Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 16 | Issue 2 Article 9

January 2000

Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act

Laurel Jamtgaard

BIG BIRD MEETS BIG BROTHER: A LOOK AT THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Laurel Jamtgaard[†]

TABLE OF CONTENTS

On April 21, 2000 the Children's Online Privacy Protection Act[1] ("COPPA") will go into effect and companies operating on the Internet will no longer be able to ignore the growing number of children flocking to hang out on-line. Although the intent of COPPA is to curb the activities of those who take advantage of children on-line, it will require a broad range of on-line companies to alter their web sites and information practices. Fortunately for such companies, the attention that they pay to complying with COPPA may help them comply with other privacy related regulations that are on the way.

Some view COPPA as a continuation of the U.S. "piece meal" approach to privacy regulation but others see it as evidence of a new tide of general privacy regulation in the United States. Until now, the U.S. approach to privacy has combined (a) a set of narrowly defined

[†] Associate at Fenwick & West LLP, Palo Alto, CA; A.B. Stanford; J.D. UC Berkeley, Boalt Hall. I thank the student organizers of the Santa Clara Privacy Symposium for giving me the opportunity to participate in the symposium and the incentive to write this piece. The opinions expressed herein are my own and are not necessarily the opinion of Fenwick & West LLP or any of the clients that I may advise.

1. 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).

laws focused upon specific types of bad acts,[2] with (b) a reliance upon industry "self-regulation" to develop general standards and build a consensus for privacy in the on-line world.[3] But, as consumers take to the Internet with enthusiasm and learn that everything they buy, view, or "click on" is recorded in a database and can be indexed and queried in innumerable ways, the willingness to rely on self-regulation is waning. Increasingly, federal and state regulators are stepping into the privacy arena with calls for legislation to increase consumers' control of their information.

This is indeed a busy time for privacy regulation in the United States. In addition to COPPA, we are seeing increased monitoring of privacy concerns by the Federal Trade Commission ("FTC").[4] The privacy protection provisions of the Financial Services Act of 1999 are not yet in effect but will entwine many on-line companies in the Act's regulation of data sharing among "financial institutions."[5] The Supreme Court recently affirmed the Driver's Privacy Protection Act[6] and in it the principle that Congress may regulate personal information held by state agencies. The White House and Congress

---

2. *See, e.g.*, the Video Privacy Protection Act, 18 U.S.C.A. § 2710 (West Supp. 1999) (adopted in reaction to the public disclosure of video tape rental records of Robert Bork when he was a nominee to the U.S. Supreme Court); the Cable Communications Policy Act, 47 U.S.C.A. § 551 (West 1991 & Supp. 1999); the Electronic Communications Privacy Act of 1986, 18 U.S.C.A. § 2701-2711(West Supp. 1999); and the Drivers Privacy Protection Act of 1994, 18 U.S.C. § 2721 (West Supp. 1999).

3. *See, e.g.*, Self Regulation and Privacy Online: A Report to Congress, Federal Trade Commission, July 1999. The Report can be found at <http://www.ftc.gov/os/1999/9907/privacy99.pdf>.

4. The FTC is not only leading the implementation of COPPA and the Financial Services Act privacy regulations, it has also launched investigations against individual companies based upon privacy concerns and, recently, has announced an investigation into the privacy practices of the on-line health care industry. *See* Keith Perine, *FTC Probes Health Site Privacy*, The Standard (Feb. 18, 2000) <http://www.thestandard.com/article/display/0,1151,11120,00.html?nl=dnt>.

5. *See* 12 C.F.R. § 225.28(b)(9)-(14) (1999) (explaining that among other things "financial institution" shall include companies providing certain types of management consulting services; companies issuing consumer-type payment instruments; and companies offering data processing services related to financial data); *see also* Bank Holding Company Act of 1956, 12 U.S.C. § 1841 (1994). The FTC has published proposed rules and the comment period to respond will close March 31, 2000 (Mar. 1, 2000) <http://www.ftc.gov/os/2000/02/65FR11173.pdf> (to be codified at 16 C.F.R § 313 "Privacy of Consumer Financial Information, Proposed Rule").

