Senate Hearing on Mobile Device Location Tracking Highlights Ongoing Concerns Over Consumer Privacy Protections

Dana B. Rosenfeld, Alysa Z. Hutnik

May 11, 2011

Introduction

On May 10, 2011, the U.S. Senate Judiciary Subcommittee on Privacy, Technology and the Law held a hearing to examine industry practices concerning the collection, retention, and use of consumer mobile device location information. The hearing, "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy," was spurred by recent investigative news reports that Apple and Google have been secretly collecting and storing users' mobile device location information. Two panels of witnesses, including representatives from government and industry sectors, briefed subcommittee members on the legal, enforcement, and technological aspects of the mobile location data issue.

Subcommittee members attending the hearing included Sen. Al Franken (D-MN), Sen. Sheldon Whitehouse (D-RI), Sen. Tom Coburn (R-OK), Sen. Richard Blumenthal (D-CT), Sen. Charles Schumer (D-NY), and Sen. Patrick Leahy (D-VT). Subcommittee Chairman Sen. Franken noted at the outset of the hearing that consumer sentiment toward privacy has shifted in the past decade from concerns mainly over government access to personal information to the actions of private entities that collect, store, share, and/or sell personal data. Sen. Franken called consumer awareness about the collection and use of their personal information a "fundamental right."
The subcommittee members pointedly acknowledged the benefits that come with mobile location information, but also highlighted risks to personal safety that can result when such information is in the wrong hands. As such, Sen. Franken framed the goal of the hearing as a step toward finding "a balance between the wonderful benefits and the public's right to privacy."

A summary of the two panel sessions is set forth below.

Panel 1: Perspectives from the FTC and Department of Justice

The first panel of witnesses included Jessica Rich, Deputy Director of the Bureau of Consumer Protection at the FTC, and Jason Weinstein, Deputy Assistant Attorney General in the Criminal Division of the Department of Justice.

In her initial remarks, Jessica Rich categorized personal location information on par with sensitive information, such as medical and financial information, and information about children. She called for

more stringent consumer consent requirements, noting the "always on" and personal nature of mobile devices and the resulting potential for "real consequences" when the data generated by these devices is misused. She further stated that recent events, including the Epsilon Interactive data breach, have highlighted the extent to which most Americans are unaware of the layers of information-sharing and the chain of entities that have access to personal information. Ms. Rich acknowledged consumer awareness challenges inherent with mobile devices, including the small screen size. In response, she said that the FTC is strongly advocating disclosures that are "embedded in the interaction" so that consumers are made aware of the information collection as it is requested.

When asked for the Commission's views on consumer privacy legislation, Ms. Rich applied the concepts in the FTC's privacy framework to the mobile application ("app") space. For example, she detailed how the privacy by design principle, in which privacy considerations are factored in at the initial stages of product development, can help to limit the collection of personal location information that is outside the scope of an app developer's business model. Further, the principle of streamlined choice can be applied to mobile devices by requiring or simplifying access to privacy policies through the use of icons or other means. Ms. Rich also advised that companies can provide greater transparency by providing consumers with reasonable access to the data that companies maintain on them. As for specific legislative provisions, she noted the Commission's preference for federal data breach notification requirements, as well as data security legislation that includes civil penalties.

Lastly, Ms. Rich stated that the FTC is not seeking perfection in the data security space and will continue to rely on the reasonableness standard. She advised businesses to employ reasonable security and good processes, and to limit information collection to no more than is necessary.

Mr. Weinstein discussed Justice Department priorities with respect to mobile data, which include addressing threats posed by cyber-stalkers, and identifying thieves and hackers. He discussed the current lack of legal restrictions on the sharing of personal information without consent. He further noted that in the absence of universal data security standards, companies are left to formulate their own best practices based on their own assessment of risk. He concurred with comments by Ms. Rich that the public remains under-informed as to mobile data collection practices and, in the absence of a perfect security solution, consumer vigilance must be part of a multi-pronged approach.

