

## The Children's Online Privacy Protection Act and Rule: An Overview

Elizabeth Delaney

Follow this and additional works at: <https://scholarship.law.stjohns.edu/jcred>

---

This Symposium is brought to you for free and open access by the Journals at St. John's Law Scholarship Repository. It has been accepted for inclusion in Journal of Civil Rights and Economic Development by an authorized editor of St. John's Law Scholarship Repository. For more information, please contact [selbyc@stjohns.edu](mailto:selbyc@stjohns.edu).

# THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT AND RULE: AN OVERVIEW

ELIZABETH DELANEY\*

## BACKGROUND

In the early days of the Internet, relatively few consumers, and even fewer children, were online. As the Web developed into a mass phenomenon among adults in the 1990s, an increasing number of children also began to go online.<sup>1</sup> Together with the many benefits of Internet access for children came some novel problems. First, parents and privacy advocates observed that websites were collecting a variety of personal information from children for marketing purposes.<sup>2</sup> Second, children now had the ability to provide their personal contact information (such as telephone number or email address) and to contact and be contacted online, thereby raising the risk of predation.<sup>3</sup> At the

\* Elizabeth Delaney is an attorney in the Division of Advertising Practices of the Federal Trade Commission's Bureau of Consumer Protection and is one of the primary attorneys responsible for implementing the Children's Online Privacy Protection Rule.

<sup>1</sup> Almost 10 million children under age 18 were online, about 14% of American children. See Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), at 4 and n.16; Recent data confirm that the number of children online continues to grow. Jupiter Mediametrix data indicates that approximately 14 million children between ages two and twelve were online in 2000. *Digital Divide More Economic than Ethnic* at <http://www.jup.com/company/pressrelease.jsp?doc=pr000615>, last visited June 15, 2000; see also Pew Internet and American Life Project, "More Online, Doing More," February 2001 (finding 29% of children under 12 have been online) <http://www.pewinternet.org/releases/release.asp?id=15>.

<sup>2</sup> For example, one site collected not only the child's name, address, gender, and age, but also personal finance information such as whether the child had received gifts in stock, cash, bonds, or mutual funds, and whether the child's parents owned mutual funds. *Privacy Online: A Report to Congress*, at 39.

<sup>3</sup> See e.g., *Privacy Online: A Report to Congress*, at 5 and nn.21-22. More recent data confirms the potential safety threats posed by the Internet. A June 2001 survey prepared by the Crimes Against Children Research Center, "Online Victimization: A Report on the Nation's Youth," reports that, of children 10 to 17 years old who are regular Internet users, 19% received an unwanted sexual solicitation or approach over the Internet in the year preceding the survey. See [http://www.ncmec.org/html/onlinevictim\\_report.html](http://www.ncmec.org/html/onlinevictim_report.html). About three percent said that they had been the target of aggressive sexual solicitation

same time, the nature of the Internet made it more difficult for parents to exercise their traditional gate-keeping role, monitoring and mediating their children's relationships with both inquiring strangers and companies.

A survey of children's websites, conducted by the Federal Trade Commission in March 1998, revealed the scope of information collection by these websites and the apparent lack of parental notice or supervision. For example, although the vast majority of the sites surveyed collected personal information—including information that would allow the child to be identified or located such as name, email, and physical address or telephone number—only a quarter of these sites had a privacy policy.<sup>4</sup> At the same time, only a small fraction of these websites contemplated any role for parents in the information exchange.<sup>5</sup>

This survey data and growing public concern about children's privacy and safety led the FTC to call for legislation to give parents greater control over their children's personal information, to provide parents with notice of collection and use, and to require website operators to obtain consent before collecting personal information from children. Congress responded quickly, enacting the Children's Online Privacy Protection Act (the Act or COPPA), in October 1998.<sup>6</sup> This Act directed the Commission to set forth limited rules governing the online collection of personal information from children age twelve and under.<sup>7</sup> The Commission accordingly promulgated the Children's Online Privacy Protection Rule (the "Rule"), which went into effect April 21, 2000.<sup>8</sup>

involving attempted contact with the child: someone asked them to meet, called them, or sent them mail, money, or gifts. Most of the children who were the target of these types of solicitation—77%—were older children, age 14 or above; however, the younger children reacted more strongly to the incidents, finding them more disturbing.