6. *See* Condon v. Reno, No. 98-1464, 1999 S. Ct. Cornell (Jan. 12, 2000), *rev'g* 155 F.3d 453 (holding that the Driver's Privacy Protection Act of 1994 (DPPA or "Act"), 18 U.S.C.A. §§ 2721-2725 (West Supp. 1999), did not violate the Constitutionally protected principle of federalism). The decision can be found at <http://supct.law.cornell.edu/supct/html/98-1464.ZO.html>.

are pushing toward medical privacy protection regulations.[7] And the Commerce Department, after lengthy negotiations, has reached a tentative agreement with the Europeans for "safe harbors" to enable multi-national companies to comply with the broad European consumer privacy regulations.[8] All this, combined with the flurry of class action suits against various software and on-line advertising companies, means that the risks to a U.S. company operating on the Internet of not defining, disclosing, and internalizing a reasonable privacy protection policy are very real and are growing each day.

Although this article will focus on COPPA and the issues that it raises for companies dealing with consumers on-line, it will hopefully serve a broader purpose because companies that proactively work to comply with COPPA will find that they are a step ahead as other privacy regulations arrive. In Part I, I provide a basic overview of the Children's Online Privacy Protection Act. In Part II, I discuss several issues that companies will face with regard to COPPA including (a) who in the company should be involved with decision-making about privacy, (b) whether the scope of COPPA reaches a company's on-line practices, and, (c) assuming that the company will be affected by COPPA, some options for complying with the new rule.

I. ABOUT COPPA–BACKGROUND, STATUS AND BASIC PROVISIONS

Congress passed the Children's Online Privacy Protection Act in October 1998 at the end of a session in an omnibus bill and without much fanfare or public controversy. The bill addressed the emotionally charged concern that commercial web site operators were targeting children (those under 13) and collecting personal information from them without notice to their parents. In November 1999, the FTC issued the rule to implement COPPA, known as the Children's Online Privacy Protection Rule (the "Rule").[9] The Rule goes into effect April 21, 2000.

---

7. See the recently proposed rules announced October 9, 1999, by the Department of Health and Human Services. Electronic Privacy Information Center, Wash. D.C., *HHS Medical Privacy Regulations* (last modified Oct. 29, 1999) <http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html>.

8. *See* DRAFT INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE, (Mar. 14, 2000) <http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm> and the Press Release accompanying the Draft (Mar. 14, 2000) <http://204.193.246.62/public.nsf/docs/8B7937D138B4F735852568A30053A385>.

9. 16 C.F.R. § 312 (1999). The FTC provided detailed analysis in connection with the Rule.

A central provision of COPPA provides:

> It shall be unlawful for any operator of a website or online service directed to children [age 12 or younger], or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part.[10]

An "operator" is a person or company that operates a web site or on-line service for commercial purposes and that collects personal information about users.[11] This includes e-commerce sites offering products or services for sale from the web. One important exception to note for many organizations that interact with children is that this definition of operator excludes non-profit web sites and personal home pages with "guest books."[12]

"Personal Information" is information that could enable someone to be contacted on-line or in the real world. It includes first and last name, physical address, e-mail address, instant message identifier, phone number or photographs.[13] Anonymous data such as traffic data collected using cookies will be considered "personal information" if it is tied to personally identifiable data.[14] For example, if a web site operator associates data about what pages a visitor has viewed with a unique identifier that can be used to contact the person through e-mail, a physical address or even an on-line message name, the page view data will be considered "personal information."

There are five key requirements of COPPA: (1) Notice; (2) Parental Consent; (3) Parental Review; (4) Limits on the Use of Games and Prizes; and (5) Security.

