

WHAT DO THE OHIO ART CO., Eli Lilly and Co., and various so-called "information brokers" have in common? The answer is they all recently reached a settlement with the Federal Trade Commission (FTC) relating to the contention that they violated the privacy rights of various consumers.

The rapid development of the Internet has heightened privacy concerns, especially among individual users, who are deeply concerned about the privacy of their personal information. Federal and state governments have responded. Indeed, since 1996, a number of new federal laws have had a substantial impact on privacy-related issues, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act (COPPA), the ID Theft Assumption and Deterrence Act, and the Gramm-Leach-Bliley (GLB) Act. Just as important, over the past several years, the FTC has been applying its own statute to protect privacy. Businesses engaged in Web-based marketing thus should take special note of the FTC's recent settlements because they can provide a road map to help prevent costly privacy complaints.

Etch-A-Sketch

COPPA applies to operators of commercial Web sites and online services directed to children under age 13. Among other things, the law requires these Web sites to obtain verifiable consent from a parent or guardian before collecting personal information from children. It also prohibits sites from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such an activity.

Recently, the FTC announced a COPPA settlement with the Ohio Art Co., manufacturer of the Etch-A-Sketch drawing toy. The FTC alleged that the company's Web site collected the names, mailing addresses, e-mail addresses,

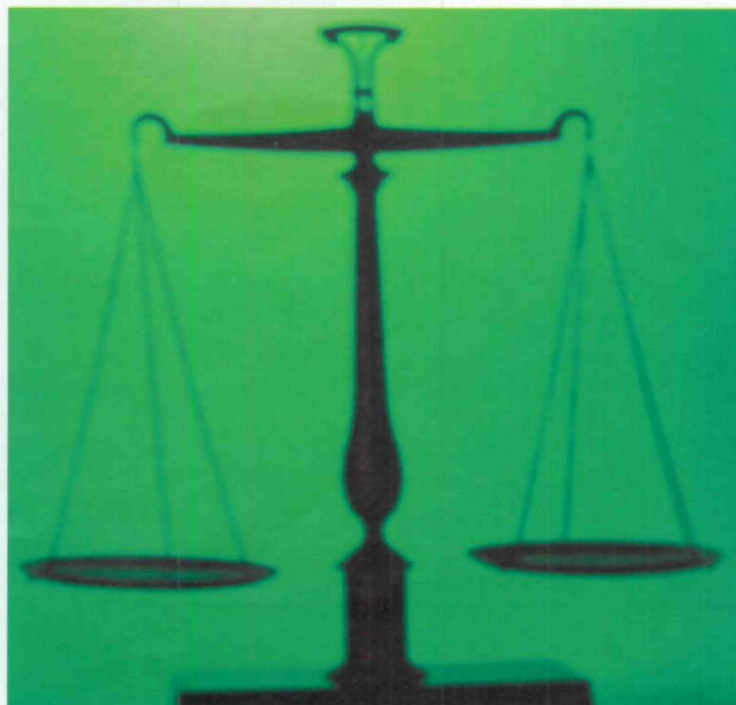
age, and date of birth from children who wanted to qualify to win an Etch-A-Sketch toy on their birthday. The FTC charged that the company merely directed children to "get your parent or guardian's permission first" and then collected the information without first obtaining parental consent as required by COPPA. In addition, the FTC alleged the company collected more information from children than was reasonably necessary for children to participate in this "birthday club" activity and that the site's privacy policy statement did not clearly or completely disclose all of its information collection practices or make certain disclosures required by COPPA. The site also failed to give parents the opportunity to review the personal information collected from their children and to inform them of their ability to prevent the further collection and use of this information, the FTC alleged.

The FTC and the company agreed to resolve the dispute. Among other things, the company agreed to (1) pay a \$35,000 civil penalty, (2) place a hyperlink to the FTC's children's privacy section on its

Protecting Online Privacy

The FTC takes notice of Web activity—and takes action.

By William M. Savino



Web site, (3) delete all personal information collected from children through the site from April 21, 2000, through the date of the settlement, and (4) report to the FTC explaining how it is complying with COPPA and the procedures it uses to protect the confidentiality, security, and integrity of personal information collected from children.

COPPA does not apply only to companies that operate Web sites directed to children. It also applies to general audience Web sites and online services that knowingly collect personal information from children. These entities must comply with all requirements imposed by the law and the FTC's rules as well.

Eli Lilly

The FTC also recently reached a settlement with Eli Lilly, an Indiana-based pharmaceutical company that manufactures, markets, and sells the anti-depressant medication Prozac. This settlement has important ramifications for all businesses that operate Web sites, given that it followed Lilly's unintentional release of personal information.

As the FTC explained, Lilly operated the prozac.com Web site, which the company promoted as "Your Guide to Evaluating and Recovering from Depression." The site offered consumers the Medi-messenger e-mail reminder service. People who used Medi-messenger could design and receive personal e-mail messages to remind them to take or refill their medication. Once a consumer registered for Medi-messenger, the reminder messages were automatically e-mailed from Lilly to the subscriber at the e-mail address he or she had provided according to the subscriber's requested schedule. These reminders were individualized e-mails and did not identify any other subscribers to the service.

