This article was published in the March 2002 edition of *The Metropolitan Corporate Counsel*

The Lesson from Eli Lilly's Privacy Woes: Practice What You Preach

Inadvertent Disclosure of E-mail Addresses Ends in 20-Year Consent Order with the FTC

By Elaine M. Laflamme, Noel D. Humphreys and Michael B. Kupin

Akin, Gump, Strauss, Hauer & Feld, L.L.P.

The Federal Trade Commission (FTC) recently announced a settlement with Eli Lilly (Lilly) for deceptive and unfair practices stemming from that company's one-time, accidental release of 669 e-mail addresses. The e-mail addresses identified customers of Lilly who had signed up for an alert service on prozac.com. Under the consent order, Lilly must implement a four-stage security program that includes better training and supervision of its employees, internal and external risk assessments, and an annual review of the security program. The order provides great insight into what the FTC expects of companies that have publicly stated their commitment to protecting customer information in privacy policies posted on Web sites.

Unlike prior cases involving the intentional release of personally identifying information (PII) to third parties, Lilly's predicament arose from the accidental release of PII. This was not a situation where Lilly violated its *external* privacy policy by purposely disclosing PII to a third party (such as a co-marketer). Rather, it is about Lilly's failure to implement an effective *internal* information security program to prevent an entirely unintentional disclosure.

The consent order is significant in several respects. First, it makes clear that a company's obligation to maintain the confidentiality of PII goes well beyond the act of posting a privacy statement on the company's Web site. The FTC accused Lilly of posting a false and misleading privacy policy on its Web site based on the company's failure to implement appropriate measures to protect the confidentiality of customer information, that is, its failure to train and supervise employees. Second, the consent order suggests that a company's online privacy policy will be applied to its off-line data protection practices. Tellingly, the order does not distinguish between Lilly's online and off-line data protection practices in describing the steps Lilly must take to ameliorate faulty practices. The details of the accidental release and the resulting consent order provide necessary guidelines to other companies wishing to evaluate their data collection and handling practices in light of the FTC's emphasis on enforcement.

Lilly's Web site, prozac.com, offered a service to users that alerted them when to renew prescriptions. In keeping with industry standards, Lilly posted a typical privacy policy on prozac.com. The policy stated in part:

> "Eli Lilly and Company respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource. As a result, we have developed this privacy code. …
>
> "We will use Your Information to respond to requests you may make of us, and from time to time, we may refer to Your Information to better understand your needs and how we can improve our Web sites, products and services. …

> "Our Web sites have security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any of Your Information that you volunteer. ..."

Lilly terminated the service and directed an employee to alert customers to that fact. Instead of sending an individual e-mail to each customer, the employee sent a single e-mail to all of the 669 customers receiving the service, accidentally identifying each customer's e-mail address in the e-mail's "To" line.

Acting on a complaint by the American Civil Liberties Union, the FTC investigated the matter. The FTC concluded that the e-mail addresses were released "unintentionally," but drafted a complaint against Lilly anyway, charging the giant pharmaceutical company with unfair and deceptive acts or practices under Section 5(a) of the Federal Trade Commission Act. (The text of the complaint is available on the agency's site at www.ftc.gov.) The complaint accused Lilly of "fail[ing] to maintain or implement internal measures under the circumstances to protect sensitive consumer information." It cited numerous shortcomings in Lilly's data-handling practices, noting that Lilly had failed:

- to provide appropriate training for its employees regarding consumer privacy and information security
- to provide appropriate oversight and assistance for the employee who sent out the e-mail ...
- to 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.

The failure to take appropriate steps to protect the confidentiality of customer information, according to the FTC, violated Lilly's own written policies and made Lilly's privacy policy "false and misleading." Rather than litigate, the FTC and Lilly entered into a consent order.

The consent order requires Lilly to implement, among other acts, the following four-stage information security program:

- designate appropriate personnel to coordinate and oversee the information security program
- identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including such risks posed by lack of training, and address these risks in each relevant area of its operations, whether performed by employees or agents, including:

    - ♦ management and training of personnel
    - ♦ information systems for the processing, storage, transmission, or disposal of personal information
    - ♦ prevention and response to attacks, intrusions, unauthorized access, or other information systems failures

- conduct an annual written review by qualified persons ... which review shall monitor and document compliance with the program, evaluate the program's effectiveness, and recommend changes to it

- 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.

Lilly must also keep a sample copy of each "consumer-targeted print, broadcast, cable, or Internet advertisement, promotion, information collection form, Web page, screen, email message, or other document containing any representation regarding the Lilly USA division's collection, use, and security of personal information from or about consumers" and make it available to FTC investigators. The order's failure to distinguish between online and off-line practices comports with the recent observation of Howard Beale, director of the FTC's consumer protection bureau, that "privacy policies posted by companies online apply to their off-line practices as well."[1] It also indicates that the FTC's shift in focus—away from privacy legislation towards enforcement—should not be viewed as a weakening in the FTC's commitment to privacy.

Underscoring the view that privacy is becoming a "company" affair rather than the responsibility of a lone IT employee, Lilly must deliver a copy of the order to an exhaustive list of people, including "all current and future principals, officers, directors and managers." Surprisingly, the consent order is to remain in place no less than 20 years from its issuance.

Conclusion

The settlement provides a number of critical lessons:

- Companies must align their internal actions with their public words.
- Companies must support the statements in their privacy policies with demonstrable actions that go beyond implementing the latest technology. One failure to treat confidential customer information with adequate respect can have lasting consequences.
- Auditors should assess a company's internal practices and the possibility of unintentional disclosures of PII. Responsible leaders will examine carefully their internal and external policies with respect to handling, storing and using PII, no matter what the source.
- Web site privacy policies should state clearly whether they apply only to data collected online. If a company treats information collected off-line differently from the way the company treats information collected online, the company should publicize the differences.
- When a company possesses important confidential information about its customers, there is little room for error in handling that data.
- A company needs a responsible person with authority to oversee PII-related policies and practices.
- Companies must establish secure, practical, foolproof procedures for collecting, managing, storing and handling PII.
- Employees (both new and old) with access to PII must receive training to alert them to the risks inherent in PII and to follow the employer's practices and procedures relating to PII.
- Supervisors must monitor employees to ensure that they follow established practices and procedures for dealing with PII.

---

[1] "Administration to Stay on Sidelines of Privacy Debate Now, Official Says," February 1, 2002 edition of *Pike & Fischer Internet Law and Regulation*.

- Finally, responsible individuals must revise a company's practices and procedures on a regular basis to match the company's changing needs, new technologies, changes in personal information laws and practices in the marketplace generally.

Anything less risks being called to task for unfair and deceptive practices.

Elaine M. Laflamme is a partner and is head of the transactional intellectual property/information technology practice in the New York office of Akin, Gump, Strauss, Hauer & Feld, L.L.P.; **Noel D. Humphreys** and **Michael B. Kupin** are senior counsel in the corporate and technology practice groups in Akin Gump's New York office. Ms. Laflamme works closely with technology and Internet companies in negotiating and drafting all forms of intellectual property, information technology and Internet-related agreements. Mr. Humphreys focuses on business combination transactions, including mergers; stock and asset purchases; joint ventures; and sales of electronic, pharmaceutical, technology, medical, office products, retail and other businesses. Mr. Kupin counsels early- and intermediate-stage Internet and new technology companies, represents application service providers and software development companies, and Internet-focused venture capital funds with regard to their formation and their investments in portfolio companies.