With the notice requirement, an operator of an on-line service directed to children must provide notice about what information it collects from the children that use its service, how it uses the information it collects and to whom, if anyone, it discloses that information.[15] The notice must be placed in a "clear and prominent" manner on the home page of the site, or area directed to children, and on any page where personal information is collected.[16]

---

10. *Id.* § 312.3.
11. *See id.* § 312.2.
12. *See id.*
13. *See id.*
14. *See id.*
15. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(b) (1999).
16. *Id.*

The parental consent requirement is perhaps the most onerous. It states: "Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent."[17] Web sites seeking consent must employ reasonable efforts to ensure that the consent is genuine taking into account available technology. I discuss this consent requirement further in Part II.

An operator must provide a means for a parent to review information that has been collected and a means for the parent to contact the operator to prohibit further use or maintenance of the child's personal information.[18] The FTC does not go so far as to require that an operator enable a parent to *alter* the data provided by the child, but encourages companies to enable that option.[19] Except as limited by section 312.7 of the Rule discussed below, an operator may refuse to continue to provide its service to a child if the parent has prohibited further use of the personal information.[20]

In order to avoid enabling improper access to a child's personal information, the process for enabling a parent to review a child's information must itself involve some reasonable procedure of verification of the parent without unduly burdening the parent.[21] This identification process is not required for an operator who provides the requesting adult only with the *types* of information collected about a child. But the identification process is required before revealing the child's personal information to the requesting adult.

Web sites that direct games and prizes to children in an effort to get targeting information about them should take careful note of section 312.7. It states that "[a]n operator is prohibited from conditioning a child's participation in a game, the offering of a prize of another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[22] The FTC provided very few comments about this section, thus web sites are likely to have questions about what information would be considered "reasonably necessary."

Under section 312.8, operators must protect the confidentiality,

17. *Id.* § 312.5.

18. *See id.* § 312.6.

19. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59904 (1999) (to be codified at 16 C.F.R. pt. 312).

20. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.6(c) (1999).

21. *See id.* § 312.6(a); *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59903.

22. 16 C.F.R. § 312.7 (1999).

security, and integrity of personal information collected from children. Most web sites are increasing security procedures at a rapid pace to keep up with the danger of hackers and system outages. Section 312.8 reiterates the importance of establishing and maintaining internal and external security measures including firewalls, information deletion, limits on employee access to data, and careful screening of third parties to whom such information is disclosed.[23]

II. INTERNALIZING COPPA–QUESTIONS AND ISSUES

A. Who in the Company Should be Involved?

Before discussing the legal issues surrounding COPPA, it is important to highlight corporate awareness as the most important goal for a company subject to COPPA. The first thing a company should do is decide which internal employees and outside advisors should be involved in evaluating the company's approach to user privacy. For many small start-up web companies, this is fairly straight-forward. Usually, whoever is in control of the web site's content (often a marketing manager) will contact the company's outside counsel to discuss the company's compliance with COPPA. As questions arise, the company's information technology or computer services director may get involved to advise on how the solution may be implemented using the company's existing database applications and user registration processes.

For a large company, determining who should be involved can be daunting. There may be hundreds of people within the corporation who have direct design responsibilities for some portion of the web site or network of related web sites and who may have access to the information collected from the web site or from customers via e-mail. Large portals or media sites will have a tough job getting a privacy message out to all the employees who have a need to know. To address this problem, many companies have created whole departments focused on setting and implementing privacy, data management, and data integrity policies. And, job postings for "Chief Privacy Officer" are on the rise.

A review of a company's privacy policy and its exposure under COPPA will involve marketing, business development, legal, and

23. *See id.* § 312.8; *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59906.

information technology issues. Companies that want to get ahead of the privacy wave should plan to involve voices from each of these areas in planning their approach to user privacy. Companies with international operations will have already begun this privacy review as a result of privacy regulation in other parts of the world. With COPPA in place, many more U.S. companies now have a clear incentive to do so.

