Shook, Hardy & Bacon L.L.P.

NOVEMBER 21, 2013

DATA SECURITY ALERT

WHAT'S THE NEXT WAVE OF PRIVACY LITIGATION? "FAILURE TO MATCH"

A client recently asked me to identify the next wave of data privacy litigation. I said that with so much attention on lawsuits arising from data breaches, particularly in light of some recent successes for the plaintiffs in those lawsuits, the way in which companies collect information and disclose what they are collecting is flying under the radar. This "failure to match" what is *actually* being collected with what companies are *saying* they're collecting and doing with that information *could* lead to the next wave of data privacy class action litigation.

Here's an example. A privacy policy in a mobile app might state that the app collects the user's name, mailing address, and purchasing behavior. In fact, and often unbeknownst to the person who drafted the privacy policy, the app is also collecting information like the user's geolocation and mobile device identification number, but that collection is not disclosed to the user in the privacy policy. The *collection* of the additional information isn't what gets the company into trouble. It's the failure to fully and accurately *disclose* the collection practice and how that information is used and disclosed to others that creates the legal risk.

What is the source of this problem? In an effort to minimize costs, small companies often slap together a privacy policy by cutting-and-pasting from a form provided by a website designer or found on the Internet. Little care is given to the accuracy and depth of the policy because there is little awareness of the potential risk. Larger companies face a different problem: the left hand sometimes doesn't know what the right hand is doing. Legal, privacy, and compliance departments often do not ask the right questions of IT, web/app developers, and marketing, and the latter may not do a sufficiently good job of volunteering more than what is asked of them. This problem is can be further exacerbated where the app/website development and maintenance is outsourced. This failure to communicate can, unintentionally, result in a "failure to match" a company's words with its actions when it comes to information collection.

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

SHB guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy services, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

We have already seen state and federal regulators become active in this area. The Federal Trade Commission has brought a significant number of enforcement actions against organizations seeking to make sure that companies live up to the promises they make to consumers about how they collect and use their information. Similarly, the Office of the California Attorney General recently brought a lawsuit against Delta Air Lines alleging a violation of California's Online Privacy Protection Act for failure to provide a reasonably accessible privacy policy in its mobile app. Additionally, the California Attorney General's Office has issued a guidance on how mobile apps can better protect consumer privacy, which includes the conspicuous placement and fulsome disclosure of information collection, sharing, and disclosure practices. As the use of mobile apps and collection of electronic information about consumers increase, we can expect to see a ramping up of these enforcement actions.

What sort of civil class action liability could companies face for "failure to match"? Based on what we've seen in privacy and security litigation thus far, if the failure to match a policy with a practice is intentional or reckless, companies could face exposure under theories of fraud or deceptive trade practice statutes that provide a private right of action (e.g., state "Little FTC Acts"). Even if the failure to disclose is unintentional, the company could still face a lawsuit alleging negligent misrepresentation, breach of contract, and statutory violations that include violations of Gramm Leach Bliley, HIPAA's privacy rule, or California's Online Privacy Protection Act. Without weighing in on the merits of these lawsuits, I would venture to guess that the class actions that will have the greatest chances of success will be those where the plaintiffs can show some financial harm (e.g., they paid for the apps in which the deficient privacy policy was contained) or there is a statute that provides set monetary relief as damages (e.g., $1,000 per violation/download).

What can companies do to minimize this risk? To minimize the risks, companies should begin by evaluating whether their privacy policies match their collection, use, and sharing practices. This process starts with the formation of a task force under the direction of counsel that is comprised of representatives from legal, compliance, IT, and marketing and that is dedicated to identifying: (1) all company statements about what information is collected (on company websites, in mobile apps, in written documents, etc.); (2) what information is *actually* being collected by the company's website, mobile app, and other information collection processes; and (3) how the information is being used and shared. The second part requires a really deep dive, perhaps even an independent forensic analysis, to ensure that the company's statements about what information is being collected are correct. It's important that the "tech guys" (the individuals responsible for developing the app/website) understand the significance of full disclosure. Companies should

also ask, "do we really need everything we're collecting?" If not, why are you taking on the additional risk? Also remember that this is not a static process. Companies should regularly evaluate their privacy policies and monitor the information they collect. A system must be in place to quickly identify when these collection, use, and sharing practices change, so the policies can be updated promptly where necessary.

For more information about these and other issues relating to data security law, visit Al's blog at **www.datasecuritylawjournal.com**.

OFFICE LOCATIONS

Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
Philadelphia, Pennsylvania
+1-215-278-2555
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400