<sup>4</sup> See *Privacy Online: A Report to Congress*, at 31, 35 (noting 89% collected personal information, while only 24% of these sites had a privacy policy).

<sup>5</sup> *Id.* at 37 (commenting that 1% of the sites required parental consent prior to the collection and use of information, 23% merely told children to ask for parental permission before submitting information, and less than 8% notified parents of their information practices).

<sup>6</sup> See Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2001).

<sup>7</sup> The FTC's rulemaking process included publishing a Notice of Proposed Rulemaking and Request for Public Comment (NPR), as well as holding a public workshop on parental consent mechanisms. In response to the NPR, over 145 comments were submitted to the FTC from a broad range of interested consumers, consumer and child advocacy groups, website operators, and other businesses.

<sup>8</sup> See 16 C.F.R. § 312 (2001).

## OVERVIEW OF THE ACT AND THE RULE

The primary goal of COPPA is to put parents in control over the types of personal information collected from their children and how that personal information is then used. COPPA applies to operators of commercial websites directed to children age twelve and under that collect or maintain personal information from children, as well as other websites that have actual knowledge that they are collecting or maintaining personal information from children age twelve and under.<sup>9</sup> In determining whether a website is "directed to children," the FTC will consider a number of factors including: the website's subject matter; visual or audio content, age of models, language or other characteristics of the website; as well as whether advertising promoting or appearing on the website is directed to children.<sup>10</sup> In addition, the FTC may also consider empirical evidence regarding the age of the website's visitors.

Principally, COPPA requires website operators to:

1. **POST A PRIVACY POLICY.** Websites that are subject to the Rule must post a notice of their information collection practices, or a privacy policy. In the privacy policy, the website must inform the visitor about the types of personal information they collect from children; how the site will use the information; and whether such personal information is shared with advertisers or other third parties. A link to the privacy policy must be located on the home page of the website and at each area where personal information is collected.

2. **PROVIDE NOTICE DIRECTLY TO PARENTS.** In certain circumstances, websites must send direct notice to a parent of the site's information practices and give parents the opportunity to opt-out on behalf of their child. In other instances, websites must directly notify parents of their information collection practices when requesting parental consent for information collection.

3. **GET PARENTAL CONSENT.** As a general matter, a website

<sup>9</sup> For purposes of the Rule, personal information includes any personally identifiable information about an individual collected online (*e.g.*, name, address, email address, social security number), as well as any other information collected online which is tied to that personally identifying information, such as a persistent identifier (*e.g.*, a cookie) or non-identifying information (*e.g.*, demographic information). 16 C.F.R. § 312.2 (2001).

<sup>10</sup> 16 C.F.R. § 312.2 (2001).

must obtain verifiable parental consent before collecting, using or disclosing personal information about a child.<sup>11</sup> Sites must also get verifiable parental consent before allowing children to open an email account or post messages in a chat room or on a bulletin board.

The Rule has adopted a “sliding scale” approach that allows website operators to vary consent methods based upon the intended uses of a child’s information.<sup>12</sup> For those activities that pose the greatest risks to a child’s safety and privacy—that is, disclosing personal information to third parties or permitting children to disclose their personal information publicly through email, chat rooms, bulletin boards, or other activities—a website operator must use the “more reliable” methods of consent. These methods include using a print-and-send form via postal mail or facsimile, providing a toll-free telephone number, using a credit card in combination with a transaction, using a digital signature, or employing email accompanied by a PIN or password obtained by the previously mentioned methods.<sup>13</sup>

For internal uses of information, such as a website’s own marketing back to a child or customization of a web page, under the sliding scale, websites are permitted to obtain a parent’s consent through the use of an email from the parent, so long as the website takes additional steps to assure that the person providing consent through the email is the parent. Such steps could include sending a confirmatory email to the parent following receipt of the emailed consent or obtaining a postal address or telephone number from the parent in the initial emailed consent from the parent and then confirming the parent’s consent by letter or telephone call.