B. Scope of the Rule

For companies evaluating COPPA's impact on their business, the threshold question is whether the company's activities even come within the scope of the regulation. With COPPA, this can be a difficult determination to make. COPPA only applies to: (1) web sites directed/targeted to children under 13 years of age; (2) "general audience" web sites that have a portion of the site targeted to children; and (3) general audience web sites that have "actual knowledge" that they are dealing with a child or that a child is disclosing personal information through the web site.[24]

1. Sites Targeted to Children

If a web site is "targeted to children," the rules of COPPA apply across the board to the site's information collection practices. Thus, in order for the site to collect any personal information from any visitors, even adults, the site must comply with the provisions of COPPA and seek some sort of adult verification.

A likely result of COPPA will be that sites clearly targeted to young children under 13 will not collect any information that would require obtaining parental consent. Sites targeted to teenagers, or that have content that is attractive to kids of all ages, will be in an uncertain position because they may be unsure whether the FTC or a court will consider them to be "targeted to children."

Under COPPA, determining whether a site is "targeted to children" will involve consideration of "subject matter, visual or audio content, age of models, language or other characteristics of the web site or on-line service, as well as whether advertising promoting or appearing on the web site or on-line service is directed to children."[25] The use of animated characters may increase the

24. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.3 (1999); *see also* § 312.2 (definition of "website or online service directed to children").

25. *Id.* § 312.2.

likelihood that the site will be considered targeted to children.[26] The FTC will consider empirical evidence regarding audience composition and evidence about the "intended audience."[27] Unfortunately for some web sites this "guidance" leaves a lot of room for interpretation and, as discussed below, may chill the information practices and services of web sites unsure of where they stand.

Because the FTC has said that it will look at the intent of the web site operator, I have encouraged clients to review their web sites, focusing on areas and features that may unintentionally seem to be directed to children. Companies should take the time to make a conscious decision about directing or not directing content to children if they have any desire to gather personal information from visitors to those areas of their site.

The growing on-line advertising industry led by the much publicized DoubleClick will need to be cautious about serving ads to sites or areas of sites directed to children. In the FTC's Statement accompanying the Rule, the FTC stated that if companies that serve banner advertisements "collect personal information directly from children who click on ads placed on web sites or on-line services directed to children, then they will be considered operators who must comply with the Act, unless one of the exceptions applies."[28] The FTC added in a footnote that: "It may be appropriate for such companies to provide a joint notice with the operator of the host website."[29] With the pace of the industry, it is difficult to ascertain what level of information is being collected by such companies, but, if they are either collecting personally identifiable information from kids who click on ads, or if they are able to tie anonymous cookie data they collect with personally identifiable information from another source, they will need to comply with the Rule.

In fact, COPPA may impact many players in the on-line advertising industry. Banner advertisements increasingly employ data entry windows. That data may be sent directly to one or more of several entities including the company that is advertising its products or services, an advertising agency, and advertising serving company, or the web site providing the banner space itself. If the web site that offers a banner window "knows" that the user viewing the web page

26. *See id.*

27. *Id.*

28. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59891 (1999) (to be codified at 16 C.F.R. pt. 312).

29. *Id.* at 59892 n.57.

is a child, will that knowledge be imputed to the advertising agency or the ad serving company? Perhaps banner ads will have to have their own privacy policies?

These questions are complicated further when one realizes that an ad serving company is often not in a direct contractual relationship with the web sites to which it serves ads, but rather it may have an intermediary agreement with an advertising agency. This lack of contractual privity between the ad serving company and the web site may either protect the ad serving company from knowledge or may just make it more important for them to monitor where they are serving ads. As the contracting party, it may bring the advertising agencies into COPPA's reach even if they do not place cookies, collect the information or serve the ads.

2. General Audience Sites

The primary choices available to a general audience web site under COPPA are to: (1) stop collecting subscriber information (not attractive); (2) refrain from asking for age; (3) prohibit membership by those under 13; and/or (4) seek adult verification for those who self-identify as under 13. For general audience sites, the choice between options 2, 3 and 4 or some combination thereof, will come down to a cost benefit analysis and depend largely on the make up of the user base, the relative dependence on age-targeted advertising, and the types of services offered.

