CLIENT ALERT

Fierce in February: FTC & Mobile Privacy—Making the Most of the Shortest Month

Mar.11.2013

Although it is March that traditionally "comes in like a lion," the Federal Trade Commission has roared through February—especially when it comes to the issue of consumer privacy in the mobile arena.

The month started off with a one-two punch: First, on February 1, the FTC released its staff report on mobile privacy titled, "*Mobile Privacy Disclosures: Building Trust Through Transparency*," which focuses on the need for "just-in-time" disclosures and the benefits of "Do Not Track" software, consumer education, short-form disclosures, and standardized privacy policies on mobile devices.

Second, on that same day, the Commission also announced a settlement with Path Social Networking App, a mobile app which, the FTC charged, deceived users by collecting personal information from mobile devices without users' knowledge and consent. The settlement included a requirement that Path establish a comprehensive privacy program, obtain independent privacy assessments every other year until 2033, and pay $800,000 to settle charges that it illegally collected children's personal information without parental consent.

As February rolled on, the FTC continued to demonstrate a focus on mobile privacy and security. On February 4, the FTC issued another publication, "*Mobile App Developers: Start with Security,*" a guide for developers of mobile apps that highlights the importance of data security and protecting consumer information. And then, last week, the FTC announced a settlement with smartphone manufacturer HTC regarding security flaws that the FTC alleged could compromise the privacy of sensitive consumer information. The charges against HTC include claims that HTC failed to provide its engineers with adequate security training, failed to review and test software for potential security vulnerabilities, and failed to establish a process for receiving, reviewing and addressing reports of security flaws.

The impact of these failures, according to the FTC, is that millions of HTC devices had compromised security and were vulnerable to "malware" applications that could send text messages, record audio, and install additional programs without the user's knowledge or consent. This meant that financial, medical, and geolocation information, as well as the content of users' text messages, was potentially available to third-parties.

In a first-of-its-kind settlement, HTC is required to develop and release software patches to fix weaknesses in millions of HTC smartphones. In addition to the patches, the FTC has applied some traditional remedies, including requiring HTC to create a comprehensive security program to address security risks during the development of future devices and to submit to independent security assessments every other years for 20 years.

The FTC's attention to HTC, one of the leading mobile device manufacturers—and to the mobile arena in general—is hardly surprising. The Commission has noted that there has been an "explosive growth of mobile services," citing to the fact that, in the fourth quarter of 2012, consumers worldwide bought approximately 217 million smartphones.[1] And the FTC's concern with mobile devices isn't just because mobile is booming; the FTC believes that mobile devices "rais[e] unique privacy concerns" by

virtue of the fact that they are personal to an individual, almost always on, and usually close at hand—or, rather, *in* hand.[2] In addition, the FTC, as "the nation's chief privacy agency" believes that it is addressing consumer concerns: the Commission notes that less than one-third of Americans feel they are in control of their personal information on their mobile devices. [3]

So, how can businesses avoid the hungry stare of the FTC? First, all manufacturers—not just those making mobile devices or apps—should be sure to take consumer privacy seriously by implementing "privacy by design," that is, taking a methodical approach to address privacy issues for the any collection, use, sharing, and destruction of consumer information. The FTC has been clear: privacy should not be an afterthought, it should be built into every element of the product being offered.

Further, companies need to be aware that the responsibility doesn't end once the product leaves the shelf. As we've seen in the HTC settlement, the FTC expects that companies will continually update their products and services to make sure that, as new threats emerge or weaknesses become apparent, the manufacturer will take affirmative steps to follow up and fix problems.

What's more, companies also need to show that they are keeping their eyes and ears open to feedback from the public regarding problems. The FTC cited HTC's lack of proper procedures for reviewing and addressing customer feedback. In order to avoid the same fate, companies need to have mechanisms to track and monitor consumer feedback and not ignore the "wisdom of the crowds."

Finally, companies should be careful when adapting or modifying other companies' software or products into their own. HTC was cited by the FTC for making changes to the Android operating system and bypassing the well-established and secure approaches for their own, less safe, techniques. In the end, if you are making changes, be careful to avoid introducing *new* security threats.

If you haven't already, now is the time for companies to start thinking proactively about ensuring that new products and services are designed with privacy in mind, that current products and services are continually reviewed for weaknesses, and that there are regular, ongoing processes in place for doing both. Proactively addressing these issues can help avoid problems down the road. It is safe to say that, as companies continue to innovate and harness the seemingly limitless functionality of personal mobile devices and consumers keep buying smartphones, mobile apps, and services, the FTC will be keeping its eye on consumer data and privacy on mobile devices. In other words, even though February won't last forever, it is unlikely that the FTC's attention to mobile devices, apps, and data privacy will "go out like a lamb" anytime soon.

---

[1] Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures, February 1, 2013, http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm.

[2] *Id*.

[3] *Id*.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.