SEPTEMBER 2010

Privacy Law Alert

from the Privacy & Information Security Group of Poyner Spruill LLP

Your Website Privacy Notice: A Publicly Available, Legally Enforceable Promise – Understand the Risk of Overpromising and Underdelivering

by Kevin Ceglowski

The Federal Trade Commission (FTC) has taken a number of enforcement actions alleging that seemingly innocuous statements in privacy notices were "deceptive." In particular, companies that post privacy notices online where the FTC can easily access and analyze them have been subject to enforcement actions when those notices are deemed deficient. If your organization posts a privacy notice online (as it is likely required by law to do), you should be aware of the risks and take steps to prevent FTC scrutiny.

One recent enforcement action against Twitter highlighted a statement in the privacy notice saying, "Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access." The FTC alleged that statement was deceptive. Many websites say something similar. So what was the problem here?

The problem was that Twitter failed to implement a "reasonable" security program to back up its seemingly innocuous privacy promise, suffered a breach that made headlines, and thus attracted the FTC's attention. In keeping with the agency's past enforcement actions, it went straight to the website to see what kind of privacy promises the company made to users. The FTC took issue with Twitter's failure to keep its system secure when contrasted with the company's public statement of concern for users' privacy and charged it with a violation of the FTC Act.

Past FTC enforcement has tended to focus on overly broad and unrealistic promises (e.g., "We will never disclose your personal information to a third party without your consent."). Such promises, while well-meaning, are impossible to enforce in the current landscape where multiple third parties, ranging from authorized service providers to unauthorized hackers, might access data.

Other problems besides government enforcement actions can also be created by broad privacy promises. A series of bankruptcy cases has created precedent that customer lists may not be sold if that disclosure would be contrary to statements made in consumer privacy notices.

Reading this, you may be tempted to simply take down your website's privacy notice. Don't. There are several laws that may require you to provide a privacy notice, and even if the law does not require online posting (some do), posting online remains an easy and inexpensive way to disseminate the notice. A nonexclusive list of laws that may require a privacy notice includes the Children's Online Privacy Protection Act, the California Online Privacy Protection Act, the Gramm-Leach-Bliley Act, HIPAA, the Fair Credit Reporting Act, state laws governing SSNs, and a slew of international laws. The variety of potentially applicable laws creates a myriad of requirements that can be difficult to navigate and reconcile. Couple that with case law and the pattern of FTC enforcement, and you've got a quagmire of legal compliance and risk issues that, if not properly addressed, end up publicly posted on your website, easily available for a regulator's review.

The attorneys of Poyner Spruill's Privacy and Information Security Practice can navigate the relevant legal requirements for you to help your organization ensure that its privacy notices meet your compliance objectives without creating unnecessary risks.

Kevin Ceglowski may be reached at 919.783.2853 or kceglowski@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW