News and Publications

Social Media and Online Advertising: What You Keep and Don't Disclose Can Hurt You

August 15, 2011

By John R. Gotaskie, Jr., Fox Rothschild LLP

Recently, the blogosphere has been all "atwitter" regarding the fact that, unbeknownst to the consumer, Apple Computer has been capturing location data from iPhones and iPads — meaning, if your employees and customers have these devices, Apple knows precisely where they have been. The captured location data is stored on an iPhone or iPad for up to one year and is uploaded to Apple's servers every time a user syncs the device with iTunes.

Apple has come under considerable criti cism for this practice both in the media as well as in Congress. It has become something of an embarrassment for Apple, which is considered one of the leading online technology companies. So what went wrong? And what are the lessons for in-house counsel and their companies? Have you taken every reasonable step to protect your organization with regard to online data tracking and collection activi ties? If not, the risks of having incomplete policies and noncompliant practices could be substantial, including a loss of con sumer confidence in your brand, investi gations from state and federal authorities — including Congressional subpoenas, one of the broadest possible law enforce ment tools — and lawsuits from those aggrieved. Sony, for example, recently was forced to shut down its Play Station online gaming network for several weeks and respond to inquires from Congress after

its security systems, including those that retain sensitive customer data collected online, were breached.

For Apple, the essential issue is that it was capturing and storing data from users' devices without receiving prior consent or at a minimum, informing users of the practice. In today's online advertising and social media world, consumers are often willing to allow the capture and use of location information *if* the data collection efforts and how such data will be used are disclosed. In this instance, Apple failed its customers on both counts.

Perhaps because many of Apple's users expect location information will be used to enhance their online experience, most consumers do not seem to be as both ered as one might expect from this "Big Brother" experience. For example, social apps such as Twitter, Foursquare, Living Social and Groupon all use the location features of Apple's PDAs to provide a richer consumer experience.

The larger issue, however, is what happens with such stored personal information once it is available in the public sphere. Within the last month, Google, Sony and Apple have all come under fire for the capture, and occasional disclosure, of sen sitive personal information. These events may provide impetus for the Federal Trade Commission's efforts to regulate online advertising and for Congress to consider additional laws.

In 2009, the FTC issued its "Principles for Online Behavioral Advertising," a practice it distinguished from "First Party Behavioral Advertising" and "Contextual Advertising." First-Party Behavioral Advertising is conducted by an entity and at a single web site (e.g., a banner or pop-up advertisement seen by an indi vidual consumer at a particular web site). Because this advertising does not involve tracking, the FTC concluded it is likely to be consistent with consumer expectations and thus less likely than Online Behavioral Advertising to lead to consumer harm.

Contextual Advertising is based on a consumer's visit to a single web page or in response to a single search query that involves no retention of data about the consumer's online activities other than those necessary for the immediate delivery of an advertisement. Think of the paid links at the top of a Google search results page. Because of its limited con cerns regarding consumer tracking from Contextual Advertising, the FTC con cluded its principles did not need to cover contextual advertising.

The FTC's principles for Online Behavioral Advertising, published in 2009, were a result of work the FTC began in 1995 when the Internet was in its infancy. It involved a number of interim reports and studies, a two-day town hall meeting in November 2007 and comments from 63 different stakeholders, including com panies, business advocacy groups such as the Chamber of Commerce, academ ics, consumer and privacy advocates and individual consumers. From the meetings and discussions coordinated by the FTC, four principles emerged: (1) transpar ency and consumer control; (2) reason able security and limited data retention for consumer data; (3) affirmative express consent for material changes to exist ing privacy promises; and (4) affirmative express consent to using sensitive data for behavioral advertising. The main points involve transparency — that is, ensuring the consumer understands to what he or she agreed with regard to any tracking of web or other online activities through apps or other tools — along with affirmative express consent — meaning the FTC wants consumers to be able to "opt-in" to track ing services.

The advertising, Internet and computer industries have taken a slightly different approach. In response to the publication of the FTC principles, a cadre of five differ ent industry groups issued its own set of seven self-regulatory principles for Online Behavioral Advertising: (1) education; (2) transparency; (3) consumer control; (4) data security; (5) notice of material changes; (6) sensitive data protection; and (7) accountability. The most significant difference between the FTC and industry approaches is that the third and fourth FTC principles, affirmative consent, are notably absent from the industry regime. The industry

regime, in other words, con templates full disclosure just as the FTC does, but wants consumers to “opt-out” from rather than “opt-in” to tracking.

So what does this mean for you? The FTC is continuing to closely monitor online tracking and data retention activities, including traditional web-based advertis"ing and searching as well as apps and the activities that companies such as Apple, Google and Foursquare are doing with location-based services. Additionally, especially in light of the Apple and Google experiences in the last several months, both Houses of Congress have announced committee investigations and will hold hearings regarding online privacy con"cerns this summer. Given this challenging regulatory and possibly changing legal environment, along with the coming presi"dential and congressional election cycle, companies need to be especially cautious.

The single most important thing compa"nies can do today is review their online data tracking and retention policies to ensure they are fully disclosing *all* types of data they are collecting, telling consumers what they are doing with such data and ensuring the data is protected as care"fully as possible. While this seems like common sense, the recent experiences of Sony and Apple demonstrate how damag"ing this situation can be for companies and how they can leave fertile ground for laws and regulations that further suppress innovation.

John R. Gotaskie, Jr., is a partner and litiga tor with Fox Rothschild LLP, and is based in the firm’s Pittsburgh office. He may be reached at jgotaskie@foxrothschild.com.