taming the wild West

Laws and Regulations Governing the Technology Industry

by John Nicholson
<*John.Nicholson@ShawPittman.com*>

John Nicholson is an attorney in the Technology Group of the firm of Shaw Pittman in Washington, D.C. He focuses on technology outsourcing, application development and system implementation, and other technology issues.

Back in the Old West, people lived in small enclaves of civilization that provided them with some protection from the dangers of the wild.[1] Outside of those small outposts, you took your chances. Inside them, people were protected by a few laws and the fact that everyone knew everyone else. Many laws and regulations that were commonly enforced in larger Eastern cities were unnecessary in these small communities. Instead, peer pressure enforced a general code of conduct and standard of behavior.

As news of the freedom and opportunity of the West spread, and as it became safer and easier to travel, more and more people moved to the West. As the West became more densely populated, more people interacted more frequently and more anonymously. Many of these interactions involved people who were transitory and/or unfamiliar with (or unwilling to comply with) the general code of conduct observed by those who already lived there. This caused increasing conflict. To avoid this increasing conflict, new laws were passed and old laws were better enforced. Those who lived in the once-small towns bemoaned the invasion of the horde of strangers and the loss of their "small-town" way of life.

Similarly, when the technology industry and the Internet were new, very little government involvement was required. The community was small enough and homogeneous enough that codes of conduct and unwritten rules governed behavior, enforced by peer pressure and public opinion within the community. Even as recently as the early '90s, one of the big rules was that the Net was not for business. How things have changed.

Just like the Old West, the technology industry and the Internet are victims of their own success. As people have realized the opportunities presented by the Net, and as technology has made getting access easier, more and more people have flooded into the "small towns" that used to populate the Net. AOL alone has millions of subscribers. Email once the realm of academics, researchers, and programmers is now a mission-critical application. The Web is now a major marketing and business tool. Until recently, there has been very little need for new legislation in this area, or even enforcement of many existing laws that apply outside of the cyber-realm. The increasing online population, however, combined with the anonymity and the relative lack of knowledge of many of these new users, has led to increasing conflicts.

Just as new laws were passed and old laws were enforced in the Old West, the same thing is happening to the technology industry. As a part of this trend, there have been several new developments that technology professionals should know about. This and my next few columns will deal with the Children's Online Privacy Protection Act (COPPA), the Uniform Commercial Information Transactions Act (UCITA), and the Digital Millennium Copyright Act (DMCA). Depending on what your company (and you) do, one or all of these new laws could have an impact on you.

The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act[2] was enacted by Congress to protect children's privacy by giving parents the ability to control what information is collected from their children online. COPPA directed the Federal Trade Commission (FTC) to draft rules that would control how Web sites gather, store, and disclose such

information. The rules enacted by the FTC[3] became effective April 21, 2000, and apply to the online collection after April 21, 2000, of "personal information" from children under 13. The new rules spell out what a Web site or online service "operator" must include in a "privacy statement," when and how to seek "verifiable consent" from a parent, and what responsibilities an operator has to protect children's privacy and safety online.

WHY DO WE NEED SOMETHING LIKE COPPA?

Aside from the obvious safety issues and the anecdotal evidence regarding stalkers and pedophiles on the Net, there is an economic reason for this type of regulation. Infor-mation has become a valuable commodity. And, as with every other valuable commodity, those who have it are trying to protect it, and those who want it are trying to come up with new ways to acquire it. One of the reasons for something like COPPA is to prevent companies from exploiting children's ignorance of the value of personal information from both a safety and an economic perspective.

For example, according to a recent survey by the Annenburg Public Policy Center,[4] two-thirds of children aged 10 to 17 were willing to provide online the names of their family's favorite stores in exchange for a free gift. In addition,

- 54% were willing to provide the names of their parents' favorite stores;
- 44% were willing to disclose the type of car the family uses;
- 39% were willing to discuss the amount of their allowance and whether their parents talk "a lot" about politics;
- 26% were willing to disclose details about their parents' activities on the weekend; and
- 16% of 10—12-year-olds admitted to having given information about themselves to a Web site.

On top of these statistics, the survey also revealed that 46% of parents were not aware that Web sites could gather information about a user without the user's knowledge.