Even if the web site is attractive to those from age 10 to 20, the 10 to 12-year-olds may be asked to stand on the sideline in order for the web site to avoid the additional burden of "knowing" that a user is a child. (Of course, many of the kids will probably just "sneak in" by registering as 15-year-olds.) If a site knows that a member is a child, requests for additional information in the future may require another round of obtaining parental consent.

COPPA applies to "disclosures" of personal information by children as well.[30] Thus, even general audience sites that do not collect personally identifying information but offer chat services with "screen names" can get in sticky territory if they monitor the chat rooms.[31] If a user identifies herself as a child and submits a message containing her personal contact information and the "monitor" sees it, then the monitor will need to delete the personal contact information from the posting in order for the site to be able to say that it did not

30. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (1999).

31. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59889.

"collect" the information. Sites that *want* to monitor their chat rooms to prevent them from degrading into worthless banter and sex talk will need to educate the employees and agents who do the "monitoring" about COPPA rules.

The potential liability for allowing children to disclose personal information is in sharp contrast to the broad shield against liability for defamation claims that on-line service providers now wield thanks to § 230 of the Communications Decency Act of 1996[32] and its broad interpretation in recent case law.[33] Neither Congress nor the courts have offered on-line service providers safe harbors from contributory liability for invasions of privacy by their users. COPPA's limited safety zones may be the guide for future regulation in this area.

3. Web Sites in the Grey Area

Until benchmark cases are addressed in the higher courts, many sites that have a significant percentage of users under age 13 will be unsure whether their policy of "prohibiting membership by those under 13" or seeking permission for those who self-identify as under 13 will suffice. If they are considered "directed to children," statements meant to dissuade participation by children will not matter – all users will need to demonstrate that they are an adult or, if a child, that they have their parental consent before the site can collect information from them (subject to the exceptions discussed below).

In particular, web sites directed to teenagers may not be able to tell whether they will be considered "directed to children." I have advised some clients to analyze their membership database to record current usage statistics by age in order to support their claim that the site is not "directed to children." When they stop collecting age information in order to avoid "actual knowledge," they will render themselves less able to demonstrate the actual age statistics of their users.

Consider web sites focused upon video games. The audience age range will be wide but concentrated in the teens and twenties. If a gaming site has an audience of 10 to 12-year-olds that makes up 5% of its total audience, would that make the web site "targeted to children?" Such a label seems unlikely, but the 5% could represent thousands of kids. Would a court or the FTC be swayed by evidence that the 5% of members of a service who are children equals fifty

32. 47 U.S.C.A. § 230 (West Supp. 1999).

33. For recent court interpretations of this statute, see *Zeran v. America Online Inc.*, 129 F.3d 327 (4th Cir. 1997), and *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.C.C. 1998).

thousand individuals? As tempting as it may seem, the answer should be "no."

As Professor Eugene Volokh reminds us in his recent article, most regulatory protections of privacy are concurrently restrictions on speech.[34] In order to avoid a potentially unconstitutional chilling of protected speech, I suggest that the FTC use a narrow analysis when determining whether a site is "directed to children." If a site can show that children under 13 (or their parents) do not make up a majority of the visitors, then I think the site should be considered a "general audience site," requiring actual knowledge that they are dealing with a child. To place all sites that have a significant number of participants under age 13 in the "directed to children" category, would, in my opinion, stretch COPPA's reach too far and would chill many web sites and services available to teenagers and young adults.

C. Issues for Implementation

1. What is "actual knowledge"?

Once a web site has determined that it is not directed to children, it need only worry about COPPA to the extent that it has actual knowledge that it is collecting information from a child. But what is "actual knowledge" and, as some clients ask, "How can I avoid it?"

