supra*. Clever children can sign up for an account using a different birth date. *Id.* As one commentator noted, "[u]nless a pair of human eyes monitors what goes in and out of [the] account, there's room for error." *Id.* Some fear that the opportunity for predation is still too high. *Id.*

¹⁰¹ 31 F. Supp. 2d 473 (E.D.P.A. 1999).

¹⁰² See *id.* at 499.

¹⁰³ See *id.* at 488-89, 491 (noting that credit card, PIN, and other verification schemes impose additional technological burdens and economic costs upon website operators and could deter thousands of users from using a website).

and COPPA examples, website operators will be under a severe financial disincentive to comply with the respective Acts.¹⁰⁴ As the *Reno* court noted, however, “[a] statute is presumptively inconsistent with the First Amendment if it imposes a financial burden on speakers because of the content of their speech.”¹⁰⁵ *Reno*’s reasoning might be no less true when applied to COPPA’s parental consent measures.

III. COPPA’S PARENTAL CONSENT MEASURES ARE IMPRACTICAL, INADEQUATE, AND CONSTITUTIONALLY SUSPECT

At best, COPPA establishes an ambiguous scheme for operators to follow,¹⁰⁶ at worst, it is unconstitutional¹⁰⁷ and provides little, if any, protection for children and parents. The parental consent measures contemplated by the Act do not sufficiently take into account the business realities of maintaining a commercial website.¹⁰⁸ Despite the useful input provided by many in the online industry,¹⁰⁹ the FTC has articulated rules that overreach in their effect. Besides being cumbersome, the measures are simply not cost effective. Last, and perhaps most important, even if a website utilizes the methods suggested in the Act, it still will not adequately protect the child’s personal information.

¹⁰⁴ *See id.* at 493 (explaining that financial disincentives can serve as deterrents to free speech); Burke, *supra* note 95 (reporting that many websites are excising whole portions of their businesses rather than come under the Act).

¹⁰⁵ *See id.* (citing *Simon & Schuster, Inc., v. Members of the New York State Crime Victims Bd.*, 502 U.S. 105 (1991)).

¹⁰⁶ *See* Ross, *supra* note 92 (noting that various provisions of Rule seem frustratingly vague, offering little guidance as to when and how website operators’ obligations are triggered).

¹⁰⁷ *See id.* (reporting that COPPA is certain to face constitutional challenges because of its enormous impact); *see also* *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D.P.A. 1999) (holding that as content-based regulation of non-obscene sexual expression, COPPA is presumptively invalid and is subject to strict scrutiny).

¹⁰⁸ *See supra* footnote 98 and accompanying text (explaining that COPPA does not resonate with business realities and parental expectations).

¹⁰⁹ *See supra* footnotes 57-61 and accompanying text (describing comment period initiated by FTC and resultant response by industry, privacy advocates, government, and consumer groups).

A. COPPA's Parental Consent Measures Are Impractical

COPPA's parental consent measures are difficult to implement and costly to realize.¹¹⁰ Print-and-send methods are antithetical to the speed and efficiency of e-commerce.¹¹¹ Postal, fax, and credit card fees, when aggregated, can be substantial.¹¹² Although some companies are developing new technologies to comply with the Act, the end-product usually makes browsing a painfully slow and laborious process.¹¹³ Indeed, companies will need to hire and compensate personnel to oversee and implement these new policies.¹¹⁴ As a result, the offline labor associated with these methods is prohibitive, for both parents and operators.¹¹⁵

B. COPPA's Parental Consent Measures Are Inadequate

Even if companies satisfy the Act's parental consent requirements, children's personal information may not be secure.¹¹⁶ Since most adults are still wary about providing their credit card information over the Internet, telephone and e-mail confirmations will most likely be the methods employed. These methods, however, are inherently unreliable; children can easily manipulate these media. Considering that many children are probably more adept than their parents at utilizing the Internet, it is likely that some sort of subterfuge will occur. Consequently, the benefits proponents of the Act had hoped for will not truly be realized.

C. COPPA's Parental Consent Measures are Constitutionally

¹¹⁰ See *supra* footnotes 81-94, 96, 98 and accompanying text (describing cost per child to obtain verifiable parental consent).

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ See *supra* footnotes 92-105 and accompanying text (describing attempts to comply with the Act).

¹¹⁴ See *supra* footnote 90 and accompanying text (explaining costs of providing personnel to implement telephone mechanisms to satisfy the Act).

¹¹⁵ See *supra* footnote 86 and accompanying text (noting high labor costs associated with switching to an offline subscription regime).

¹¹⁶ See *supra* footnote 95 and accompanying text (noting weaknesses of the Act's proscriptions).

Suspect

Finally, COPPA might be held to be unconstitutional because its suggested parental consent methods impose economic and technological burdens that will ultimately decrease the numbers of website users and which will compel website operators to engage in undue self-censorship.¹¹⁷ The Act will serve as a financial disincentive for website operators to conduct their businesses.¹¹⁸ Any statute that imposes a financial burden on speakers because of the content of their speech, however, presumptively violates the First Amendment.¹¹⁹ Website operators' fears of prosecution under COPPA has already resulted in the self-censorship of their online activities in an effort to avoid prosecution. This chilling effect is tantamount to censorship of constitutionally protected speech, and will cause irreparable harm to these website operators.¹²⁰

CONCLUSION

Matters of online privacy are at the forefront of both public and private debate. The Act and the Rules are among the first of many possible regulatory steps regarding the electronic collection, use, and disclosure of personal information. While the Act's mandates only apply to personal information collected from children on or after April 21, 2000, the scope of public and private concern regarding the use of the Internet by children of all ages is rapidly expanding. As Congress and consumers begin to focus more

¹¹⁷ See *supra* footnotes 102-04 and accompanying text (recounting plaintiff's argument that the Child Online Protection Act ("COPA") violates the First Amendment for the same reasons). Indeed, as mentioned earlier, many websites are choosing to delete all files suspected to contain information from children rather than exercise their constitutional right to engage in commercial practices under the Act. *Id.*

¹¹⁸ See *ACLU v. Reno*, 31 F. Supp. 2d 473, 493 (E.D.P.A. 1999) (explaining that "[a] statute which has the effect of deterring speech, even if not totally suppressing speech, is a restraint on free expression") (internal citation omitted).

¹¹⁹ See *Simon & Schuster, Inc., v. Members of the New York State Crime Victims Board*, 502 U.S. 105, 115 (1991).

¹²⁰ See *Reno*, 31 F. Supp. 2d at 497 (noting that "the loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury") (internal citation omitted).

attention on matters of online privacy, online companies would be wise to draft and post comprehensive privacy policies on their websites.

COPPA, however, may not be the right answer to the specific issues raised by children's online privacy interests. Offline schemes, such as "snail" mail, seem to be an expensive step backwards in dealing with forward-looking technologies, such as the Internet. Conversely, online parental consent regimes are subject to manipulation by both children and third parties, or are tedious and difficult to navigate. COPPA should work in cooperation with web business to be an effective federal regulation—not destroy substantial portions of the online industry. Although well-meaning, COPPA raises too many problems to be a truly effective mechanism to protect children's online privacy interests.