Does COPPA Apply to Your Business?

Rebecca Herold, CISSP, CISM, CISA, FLMI

September 8, 2002

What do Girlslife.com, Bigmailbox.com, Insidetheweb.com and Toysmart.com have in common? (Well, sure, the title of this article pretty much gave it away, didn't it?) They are among the growing number of companies that have faced litigation for being in violation with the Children's Online Privacy Protection Act (COPPA). These and other companies facing litigation have typically paid $30,000 to $35,000 in fines from the FTC, in addition to often three to four times the fines in costs to update their web sites and associated information collection and sharing procedures to become compliant. For example, FreeZone, a portal site for children ages eight to fourteen, reported they will spend around $100,000 to comply with the law. This even though their site had already required parental consent, but had to improve their policies and procedures to truly meet compliance. Alloy.com, a site targeting teenagers, reported to Advertising Age that it would cost them approximately $200,000 for compliance. Various other reports indicate that sites have estimated costs reaching up to $500,000 to rewrite their information collection policies and restructure their procedures.

So, what is COPPA? COPPA is the first federal online privacy protection act. It was passed in October 1998, became effective April 21, 2000, and is enforced by the FTC. As reported in a March 25, 2002 Rob Fixmer article about privacy litigation at www.eweek.com "lawyers report widespread ignorance of the law's implications among companies doing business online." It's not really surprising; with the glut of proposed and new laws that apply to most organizations, it is often hard for even the most diligent lawyer to stay on top of privacy legislation with all their other responsibilities. That is where it is your obligation as a security and/or privacy professional to ensure your legal department is aware of and addressing privacy legislation such as COPPA.

As published on the FTC web site, the goal of COPPA is to give parents the tools to protect their children's privacy. As a parent of two very young and computer-savvy children, I too am extremely concerned with how easy it is for children to fall prey to the various schemes that lay in wait on the

electronic highway, not to mention the assorted spectrum of sick and twisted minds using the internet to exploit and devastate children's innocence. As a privacy and security professional I'm concerned with helping organizations know and understand security and privacy related regulations that must be observed, and take the steps necessary to meet compliance. It is alarming how nonchalant so many security professionals are about the COPPA regulations, and how many have indicated their legal counsel are "probably addressing it", or that the regulation does not apply to them because they are not a company whose primary customers are children. If you fit this description, please take a few moments to consider if this is actually the case. I've discussed COPPA with several security professionals from publishing, manufacturing and financial companies, and even some government officials, and some were very surprised to find their respective web sites had pages created especially for children…with no type of privacy notice whatsoever. If COPPA could apply to you, pick up the phone and have a nice chat with your legal counsel to ensure they have taken appropriate actions.

The COPPA regulations are based upon the government's fair information practices with an additional requirement that limits the personal information that can be collected at web sites from children younger than thirteen years old. If your organization collects personal information online, then you especially now have a challenge; you need to determine if your organization falls under the COPPA requirements. And, the rest of you need to take a little time to look at all the pages on your web site to see if personal information can potentially be collected from children.

You definitely must comply with COPPA if your web site or online service is aimed at children under 13 and collects personal information. However, you must also observe COPPA requirements if your web site or online service is directed to a general audience, and you have knowledge that you are collecting personal information from children.

What does COPPA require? Sites covered by COPPA must not only provide a prominent link on the home page to their privacy notice, but also a link at every place within the site where personal information is collected. Keeping in mind that the notice is intended to be read by children, it should be written clearly, simply and not contain confusing or legal-eze language. The privacy notice must contain:

- Name, mailing address, phone number, and email for all the operators that obtain the personal information collected at the site.
- A list of the personal information (for example, name, address, email address, birth date, hobbies, and so on) collected and how it is collected.
- A description of how the personal information is used.
- Whether or not the collected information is given to third parties, and how they use the information.
- A statement indicating parents may agree to collecting information, but that they do not also have to agree to allow the information to be given to third parties.
- A statement that children cannot be required to disclose more information than is necessary for the corresponding activity.
- A statement indicating parents have the right to review the information collected from their children, and may request to have it deleted and its use discontinued.

In addition to the children's privacy notice, the web site organization must also do the following:

- Send a separate direct notice containing the information from the privacy notice on the web site to parents using any one of a number of methods, including an email message, or a printed message sent by postal mail.
- Obtain prior verifiable parental consent for the collection, use and/or disclosure of personal information from children.
- Provide to parents, upon request, the means to review the personal information collected from their child.
- Provide parents with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from a child.
- Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is necessary for the activity.
- Establish and maintain procedures to protect the confidentiality, security, and integrity of the personal information collected.

There are "Safe Harbor" groups (not to be confused with the similarly named EU Data Protection Directive Safe Harbor program) that have created self-regulatory programs to govern the participants' compliance

with COPPA. The guidelines must be approved by the FTC and must include independent monitoring and disciplinary procedures. If your organization collects personal information from web site visitors you may want to consider participating in a safe harbor program.

The FTC provides guidance to understanding the full range of COPPA requirements at www.ftc.gov/kidsprivacy. This is a great, informative site; go there for full details of the COPPA requirements and information about participating in a safe harbor program. You can also call the FTC's Consumer Response Center, 1-877-382-4357, to ask for specific guidance, or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Of course, there is no way you can prevent children from giving false ages at the web site, or keep them from finding other ways around the controls related to parental notification. However, you should be doing as much as you possibly can by following the requirements of COPPA if they apply to your organization.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.