Many general audience web sites collect date of birth information for password verification or just for marketing reasons. With COPPA, any site that collects this information and associates it with personally identifiable information will have "actual knowledge" that they are dealing with a child. For many sites the burden of complying with COPPA's mandate to seek parental consent for those who identify themselves as under age 13 outweighs the benefit of collecting the age data. As a result we will increasingly see notices that registration is not allowed to those under age 13. Other sites may move to merely collecting broad age range data, by for example, asking new registrants if they are "Under 18," "18-35" or "over 35." These ranges may serve the marketing needs without conveying "actual knowledge" upon a company about whether a particular user is under age 13.

The FTC will be on the lookout for web sites who do not ask for age but who ask for information that conveys the same idea. The

34. *See* Eugene Volokh, *Freedom and Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, STAN. L. REV. (forthcoming) (on file with the Santa Clara Computer and High Technology Law Journal).

FTC "will examine closely sites that do not directly ask age or grade, but ask "age identifying" questions such as "what type of school do you go to: (a) elementary; (b) middle; (c) high school; (d) college."[35]

It will be interesting to see how general agency law principles are applied to the COPPA version of "actual knowledge." When will a company be considered to have actual knowledge obtained by its third-party agents? In the comments accompanying the Rule, the FTC discussed the potential liability for affiliates and stressed that the most important factor for determining whether a company will be considered an "operator" is its relationship to the information collected and whether it has an interest in the data.[36] "The [FTC] likely will not pursue an entity that is an 'operator,' but has not facilitated or participated in, and has no reason to know of, any Rule violations."[37] The message seems to be that if a web site values the information it collects from its users, then the site better make sure that both its employees and third party service providers know how to play by COPPA's rules.

An example of a gray area involves the common practice on large interactive web sites of letting certain users become "SYSOPS" to monitor chat rooms. Many of these positions do not rise to the level of employee and yet the SYSOPS have the ability to remove postings or block certain users from the chat and bulletin board areas. Will a SYSOPS be considered an agent of a company such that if the SYSOPS learns of a child disclosing personal information in a chat area, the company itself will be deemed to have actual knowledge? The FTC Statement did not clarify this point but it will likely come up. In the meantime, there is certainly no harm for an on-line service provider to instruct SYSOPS on what to do if they do notice a child disclosing personal information in a public area of the web site.

2. Verifiable Parental Consent

For web sites directed to children and for general audience web sites who learn that they are dealing with a child, the issue of obtaining parental consent prior to collecting personal information becomes a key issue. The Rule states that: "Before collecting, using or disclosing personal information from a child, an operator must

35. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59892 (1999) (to be codified at 16 C.F.R. pt. 312).

36. *See id.* at 59891.

37. *Id.* at 59891 n.55.

obtain verifiable parental consent from the child's parent."[38] The FTC has offered some significant guidance in this area. It has called for "reasonable efforts," taking into consideration "available technology"[39] and refers to the following methods as sufficient to satisfy the requirements:

- Providing a consent form to be printed out and sigend by the parent and returned by postal mail or fax;
- Requiring a parent to use a credit card to demonstrate adult status;
- Having a parent call a toll-free number staffed by personnel trained to determine if the person is an adult;
- Verifiying a parent's digital certificate using public key technology; and
- Email approval accompanied by a PIN or password obtained through one of the above methods.[40]

In addition, until April 21, 2002, companies that will only be using children's personal information for internal purposes may obtain consent using a parent's e-mail address (collected from the child) so long as this is coupled with an additional verification step such as a follow up telephone call, letter or e-mail. This is called the "sliding scale" approach and will be reevaluated by the FTC in light of advances in technology and verification options in the next two years.[41]

Choosing between the various methods will require a thoughtful cost benefit analysis. The implementation and operational requirements for each method vary and for most companies, the decision requires a high-level corporate buy-in. For some companies, the results of the inquiry into what type of consent to require have been startling enough to dissuade them from collecting information from children altogether or from allowing children to use their site. For web sites directed to children, this may be the hoped-for result of the new law. For general audience sites, it may just mean that we will have less data about what children under 13 are doing because they will increasingly identify themselves as older to obtain access to web sites.

38. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (1999).

39. *Id.* § 312.5(b).

40. *See id.*

41. *See id.*; *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59901.

One benefit that some sites are finding as a result of seeking parental consent is the development of a positive relationship with the parents. Parents will generally appreciate being notified about their child's activities on the Internet and may think highly of a company for seeking their involvement.

3. Safe Harbors

There are a few safety-zones in the new law – instances where the collection of personal information from a child are excepted.

The first thing to note in this regard is that COPPA only applies to personal information obtained on-line after April 21, 2000. COPPA does not reach data collection done through other means such as mail-in contests, shopping malls, sports camps etc.[42] Also, personal information collected prior to April 21, 2000 is not covered under COPPA, but additions to this information would be. So, for example, if a web site has many registered users who are under 13, they do not need to cancel these childrens' accounts but the web site may not gather additional personal information from the child without obtaining parental consent. In addition, COPPA provides that the following collections of personal information from a child do not require parental consent:[43]

- Contact information collected for the sole purpose of obtaining parental consent;[44]
- Contact information to be used on a one-time basis to respond to a specific request of a child. For example, a site may use the email address of a child to respond to an email request from the child (note: cannot use the data again and must delete after the one-time use);[45]
- Contact information to be used to respond on a repetitive basis to a single request and not for any other use.[46] For example, a site will not be deemed to have "collected information from a child" if the child merely signs up for an email newsletter and the child's email address is not used for any other purpose. If

42. In the FTC's proposed rule, issued April 27, 1999, the FTC had extended the reach of COPPA to these offline areas, but the Act as passed by Congress applied only to on-line collections of information so the FTC narrowed the scope in the final rule.

43. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(c) (1999).

44. *See id.* § 312.5(c)(1).

45. *See id.* § 312.5(c)(2).

46. *See id.* § 312.5(c)(3).

the site is directed to children or is aware that the recipient is a child, the site must take reasonable steps to provide notice to the parent via letter or via the parent's email address;

- Contact information to be used to protect the safety of a child and to be used solely for that purpose.[47] This exception also required reasonable efforts to provide notice to the parent. It is difficult to predict the situations in which this exception would be applicable;
- Contact information collected to the extent reasonable to (i) protect the security or integrity of the website; (ii) to take precautions against liability; (iii) to respond to judicial process; or (iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.[48]

Finally, the FTC does offer the option for companies, organizations or groups, to apply for and receive approval of a self-regulatory plan regarding collection of on-line information from children.[49] These self-regulatory guidelines are referred to as "Safe Harbors" and at least one company has already applied for one to cover its Privacy Seal program.[50]

III. CONCLUSION

As the FTC begins to bring enforcement actions under COPPA, some of the questions I have raised in this article will surely be answered and some gray areas clarified. Until then, I recommend a careful reading of the Rule for any commercial web site that is directed to, targeted to, or used by children.

Hopefully, the FTC will be able to use COPPA to shut down the truly bad actors who collect information from children for improper purposes. In the process, however, many on-line companies collecting information without any nefarious purpose will be

47. *See id.* § 312.5(c)(4).

48. *See id.* § 312.5(c)(5).

49. *See* 16 C.F.R. § 312.10(a) (1999).

50. PrivacyBot.com became the first organization to submit a letter requesting "safe harbor" classification. *Request for "Safe Harbor" Seal Program Status Under COPPA*, Letter from PrivacyBot.com to Donald S. Clark, Secretary of the FTC (Dec. 15, 1999). See <http://www.ftc.gov/privacy/safeharbor/shp.htm> for links to this request and other FTC announcements related to COPPA's Safe Harbors.

scrutinized as well. The important sound bite for such law-abiding companies to hear is that complying with COPPA, or any new law concerning collection and use of information, may not be simple or painless and therefore deserves thoughtful attention and resources. For many in the Internet industry, COPPA will be just the incentive they need to evaluate their collection and use of consumer information before the rest of the tide of privacy regulations rolls in.