

Is Your Web Site COPPA Compliant?

By Alan L. Friel

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA), broadly expanding the Federal Trade Commission's (FTC) enforcement powers in the Internet arena. Since then, states and the FTC have become more active in regulating the collection, use and security of consumer's personal information generally. However, the protection of children's personal information remains a top FTC enforcement goal, and the commission has become more aggressive in enforcement of COPPA each year. Companies that fail to proactively act to ensure COPPA compliance do so at the risk of seven-figure penalties.

COPPA's goal is to prevent Web sites from collecting information about children under the age of 13 without informed parental consent. When Congress passed COPPA, it required the FTC to provide guidelines (Rules) to advise Web site operators on how to avoid a COPPA violation. The Rules apply a sliding scale of parental consent requirements if a Web site is "directed at children under 13 years old" or the Web site operators have knowledge that children under 13 are submitting personal information. In March 2006, the FTC completed a review of the Rule and announced that it would be retained unchanged.

Web sites that violate COPPA are subject to substantial penalties, which have increased over recent years. For example, in 2003, Mrs. Fields and Hershey's paid the then highest-to-date civil penalties of \$100,000 and \$85,000, respectively, because they collected personal information from children under the age of 13 without obtaining informed parental consent. Three years later, in September 2006, Xanga.com, a popular social networking Web site, agreed to pay a \$1 million penalty for maintaining a user registration system that permitted users under the age of 13 to submit personal information, finding that certain registration submissions established knowledge that restricted information was being improperly collected.

This article provides Web site operators with suggestions on how to comply with the spirit of COPPA when legal obligations are not crystal clear, as in the case when the operator of the Web site in question believes that it can make a good faith effort to be a "general audience" Web site, but has reason to believe that the site may attract visitors under the age of 13 and is unsure how the FTC will view and treat the site. In addition, numerous Web sites that have chat rooms, message boards, online surveys or utilize e-mail communications with users are likely, at least technically, to collect personal information from children who utilize such site applications. These Web sites could benefit by taking preventative measures to ensure that they are not collecting or publishing such information from users under 13 years of age.

DIRECTED V. GENERAL SITES

COPPA differentiates between Web sites "directed to children" and those it considers to have a "general audience." The duties a Web site has under COPPA differ dramatically depending on this classification. Web sites with a "general audience" *only* have duties when they have *actual knowledge* that children under 13 are using their Web sites *and* providing personal information. FTC Children's Online Privacy Protection Rule, 16 CFR §312.2 (1999). In contrast, Web sites "directed to children" do *not* need actual knowledge that children under 13 are providing personal information. 16 CFR §312.2. All Web sites "directed to children" that want to collect personal information are *required* to provide notice and receive informed parental consent before doing so. However, if, for any site, birth year or age data is collected from users and any such submissions indicate that the user is under 13, the knowledge requirement is likely met. Accordingly, a survey on a general audience site that includes a question on year of birth and does not prevent completion by users under the age of 13 could result in the Web site effectively being put on notice that it is collecting COPPA-regulated information and bring the entire site henceforth under the same Rules as sites directed at children. Similarly, if a site permits user profiles or user-generated content that identify users as under the age of 13, the site may similarly be deemed to have knowledge that it is collecting personal information of children under 13 years of age. Certainly, if a Web site registration collects age or birth year information and does not prohibit registration by children under 13, the site has knowledge that it is collecting such data. Accordingly, it is recommended that all sites take reasonable steps to prevent collection or publication of personal information of children under 13 years of age.

COPPA regulates the "collection" of "personal information." "Collection" of personal information can occur from online requests specifically for personal information, chat rooms, message boards, passive tracking, or using codes to identify an individual's cookies. 16 CFR §312.2. "Personal information," as defined by COPPA, includes names, addresses, phone numbers,

e-mail addresses, and other information that could identify the individual either online or offline. *Id.* For cookies, if the operator collects individually identifiable information or non-individually identifiable information that is combined with an identifier, that is “personal information” under COPPA. *Id.* Personal information does not include persistent identifiers, such as static IP addresses or processor serial numbers by themselves. *Id.* Because COPPA includes “passive tracking,” business people and in-house counsel may not even be aware that their company Web site is collecting “personal information.”