Given the willingness of children to disclose personal information about themselves and their families, as well as parents' ignorance of the methods used by Web sites to collect information, a regulation like COPPA is necessary to protect children and parents from their own ignorance.

WHY SHOULD YOU CARE ABOUT COPPA?

If COPPA applies to your Web site or online service and you do not comply with the regulations, the "operator" (see below) of the Web site or online service can be fined $10,000 per violation.[5]

WHO HAS TO COMPLY WITH COPPA?

The COPPA regulations apply to the following:

1. The "operator" of a commercial Web site or online service "directed to children under 13" that collects "personal information" from children or
2. The "operator" of a general-audience Web site who has "actual knowledge" that it is collecting "personal information" from children under 13.[6]

As with any law or regulation, the definitions are very important.

Who is an "operator"? To determine whether an entity is an "operator" with respect to information collected at a particular Web site, the FTC will consider such factors as:

- Who owns and controls the information once it is collected?
- Who pays for the collection and maintenance of the information?
- What preexisting contractual relationships exist in connection with the information?
- What role does the Web site play in collecting or maintaining the information?[7]

How do you determine whether a Web site is "directed to children"? A site will be evaluated based on:

- the subject matter;
- specific audio/video content;
- the age (or apparent age) of the models or other people pictured on the site;
- level of language used on the site;
- whether advertising on the site is targeted to children;
- the age of the actual or target audience; and
- whether the site uses "child-oriented features" such as animated characters.[8]

What is "actual knowledge"? If a site has a registration form that asks for a user's age and the user enters an age under 13, then the operator of the site must comply with the COPPA regulations with regard to information provided by that user.

What is "personal information"? According to the FTC, personal information is information about a child that is collected online, such as the child's name, home or other address including street name and name of a city or town, email address, telephone number, Social Security number, or any other information that would allow someone to contact the child — including information such as hobbies or interests or information collected passively via cookies or other tracking technology if such information is linked to other "individually identifiable" information about that child.[9]

Complying with COPPA

If the COPPA regulations apply to your Web site or online service, there are a number of things that you have to do to comply with them. The first requirement is that you must develop a "privacy statement" that describes the information practices of your site or service. Once you have developed your privacy statement, if you are the operator of a site directed to children, you have to provide a link to the privacy statement on the home page of your site and at each area where your site collects personal information from children. If you are an operator of a general-audience site with a separate area directed to children, you have to provide a link to your privacy statement on the home page of the children's area and, although the regulations do not appear to require it, it would be a probably be a good idea to provide the link at each area where your site collects personal information from children. All of the links to the privacy statement are required to be "clear and prominent" (i.e., in a larger font or a different color). The FTC guidelines specifically state, "A link in small print at the bottom of the page — or a link that is indistinguishable from other links on your site — is not considered clear and prominent."[10]

What is a "privacy statement"? According to the FTC, a privacy statement should be clearly written and understandable and should not include any unrelated or confusing materials. A privacy statement must contain the following information:

- the name and contact information (address, telephone number, and email address) of all operators collecting or maintaining children's personal information through the Web site or online service.
- the kinds of personal information collected from children (e.g., name, address, email address, hobbies, etc.) and how the information is collected (i.e., directly from the child or through cookies or other means).
- how the operator uses the personal information collected by the site. For example, is it used for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room? (Note that if your site provides any kind of chat or posting functionality, you are providing a way for the child to make information publicly available).
- whether the operator discloses to third parties information collected from children. If so, the privacy statement must also list the kinds of businesses in which the third parties are engaged; the general purposes for which the third parties will use the information; and whether the third parties have agreed to maintain the confidentiality and security of the information.
- that the parent has the option to agree to the collection and use by the operator of the child's information without also consenting to the disclosure of the information to third parties. (Note that the effect of this option is that you must develop a system for tracking whether or not information collected about each child can be disclosed to third parties.)
- that the operator may not require, as a condition of participation, a child to disclose more information than is reasonably necessary to participate in an activity.
- that the parent can review the child's personal information, ask to have it deleted, and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.[11]