Websites need to notify parents and get consent again if they materially change the kinds of information they collect or how they use the information. In addition, websites must give parents the option of consenting to the website’s internal use of

<sup>11</sup> 16 C.F.R. § 312.5(b) (2001). The exceptions to this requirement are discussed in the Email Exceptions section of this article.

<sup>12</sup> The sliding scale for obtaining parental consent was set to expire on April 21, 2002. In October 2001, the FTC published a Federal Register notice proposing to amend the Rule and extend the sliding. 66 Fed. Reg. 54,963 (Oct. 31, 2001). The comment period for this rulemaking ended on November 30, 2001. 67 Fed. Reg. 18,818 (Apr. 17, 2002) (extending the time period until Apr. 21, 2005). The Commission reviewed the comments and found widespread support for a 3-year extension of the sliding scale mechanism.

<sup>13</sup> 16 C.F.R. § 312.5(b) (2001).

the child's personal information, without having to consent to the website's disclosure of that personal information to third parties.

4. ALLOW PARENTS TO REVIEW PERSONAL INFORMATION COLLECTED FROM THEIR CHILDREN. Before doing this, website operators must verify the identity of the requesting parent. The means of reviewing the information collected from the child must not be unduly burdensome to the parent.

5. ALLOW PARENTS TO REVOKE THEIR CONSENT, AND DELETE INFORMATION COLLECTED FROM THEIR CHILDREN AT THE PARENTS' REQUEST. Parents can revoke their consent and ask that information about their children be deleted from the site's database. When a parent revokes consent, the website must stop collecting, using or disclosing information from that child. The site may end a child's participation in an activity on the website if the information it collected was necessary for participation in that activity.

6. NOT CONDITION A CHILD'S PARTICIPATION IN CERTAIN ACTIVITIES ON COLLECTION OF MORE PERSONAL INFORMATION THAN IS REASONABLY NECESSARY.

7. ESTABLISH AND MAINTAIN REASONABLE PROCEDURES TO PROTECT THE CONFIDENTIALITY, SECURITY, AND INTEGRITY OF CHILDREN'S PERSONAL INFORMATION. For example, companies must ensure that personal information is stored in such a way that it is reasonably protected from theft.

#### EMAIL EXCEPTIONS TO OBTAINING PRIOR PARENTAL CONSENT

Websites may be able to utilize an "email exception" to the requirement of obtaining prior parental consent, in cases where only an email address is collected from the child and is used for certain, limited purposes. The Rule sets forth five exceptions to the requirement of obtaining prior parental consent.<sup>14</sup> The first exception allows a website to collect the name and online contact information of a parent or a child for the sole purpose of obtaining parental consent or providing notice to the parent.<sup>15</sup> The site must delete this information if it has not obtained parental consent within a reasonable amount of time.

The second and third exceptions allow the website to offer

<sup>14</sup> 16 C.F.R. § 312.5(c) (2001).

<sup>15</sup> *Id.* at § 312.5(c)(1) (2001).

some interactive content for children without first having to obtain parental consent. For example, under the “one-time” use exception, a website is allowed to collect a child’s email address for the sole purpose of responding directly on a one-time basis to a specific request of the child.<sup>16</sup> One-time uses include responding to a child asking for “Homework Help” or responding to an interactive activity on the site such as “Ask the Veterinarian.” The website could also provide the child with other information requested from the site, such as a one-time newsletter. In addition, the site may also use this exception for the purposes of running a contest. In that case, the site would collect an email address from the child for entry into the contest and then would use the email address only once, to notify the child that they had won the contest.<sup>17</sup> In any of these examples, the email address can be used only once, for the limited purpose stated, and the website must delete the child’s email address following the contact.