Panel 2: Industry Response to Location Information Concerns

The second panel of witnesses consisted of industry representatives and consumer advocates, and included executives from Apple, Google, and the Association for Competitive Technologies, in addition to a representative from the Center for Democracy and Technology and an independent privacy technologist.

Bud Tribble, Vice President of Software Technology at Apple, responded to reports on Apple's location information practices by stating emphatically that Apple has never tracked its users' locations, and provides customers with full control over their location-based services. He noted, for example, that Apple requires express customer consent when an app initially requests location-based information. While acknowledging reports that Apple permitted location information to be collected even after users deactivated their devices' location feature, Mr. Tribble stated that the issue has since been resolved.

Mr. Tribble responded to querying from subcommittee members on why Apple doesn't require all

apps to include a privacy policy by stating that Apple already employs the privacy-by-design framework championed by the FTC. For example, he described Apple's process by which it contractually requires third-party apps to include clear notice on the consumer information they intend to collect. He also described the app review and approval process, and continuous interaction with Apple's community of app users. To enforce its terms of use, Apple relies on random audits of the 350,000 apps in its app store, coupled with network traffic monitoring to identify deviations from accepted policies.

Alan Davidson, Director of Public Policy for the Americas at Google, explained how Google, like Apple, has adopted the FTC's privacy by design framework with respect to mobile apps. He emphasized that Google's Android mobile location services are opt-in only, and that information on app location-tracking is clearly disclosed in plain language at the outset of the app download process. If a user opts to share his personal information, the data is anonymized, and the user retains the ability to deny access at any time.

Mr. Davidson affirmed Google's support for comprehensive privacy legislation and federal data breach notification requirements. Like Apple, Google would not commit during the hearing to a requirement that apps include privacy policies. Instead, Mr. Davidson said that Google attempts to keep its platform "as open as possible" and relies on the device to tell the user what the app intends to do. Responding to Sen. Whitehouse's comment that "as open as possible" is not a good standard, Mr. Davidson noted that Google seeks a balance between innovation and privacy and that Google's approach is not "open at all costs."

The consumer advocate perspective was provided by Justin Brookman, with the Center for Democracy and Technology, who noted that entities who collect mobile location information keep their privacy policies intentionally vague because a policy with clear and concrete statements of responsibility provides the easiest path to liability. Ashkan Soltani, a privacy technologist, described Google's StreetView wi-fi issues and Apple's inadvertent collection of mobile location data as prime examples that even the largest technology companies are finding themselves as surprised as consumers as to the scope of the personal information that is being collected.

Current and Pending Privacy Legislation

The Senate hearing is the latest event during a particularly active period for consumer privacy and data security-related Congressional activity. On May 4, 2011, a House Commerce Subcommittee held a hearing in response to the recent data breaches announced by Epsilon Interactive and Sony that affected more than 100 million consumers. During the hearing, Rep. Mary Bono Mack (R-CA) stated her intention to introduce federal data breach notification legislation.

New bills responding to consumer privacy and data security concerns continue to be introduced. On May 11, 2011, Sen. Jay Rockefeller (D-WV) introduced the Do Not Track Online Act of 2011, which would prohibit online providers from tracking consumer online activities, including online mobile activities, without express consent. On May 4th, 2011, Rep. Bobby Rush (D-IL) introduced the Data Accountability and Trust Act (H.R. 1707), which would require companies to implement data security policies to protect personal information and would impose data breach notification requirements. These bill are the most recent in a growing list of consumer privacy and data security legislation introduced during the current session of Congress. The chart accompanying this advisory offers a helpful snapshot of the key provisions within both the introduced legislation and pending legislation.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

Kelley Drye's Government Relations and Public Policy Practice Group helps clients interpret and shape governing laws, enabling them to achieve and maintain market leadership. The varied backgrounds of its government relations lawyers and professionals enable the team to handle a variety of clients needs including representation and strategic planning.

For more information about this advisory, contact:

Dana B. Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

Alysa Zeltzer Hutnik
(202) 342-8603
ahutnik@kelleydrye.com