Parental Consent

Until 2002 (when the system will be reviewed), the COPPA regulations provide for two levels of parental consent, depending on what the operator intends to do with the information it gathers. If the operator of a Web site does not share with other companies or organizations any of the information it collects from children, then it can ask parents to grant consent to collect the information via an email, provided that the operator uses some type of follow-up (i.e., delayed email, fax, letter, or phone call) to increase the likelihood that the parent has actually consented. If the operator of the Web site intends to share the information it collects, it must set up a more verifiable system to obtain parental consent. This means that an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices. Possible methods for obtaining parental consent include requiring the input and verification of a credit card number, setting up toll-free numbers where operators are trained to recognize the difference between the voice and language of a 12-year-old and those of an adult, providing a form for parents to fill out and fax or mail back to the operator, or email from the parent signed with a digital signature.

The notice to parents must contain the same information included on the privacy statement on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use, and disclosure of the information; and how the parent can provide consent. The notice to parents must be clear and understandable, and must not contain unrelated or confusing information. An operator of a Web site or online service may provide the notice to parents by sending an email message, fax, or a notice by mail to the parent. Given the amount of information to be conveyed to a parent, a telephone call is probably not the best way to provide the notice.

Exceptions

The COPPA regulations require an operator to give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. However, if a parent agrees to the collection and use of their child's personal information, the operator may release that information to others who use it solely to provide support for the internal operations of the Web site or service, including technical support and order fulfillment.[12]

In the case of a monitored chat room, if all individually identifiable information is stripped from postings before they are made public and the information is deleted from the operator's records, then an operator is not required to get prior parental consent.

The COPPA regulations also include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance. Prior parental consent is not required for an operator to collect:

- a child's or parent's email address to provide notice and seek parental consent;
- an email address to respond one time to a single request from a child, provided that the operator then deletes the child's email address;
- an email address to respond more than once to a specific request (e.g., for a subscription to a newsletter), provided that the operator notifies the parent that it is communicating regularly with the child and provides the parent with the opportunity to stop the communication before sending or delivering a second communication to a child. (Note that to take advantage of this exception an operator must develop a system that notifies the parent before sending a second communication to the child and cancels the second communication if the parent does not consent.)
- a child's name or online contact information to protect the safety of a child who is participating on the site, provided that the operator notifies the parent and gives the parent the opportunity to prevent further use of the information;
- a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, provided that the operator does not use it for any other purpose.[13]

New Notice and Consent Required for Changed Practices

An operator is required to send a *new notice and request for consent* to parents if the operator materially changes the collection, use, or disclosure practices to which the parent had previously agreed. This means that each operator must develop a system for tracking *by child* the date that a parent provided consent, the uses of information to which

the parent consented, and a means of contacting the parent in the event that the use by the operator changes. For example, parental consent for a child to participate in contests that require the child to submit specific, limited personal information would not cover the addition by the Web site or online service of access for the child to chat rooms. Alternatively, parental consent for the operator to disclose collected information to marketers that provide one type of product might not extend to providing the information to a marketer of a different type of product. Unfortunately, in this case there is no clear line to identify when new consent is required.

Disclosure of Collected Information to Parents

Upon request, an operator must disclose the general kinds of personal information it collects online from children (e.g., name, address, telephone number, email address, interests, hobbies, etc.). In addition, upon verified request from a child's parent, an operator must disclose to the parent the specific information collected by the operator from the parent's children who have visited the operator's site(s) or used the operator's service(s). The FTC requires that an operator must use reasonable procedures to verify that the person requesting the child's information is, in fact, the child's parent before providing the information. According to the FTC, acceptable methods for verifying the parent's identity include:

- obtaining a signed form from the parent via mail or fax;
- accepting and verifying a credit-card number;
- taking calls from parents on a toll-free telephone number staffed by trained personnel (although the FTC does not describe the nature of the training to be provided to the personnel);
- email from the parent signed with a digital signature;
- email from the parent including a PIN or password obtained through one of the other verification methods listed above.[14]

The FTC provides protection from liability for inadvertent disclosures of a child's personal information to someone who claims to be a parent so long as the operator has used one of the above procedures and was acting in good faith to respond to a request for parental access to the information collected by the operator.