The third exception allows a site to collect a child’s email address to respond “more than once” to a child’s request. Under this scenario, if the website wishes to use the email address to contact the child on a regular basis, a notice must be sent to the parent, letting the parent know about the regular contact and giving the parent a chance to say no to the arrangement.<sup>18</sup> This so-called multiple use e-mail exception permits a site to send a weekly newsletter to a child or to enter a child into a contest and then send the child confirmation of her entry and notification of whether or not she has won the contest. In addition to notifying the parent, the website cannot use the child’s email address for any other purpose, must delete the email address within a reasonable time period after the limited use ends, and must keep the email address secure during its use.

The fourth exception to the prior parental consent requirement allows the website to collect the child’s name and online contact information to the extent necessary to protect the safety of the child on the site.<sup>19</sup> In this instance, the information can only be

<sup>16</sup> 16 C.F.R. § 312.5(c)(2) (2001).

<sup>17</sup> Any further information collection, for the purposes of prize fulfillment, would have to be either offline or with the parent’s prior verifiable consent.

<sup>18</sup> 16 C.F.R. § 312.5(c)(3) (2001).

<sup>19</sup> 16 C.F.R. § 312.5(c)(4) (2001).

used to protect the child's safety. The site cannot use the information to recontact the child and the information cannot be disclosed on the website. The fifth exception allows the same collection of information, but for slightly different purposes: the site can collect the information to protect the security or integrity of the site, to take precautions against liability or to respond to judicial process.<sup>20</sup>

Collection of any personal information besides the parent's or child's email address (and sometimes name) requires prior parental notice and verifiable parental consent.

### SAFE HARBOR PROGRAMS

COPPA also provides the opportunity for industry groups to get involved in self-regulation through the Rule's "safe harbor" provision. The safe harbor provision enables industry groups or others to apply for FTC approval of their self-regulatory programs to govern participants' compliance.<sup>21</sup> FTC-approved safe harbors will provide website operators with the opportunity to tailor compliance obligations to their business models with the assurance that if they follow the safe harbor guidelines, they will be in compliance with the Rule. Websites participating in FTC-approved safe harbor programs will be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal FTC action.

### FTC ENFORCEMENT OF THE RULE

COPPA authorizes the FTC to bring enforcement actions and impose civil penalties in the same manner as for other rules promulgated under the Federal Trade Commission Act. Website operators who violate the Rule may be liable for civil penalties of up to \$11,000 per Rule violation. The amount of penalties assessed may turn on a number of factors, including the egregiousness of the violation, the number of children involved, the amount and type of personal information collected, how the information was used, and whether the information was disclosed to third parties. COPPA also authorizes States and

<sup>20</sup> 16 C.F.R. § 312.5(c)(5) (2001).

<sup>21</sup> 16 C.F.R. § 312.10 (2001).



certain other federal agencies to bring their own enforcement actions with respect to entities within their jurisdiction.

The FTC has a comprehensive website located at <http://www.ftc.gov> with information concerning all of the FTC's activities. On the home page are two hyperlinks entitled "Privacy Initiatives" and "Kidzprivacy." The "Privacy Initiatives" hyperlink connects to copies of COPPA, the proposed Rule and public comments, the final Rule, applications for approval of safe harbor guidelines and public comments, a list of "Frequently Asked Questions," and other privacy materials. The "Kidzprivacy" hyperlink connects to compliance materials for businesses, information for parents, online safety tips for children and other useful educational resources about the Rule and online privacy in general. Copies of many documents are also available from the FTC Consumer Response Center, Room 130, 600 Pennsylvania Avenue NW, Washington, DC 20580; toll-free at 877-FTC-HELP (877-382-4357); TDD for the hearing impaired at 202-326-2502. The FTC also has an online form to request information at the FTC website.