Legal Opinion Letter

WLF Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Vol. 15 No. 8 April 22, 2005

INFORMATION SECURITY STATEMENTS CAN BECOME LEGAL OBLIGATIONS

by
Holly K. Towle

Privacy policies are ubiquitous either because they are required by law or because businesses voluntarily provide them to meet or exceed consumer expectations. Companies may wish to review their policies and website statements to see if they include statements like the following:

> 1) "Your **information is secure**. At __.com our customers' data is strictly protected against any unauthorized access." 2) "**Payment Options**. Entering your credit card number via our secure server is completely safe. The server encrypts all of your information; no one except you can access it." 3) "**Is my personal information secure?** At __.com, protecting your information is our number one priority, and your personal data is strictly shielded from unauthorized access. Our '100% Safeguard Your Shopping Experience Guarantee' means you never have to worry about the safety of your credit card information. "

If those kinds of statements appear, the company may be at risk. The statements were the subject of a recent Federal Trade Commission action against Petco.com for unfair and deceptive practices because Petco's practices did not live up to its representations. The FTC's action, together with a new California statute and other developments, signal a significant shift in U.S. law that should be considered by all businesses.

What was Wrong with the Statements? The FTC alleged the express or, notably, "implied," representations made by Petco regarding information security were misleading. The FTC alleged that:

- The website was vulnerable to "commonly known or reasonably foreseeable" Structured Query Language injection database attacks. By using such attacks, hackers could gain access to tables containing personal information in clear readable text.

- Petco "created these vulnerabilities by failing to implement reasonable and appropriate measures to secure and protect databases that support or connect to the website;" and Petco failed to "adopt policies and procedures adequate to protect sensitive consumer information … or implement simple, readily available defenses to prevent…visitors from gaining access …."

- Petco said the personal information was maintained in encrypted format, but it was not. This can be a common overstatement made on sites using Secure Sockets Layer (SSL), a protocol for managing security of message transmissions. As stated by the FTC, SSL encrypts credit card information during certain transmissions, but not during storage. Once the information hit the Petco server, it was decrypted and maintained in readable text.

Holly K. Towle is a partner with Preston Gates Ellis LLP, a national law firm with strategic international locations. She chairs the firm's Electronics in Commerce group from her office in Seattle, Washington.

- Petco expressly or impliedly represented that it implemented reasonable and appropriate protection measures, when it in fact did not. It "failed to implement procedures that were reasonable and appropriate to: (1) detect reasonably foreseeable application vulnerabilities, and (2) prevent visitors from exploiting such vulnerabilities and obtaining unauthorized access to sensitive consumer information. Therefore, the representation was false or misleading."

To the extent Petco said one thing and did another, the FTC's action is not surprising. Its more notable aspect is that the FTC assumes a duty exists for companies to adopt reasonable security procedures. The basis for that is not yet clear in general law (as opposed to specific statutes), but it is abundantly clear that it is the FTC's view.

A New California Statute. As of September, 2004, a new California law, CA CIV. CODE § 1798.81.5 (2004), creates a general security requirement for personal information on state residents. Businesses controlling covered information must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The new law also impacts other parties. If the business discloses the information under a contract with a nonaffiliated third party, it must require *by contract* that the third party implement and maintain these security procedures. Generally, the new law does not cover entities already subject to greater requirements (e.g., under federal laws for financial institutions or health care providers), so its primary impact is to create a security obligation for all other businesses. If it withstands challenge, it will be the first federal or state law to impose such a general requirement.

Other Noteworthy Developments in the Information Security Arena:

- **Actions Against "Financial Institutions."** The FTC recently took enforcement action against two relatively small mortgage companies for violation of the federal Gramm-Leach-Bliley (GLB) Act. Although GLB only applies to "financial institutions," that term is broadly defined to include businesses not commonly viewed as "financial institutions," including insurance and investment and securities companies, as well as (per the FTC) "companies providing many other types of financial products and services to consumers. These institutions include, for example, payday lenders, check-cashing businesses, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, and retailers that issue credit cards to consumers." This is a broad group and the list is not complete.

- **Peer-to-Peer File Sharing**. The governor of California and the federal Office of Management and Budget issued directives concerning the use of peer-to-peer file-sharing technology (technology facilitating file sharing among computer users). Government officials and agencies must establish appropriate safeguards before allowing use on governmental computer systems. Forty-seven state attorneys general also sent a letter to peer-to-peer publishers, suggesting that those officials may view as an unfair or deceptive act against consumers a failure to make certain disclosures about the technology that can "invade their privacy and threaten their security."

- **Disposal of Individual Information**. Effective June 1, 2005, a new FTC rule requires businesses to take "reasonable measures to protect against unauthorized access to or use" of "consumer information" upon disposal. Other regulators are issuing parallel rules and all will apply in addition to GLB obligations. "Consumer information" is electronic or paper information about *individuals* if it *is* a consumer report (a.k.a. credit report), *or is derived from* one. According to FTC staff, "derived from" covers the waterfront, including information *taken from* a consumer report or resulting from its *manipulation* or *combination* with *other* information. "Disposal" includes both discarding the information and/or disposing of (or selling or donating) any *medium* on which it is stored (such as a computer or personal data assistant). A wide universe of businesses is impacted by this new rule.

There are many other rules relating to information security and many require adoption of written policies and procedures, implementation and monitoring. It is important for businesses holding covered information to respond appropriately.

  ISBN 1056 3059