If a Web site is “directed at children,” or has a “general audience” and has actual knowledge that it is collecting or maintaining personal information of children under 13 are using the site, the site must, among other things, provide clear notice and obtain informed, verifiable parental consent in order to comply with COPPA. (See the Rules for more information on the requirements.)

The Rules state that the FTC, in determining the adequacy of the parental consent, will look at two factors: 1) whether the method ensures that it is the parent providing the consent; and 2) whether the method is a “reasonable effort,” taking into consideration available technology. 16 CFR §312.5(b). Some methods listed by the Rules include: downloading forms that parents send in with a signature, using credit card verification, calling a toll-free number with trained personnel and using a digital signature. The measure the FTC will deem appropriate to obtain verifiable parental consent depends upon how the operator intends to use the information collected. The FTC uses a sliding scale, with internal use requiring minimal verification and use for third party marketing purposes requiring the most verifiable

forms of consent. If the Web site is directed to children under 13, or the operator is deemed to have knowledge that it is collecting, maintaining or publishing personal information of children under 13, the operator must also:

- Post a privacy policy on the Home Page of the Web site and link to the privacy policy on every page where personal information is collected;
- Provide notice about the site’s information collection practices to parents and obtain verifiable parental consent before collecting personal information from children;
- Give parents a choice as to whether their child’s personal information will be disclosed to third parties;
- Provide parents access to their child’s personal information and the opportunity to delete the child’s personal information and opt-out future collection or use of the information;
- Not condition a child’s participation in a game, contest or other activity on the child’s disclosing more personal information than is reasonably necessary to participate in that activity; and
- Maintain the confidentiality, security and integrity of personal information collected from children.

The Rules provide a number of factors that the FTC would use in determining a Web site’s classification as “directed to children” or “general audience.” These factors include: the site’s subject matter, visual or audio content, age of models, language, other characteristics of the Web site or online service and empirical evidence regarding actual and intended audience compositions. 16 CFR §312.2.

BE PROACTIVE

Unfortunately, even after a good faith application of site characteristics to these factors, numerous “youth-oriented” Web sites may still be unsure which category they will be deemed to belong to and how to avoid a COPPA violation. A Web site that believes it is has a “general audience” but is possibly attracting some users under 13 years of age should take proactive steps to decrease the likelihood that the FTC classifies it as a Web site “directed at” children.

Show Older Appeal

For example, it can use older models that appeal to a more young adult or adult audience — most cartoon characters would make a Web site look like it is “directed at children.”

A Web site can place advertisements that appeal to an older clientele and avoid advertisers that have products that might appeal to children.

Finally, a Web site can use songs and graphics that are likely to appeal to an older demographic.

Unfortunately, even taking these steps may not be enough to ensure that the FTC will not classify the site as “directed to children,” especially when teens and college students are the target demographic. Many programmers believe that children aspire up in age, and that content targeting teens will thus be popular with pre-teens and children. The FTC will also evaluate empirical evidence, if available, about the Web site’s traffic, including age information. The Rules have provided no guidance on how many visitors under the age of 13 need to visit the Web site in order for it to receive the “directed to children” classification — or when it will be imputed with knowledge. Thus, Web sites that believe they have a “general audience” still may want to take preventative measures in a good faith effort to comply with COPPA’s goals.

Notice and Consent

The safest option for a Web site to comply with COPPA would be to follow the notice and consent requirements listed above. This would require asking *all* the participants to provide self-disclosed age information plus some additional means of verification. Then, depending upon the age of the participant, notice and informed, verifiable parent consent may be necessary. Unfortunately, while perhaps the safest route, such an approach would not be consistent with typical Web site operation for general audience sites and would likely make a site more difficult to use than a competitor’s site.

Certification

Another available option for a Web site is to receive certification under an industry self-regulation program such as the so-called “safe harbor” programs such as the FTC-approved

Alan L. Friel is Counsel in the Los Angeles office of international law firm Kaye Scholer LLP, where he practices in the areas of advertising, entertainment and technology law. He can be reached at AFriel@kayescholer.com. Research assistance was provided by Kaye Scholer Associate **Steven Wright** and Summer Associate **Jessica Post**.

Better Business Bureau's Children's Advertising Review Unit (CARU), ESRB Privacy Online, a Division of the Entertainment Software Rating Board, or the programs administered by the companies TRUSTe and Privo, Inc. Consideration for these programs requires financially supporting the industry organization or paying a fee. These safe harbor program requirements are also more stringent than the text of the Rules, and for many sites that are unsure of how the FTC would classify them, would probably require one of the age verification methods listed above that cost money to implement and could also reduce Web site traffic. The advantage, however, to safe harbor certification programs is that the FTC will not bring enforcement actions against Web site operators that have been certified by an approved program and comply with its FTC-approved guidelines.

Age Screening

The next best alternative for a Web site that believes it has a "general audience," but is unsure about how the FTC would classify it, is to take reasonable steps to prevent collection or publication of personal information of children under 13 years of age. This requires asking users about their age before "collecting" "personal information" and then segregating those that are under 13 from those that are over 13 before any personally identifying information is requested or access is permitted to applications (*e.g.*, profiles and chat rooms) that could enable users to submit such data. In making this age determination, a Web site could ask for a birth date or a grade level through open-ended questions. Web sites should be conservative in estimating the age of grade levels and require any borderline grade participants, such as 8th graders, to furnish verifiable identification or be screened as under 13. Better yet, a Web site could also require a participant to fill out both grade level and birth date questions, creating a more reliable

screening mechanism — an approach recommended for sites that are for young adults but might arguably be attractive to younger children.

In creating age-screening mechanisms, Web sites should take precautions not to ask participants for their ages in a way that might tip them off to the fact that there is a specific age requirement for use without parental consent. The FTC disapproves of such "tipping" and an operator risks an enforcement action if it does so. Tipping is more likely to be found if the age requirement is disclosed in connection with the request for the age, as opposed to a mere reference in the Privacy Policy or Terms of Use to minimum age requirements for registered users.

After the Web site performs its initial screen, it has two options for how to deal with participants it identifies as under 13. The Web site could provide the identified participant the opportunity to provide informed, verifiable parental consent and ban the user activities that could lead to disclosure of personal information until he or she does so. Alternatively, the Web site could just refuse to allow the screened participant to partake in any online activity where "personal information" is collected. This could include not allowing participation in chat rooms, postings or e-mail type functions. If it is possible to disable the chat, posting and e-mail functions of the Web site for users under 13, that would seem to be preferable to totally banning them, both from a commercial standpoint and because the FTC encourages Web sites to find ways to comply with COPPA without totally excluding children under 13. The site operator should employ technical measures to prevent the rejected user from simply registering again using a different birth year (*e.g.*, attaching a cookie that blocks the user).

In addition, a site that has applications that a child could use to submit or publish personal information (*e.g.*,

chat rooms, user generated content and profiles, etc.) can utilize technology such as robots that search for user-generated content that lists a birth year or age. Chat room monitors can perform a similar function. These precautions are especially recommended for sites that could potentially attract children under 13, but are not intended for — or directed to — children. For sites directed to children, in addition to restricting access to these areas to children whose parents have given the requisite consent, these types of precautions are essential. Several children's sites have gone so far as to employ software systems that prohibit a user from posting e-mail addresses, phone numbers and other personal information, in addition to inappropriate language.

CONCLUSION

All Web site privacy policies should explain consumer's COPPA rights and the site's intention to comply with COPPA. Even general audience sites should provide parents with a mechanism to contact the operator and have the personal information of children under 13 removed in the event it was inadvertently submitted.

Complete assurance that even general audience Web sites will be in absolute compliance with COPPA may not be practicable or possible, absent taking certain measures to comply with COPPA as discussed above. The more proactive a company is in taking steps to comply with the spirit and purpose of COPPA, the more likely they will avoid FTC problems. COPPA compliance is an essential part of every Web site operator's ongoing privacy law compliance program.



The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.