The FTC alleged that, on June 27, 2001, a Lilly employee created a new computer program to access Medi-messenger subscribers' e-mail addresses and sent them an e-mail message announcing the termination of the Medi-messenger service. The June 27 e-mail message included all of the recipients' e-mail addresses within the "To:" line of the message, thereby unintentionally disclosing to each individual subscriber the e-mail addresses of all 669 Medi-messenger subscribers.

According to the FTC's complaint, Lilly claimed that it employed measures and took steps appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through the Web site. For example, Lilly stated that it "respects the privacy of visitors" to the site, "and we feel it is important to maintain our guests' privacy as they take advantage of this resource."

The FTC complaint alleged, however, that Lilly's claim of privacy and confidentiality was deceptive because Lilly failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information, which led to the company's unintentional disclosure of Medi-messenger subscribers' personal information (i.e., e-mail addresses). In fact, according to the complaint, Lilly failed to do the following:

- Provide appropriate training for its employees regarding consumer privacy and information security
- Provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used
- Implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail

Under the settlement, Lilly agreed to establish and maintain a four-stage information security program designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect consumers' personal information against any reasonably anticipated threats or hazards to its security, confidentiality, or integrity, and to protect such information against unauthorized access, use, or disclosure.

Specifically, Lilly agreed to designate appropriate personnel to coordinate and oversee the program. It also agreed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including any such risks posed by lack of training, and to address these risks in each relevant area of its operations, whether

**Over the past
several years,
the FTC has
been applying
its own statute
to protect privacy.**

performed by employees or agents, including management and training of personnel; information systems for the processing, storage, transmission or disposal of personal information; and prevention and response to attacks, intrusions, unauthorized access, or other information systems failures.

Lilly was also required to conduct an annual written review by qualified persons that monitors and documents compliance with the program, evaluates the program's effectiveness, and recommends changes to it. In addition, Lilly agreed to adjust the program in light of any findings and recommendations resulting from reviews or ongoing monitoring, and in light of any material changes to Lilly's operations that affect the program.

This settlement is significant for a number of reasons. For one thing, the release of the information was unintentional—yet the FTC nevertheless acted. Additionally, the FTC objected to the release in large measure because it violated Lilly's self-professed privacy policies. The FTC appears to be saying that it's a violation of federal law for a company to develop a privacy policy and then to fail to follow it.

Pretexting

In another recent settlement, the FTC addressed the emerging topic of pretexting, which is the practice of obtaining consumers' private financial information under false pretenses. The GLB Act specifically outlaws pretexting and soliciting others to pretext.

In this case, the FTC contended that a number of information brokers allegedly used false pretenses, fraudulent statements, or impersonation to illegally obtain consumers' confidential financial information (e.g., bank balances) and sell it.

In particular, the FTC charged that a number of brokers maintained Web sites where they advertised they could obtain non-public, confidential, financial information—including such things as checking and savings account numbers and balances, stock, bond, and mutual fund accounts, and safe deposit box locations—for fees ranging from \$100 to \$600, depending on the information sought. In cooperation with local banks, FTC investigators established dummy bank accounts in the names of cooperating witnesses, called the brokers, and posed as

a consumer seeking account balance information on her fiancé's checking account. The investigator provided limited information about the account to the brokers. The brokers or persons they hired allegedly called the bank, identifying themselves by the name of the supposed fiancé, and asked to check the balance. Thereafter, the brokers allegedly provided the account balance information to the FTC investigator.

The settlements barred the brokers, in connection with the obtaining, offering for sale, or selling of customer information of a financial institution, from (1) misrepresenting their identities or their right to receive customer information, (2) using others who will obtain information using deception, (3) selling or disclosing customer information obtained from a financial institution, and (4) making false and misleading statements.

The settlements also barred the operators from obtaining or hiring others to obtain consumers' financial information through illegal means or by hiring or contracting with others who use illegal methods to obtain consumers' financial information.

Upping the Ante

This past year, the FTC increased the resources dedicated to privacy protection by 50%. In addition to its enforcement of existing laws, the FTC is proposing additional rules (including consideration of a national do-not-call list that would be binding on telemarketers) and acting to educate businesses and consumers. Congress, too, is continuing its involvement in this field. A proposed Online Personal Privacy Act would affect a wide variety of very different businesses, ranging from the Web sites of local retailers whose sales cross state lines to the largest Internet service providers in the world. Privacy, a topic that many thought would be of little interest following Sept. 11, is more relevant—and more important—for businesses now than ever before. ■

About the Author

William M. Savino is the managing partner of Rivkin Radler LLP, a national law firm with offices in New York; Summit, NJ; and Santa Rosa, Calif. He may be reached at william.savino@rivkin.com.

**COPPA does not
apply only to
companies that
operate Web
sites directed
to children.**

Copyright of *Marketing Management* is the property of American Marketing Association and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.