Parental Revocation of Consent and Requests for Deletion

Under the COPPA regulations, a parent may at any time revoke his or her consent, refuse to allow an operator to further use or collect his or her child's personal information, and direct the operator to delete the information.[15] If a parent does this, the operator is allowed to terminate any service provided to the child, but only if the information at issue is reasonably necessary for the child's participation in that activity. For example, an operator may require a child to provide his or her email address to participate in a chat room. If a parent later requests that the operator delete the child's information, the operator may refuse to allow the child to participate in the chat room. However, if other activities or services on the site do not require an email address, the operator must continue to allow the child access to those activities or services.

"Safe Harbors"

The COPPA regulations specify that industry groups or others can propose self-regulatory programs to govern participants' compliance with the COPPA regulations. Such self-regulatory programs must provide for independent monitoring and disciplinary procedures and must be approved by the FTC. If an operator complies with an approved self-regulatory program, that will generally protect the operator from fines for violations of the COPPA regulations.[16]

So far, the FTC has received two applications to create self-regulatory programs. The first was submitted by PrivacyBot.com[17] and the second by the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus.[18] The FTC has received public comments for both proposals,[19] and both are currently under consideration.

What Are People Doing Already?

Rather than set up procedures to comply with the COPPA regulations, E-Crush.com[20] and Email.com (a service of NBC Internet)[21] have banned those under 13 from their sites. From now on, Disney will require a credit card to set up a "family account" for use by those under 13, although the cards will not be charged.[22] As of April 24, 2000,

SurfMonkey.com estimated that it has spent between $50,000 and $100,000 to comply with the COPPA regulations.[23]FreeZone, a portal for kids from 8 to 14 that already requires parental consent, estimates that it will spend about $100,000 to comply with the COPPA regulations.[24] Alloy.com, a site targeted to teens, reported that it will spend approximately $200,000 to comply.[25]

Conclusion

Although necessary, the COPPA regulations place a substantial burden on Web sites that intend to collect and use or distribute personal information about children under 13. Sites will either have to develop the required systems and procedures or they will have to stop providing service to those identified as being under 13. It remains to be seen whether any of the regulatory "safe harbors" will be approved (the FTC may have acted on them by the time this article goes to print; if so, I'll provide an update in the next issue) and whether they will provide any relief from the burdens imposed by the COPPA regulations.

In the next issue, I'll discuss UCITA and some of its implications.

1. This article provides general information and represents the author's views. It does not constitute legal advice and should not be used or taken as legal advice relating to any specific situation.

2. 15 U.S.C. §§6501-6506.

3. 16 C.F.R. §312.

4. "Weak Link in Net Privacy: Kids," <*http://www.zdnet.com*>.

5. Brown, "COPPA: Locked, Loaded, Patrolling the Net," <*http://www.zdnet.com*>, 3/13/2000.

6. "How to Comply with the Children's Online Privacy Protection Rule,"<*http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm*>, Nov. 1999.

7. Ibid.

8. Ibid.

9. 16 CFR Section 312.2.

10. "How to Comply with the Children's Online Privacy Protection Rule," <*http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm*>, Nov. 1999.

11. Ibid.

12. Ibid.

13. Ibid.

14. Ibid.

15. Ibid.

16. 16 CFR Section 312.10.

17. <*http://www.ftc.gov/os/2000/02/privacybot.pdf*>.

18. <*http://www.ftc.gov/privacy/safeharbor/caruappmaterials.pdf*>.

19. <*http://www.ftc.gov/privacy.safeharbor/privacybotcomments/index.html*> and <*http://www.ftc.gov/privacy/safeharbor/65FR/24960*>.

20. Bowman, "Sites Brace for COPPA Fallout," <*http://www.zdnet.com*>, 4/20/2000.

21. Brown, "COPPA: Locked, Loaded, Patrolling the Net," <*http://www.zdnet.com*>, 3/13/2000.

22. Bowman, "Sites Brace for COPPA Fallout," <*http://www.zdnet.com*>, 4/20/2000.

23. Angwin, Wingfield, and Tran, "COPPA Cost Too High for Some Sites," <*http://www.zdnet.com*>, 4/24/2000.

24. Bowman, "Sites Brace for COPPA Fallout," <*http://www.zdnet.com*>, 4/20/2000.

25. Ibid.