InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
August 13, 2013
IP

INTELLECTUAL PROPERTY

5 ways to reduce the risk of privacy breach claims

Recent court decisions and government actions should make companies take a long, hard look at how they handle personal information

KAREN BROMBERG

The increasing number of Federal Trade Commission (FTC) enforcement actions in recent years against high-profile companies like Google, Facebook and Twitter for alleged privacy breaches — and the penalties imposed by the FTC, including 20 years of FTC supervision and a record $22.5 million civil penalty against Google — should make companies take a long, hard look at their privacy policies and how they handle their consumers' personal information.

But the courts have recently provided another reason to be concerned. In one of the largest privacy class action suits ever filed, the 7th Circuit in Harris v. comScore allowed a class action to proceed against an online data research company for alleged violations of federal privacy statutes, including the Stored Communications Act (SCA) and the Electronic Communications Privacy Act (ECPA). At the heart of the complaint was the plaintiff's claim that comScore's software collected more personal information about its users than was disclosed in the company's terms of service and that the company secretly sold this information to third parties, who in turn used the data for marketing research.

The holding in comScore may signal a change in this area of the law: Until recently, courts have generally found that putative class members lack standing to pursue class actions where there is no evidence of actual harm, and therefore plaintiffs had difficulty in surviving motions to dismiss in privacy breach cases. In comScore, however, the court rejected the research company's argument that the class was unmanageable because each plaintiff had to prove actual damages. The court instead held that the damages claimed were statutory in nature and thus easily ascertainable in a class proceeding, with no need for individual showings of injury. The SCA, for example, provides a minimum statutory fine of $1,000 for a violation, while the ECPA provides a statutory penalty range of $50 to $10,000.

With the stakes so high, companies should, at a minimum, take the following steps to limit the potential risk for privacy breach claims.

1. First and foremost, say what you do, and do what you say. Most FTC enforcement actions and civil privacy cases arise from a company's violation of its own privacy policy. There is no such thing as a privacy policy template. Privacy policies must be thoughtful and must accurately and clearly describe how a company uses the consumer's personal information.
2. Monitor all representations made by or on behalf of your company about its privacy policies, and periodically compare these promises to what is done in practice. If the promises change, your policy needs to change. And if the change is material, it cannot be made retroactively unless consumers expressly opt in to the change.
3. Educate your information technology, information security, marketing, HR and sales teams about the terms of your company's privacy policy and require senior management approval for any proposed changes to, or deviations from, the policy.
4. Ensure that your company abides by all of its privacy promises and establish stated consequences for failure to comply.
5. Collect only personal information that is reasonably necessary for your business to provide goods or services to the consumer, and don't retain personal information beyond what is reasonably necessary to complete a transaction or provide a service.
6. Make your privacy policy easy to read and provide access to this policy on every single page of your website.

Until Congress implements general privacy legislation, it will remain challenging to strike the right balance in drafting a privacy policy. That said, the FTC has issued guidelines that companies should consider when drafting a privacy policy and deciding what safeguards to implement. The

FTC's recent report entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers" outlines what the agency believes to be best practices for companies to protect consumer privacy and give consumers greater control over the collection and use of their personal data. This includes building in privacy protections at every stage of product/service development, simplifying consumer choice regarding information sharing, including do-not-track mechanisms, ensuring greater transparency, and disclosing details about the collection and use of consumers' information. The FTC has also issued privacy guidelines specifically for mobile use. At a minimum, it would be wise for companies to consult these and future FTC guidelines and work closely with counsel in crafting a sensible policy with which the company can and will comply.

Karen H. Bromberg is a partner with Cohen & Gresser LLP and heads its intellectual property and technology group.

Counsel Commentary is a column published by InsideCounsel.com. Updated daily, it features commentary on and analysis of legal issue affecting in-house counsel. Written by senior level law firm lawyers, the columns cover various fields of law including labor & employment, IP, litigation and technology.