Client Alert

pillsbury

Antitrust & Competition | Litigation
Social Media & Games | Consumer & Retail
Communications | Privacy, Data Security & Information Use

March 31, 2014

FTC Expands Focus on Tracking and Use of Consumers' Location Data

In-store monitoring of shoppers' mobile devices under scrutiny.

By Roxane A. Polidora, Catherine D. Meyer, Lindsay A. Lutz and Kristen E. Baker

Over the past few years, the Federal Trade Commission ("FTC") has provided guidance regarding mobile platforms and app providers' practices of collecting data about consumers' locations through their mobile devices, with a focus on transparency and notice to consumers. The FTC recently hosted a spring seminar on emerging consumer privacy issues that focused on a new type of mobile device tracking: brick-and-mortar businesses tracking consumer movements in or around their premises using signals from the consumer's mobile device.

FTC Guidance on Location Data Tracking Disclosures

In March 2012, the FTC published its report, *Protecting Consumer Privacy in an Era of Rapid Change*. The report contained a case study on data collection for mobile phones and noted that the unique features of a mobile phone—users keep it on all the time and carry it with them wherever they go—facilitate "unprecedented levels" of data collection.[1] Particularly as to the collection of location data, the FTC called upon companies to disclose the frequency or extent of the collection, transfer, and use of location data and to give consumers more prominent notice and choices about the sharing of location data with third parties.

In February 2013, the FTC again weighed in on this issue through its report, *Mobile Privacy Disclosures: Building Trust Through Transparency*. As to mobile apps, the FTC stated that if an "app developer decides to share that geolocation data with a third party, the app developer should provide a just-in-time disclosure and obtain affirmative consent from users for that data sharing."[2] The FTC guidance focused on how transparency in disclosures allows consumers to give informed consent regarding the collection of their

[1] *Protecting Consumer Privacy*, p. 33.
[2] *Mobile Privacy Disclosures,* p. 24.

data, how their data is used, and the types of third parties, such as advertisers and analytics firms, with whom their data is shared.

The FTC demonstrated its willingness to file complaints against companies that do not provide adequate disclosures about the collection of location data in its case against Goldenshores Technologies, LLC, the company that developed the popular "Brightest Flashlight" app. The FTC filed an administrative complaint against Goldenshores pursuant to its authority to enforce Section 5(a) of the FTC Act, which declares "unfair or deceptive acts or practices in or affecting commerce" to be illegal. 15 U.S.C. Sec. 45(a)(1)). The FTC's complaint alleged that the Brightest Flashlight app collected a "device's precise geolocation along with persistent device identifiers that can be used to track a user's location over time" and transmitted that data to third parties including advertising networks without adequately disclosing such practices to users.

Goldenshores entered into a consent order with the FTC in December 2013 that requires it to clearly and prominently disclose its practices regarding the collection and transmission of geolocation information, including the identity or categories of third parties that receive geolocation information from the app. The consent order also requires Goldenshores to obtain "affirmative express consent" from the consumers to transmit such information.[3] Key to the FTC's decision to institute a case against Goldenshores appears to have been the company's failure to disclose to customers how their location information would be used.

FTC Discusses Mobile Device Tracking Issues in Brick-and-Mortar Retailers at Spring Seminar

The FTC's spring seminar on mobile device tracking consisted of a technical presentation regarding how an individual's location may be tracked based on the signals emitted by his or her mobile device, as well as a panel discussion featuring representatives from privacy, retail, and data collection and analytics organizations, moderated by the FTC.[4]

Smartphones constantly send out signals, via various transmitting antennas – including Bluetooth, Wi-Fi, GPS, and GSM – and companies can intercept those signals, picking up the phone's globally unique identification number, known as a "MAC address," and its location, or approximate location. The FTC has noted that, in most cases, this tracking is invisible to consumers and occurs with no customer interaction.

Entities like airports, department stores, and shopping malls can track customer location information to better understand customer experiences. Data collected can provide information about pathing (i.e., how, in the aggregate, customers walk through a store), dwell time (including how many customers go in a particular department and how much time is spent there), wait time (including what days and times customers must wait in queues at registers for longer than the company's goal wait times), whether customers are stopping at registers at the end of their visit (i.e., whether customers are buying or "just looking"), and repeat customer visitation rates.

To date, the FTC guidance has broadly focused on disclosures to consumers regarding the collection by a mobile application of precise geolocation data of an individual mobile device, but the FTC has yet to issue guidance regarding its expectations about informing customers at brick-and-mortar businesses that their location data is being collected.

Based on the FTC's guidance to mobile app companies, providing disclosures to customers about the business' geolocation tracking practices through physical signs at store locations may be one method of

[3] Consent order, p. 4.

[4] PowerPoint materials and the transcript from the workshop are publicly available on the FTC's website at this link.

diminishing privacy concerns. For mobile apps the FTC has emphasized disclosure of the type of location data being collected and how it is being used prior to the collection of such data. How this functions in a brick-and-mortar context may be more complicated than in the mobile context, however. Unlike app just-in-time disclosures that inform a user of the collection of data immediately prior to collection, retailers may be tracking customers through Wi-Fi signals outside the four walls of a business—in other words, retailers may be tracking consumers before they reach a sign disclosing the tracking. Retailers may choose to limit the collection to only times when the consumer is within the store to limit such concerns. Immediately stripping geolocation data of persistent device identifiers and aggregating such data may also help lessen privacy concerns.

Retail industry analytics firms have already begun to respond to privacy concerns regarding such conduct by developing a Mobile Location Analytics Code of Conduct. The Code, released by the Future of Privacy Forum in October 2013, provides a framework for the collection and use of mobile location data by retailers. Analytics firms that adhere to the Code must take steps to strip the data of identifying information and ensure that their clients post signs to notify customers about the collection and use of such data. Such firms must also provide individuals with the ability to decline to have their mobile devices tracked.

While it is still unclear how the FTC will apply its previous guidance on mobile device tracking to brick-and-mortar retailers, the FTC's recent spring privacy seminar confirms that this is an emerging issue on the FTC's radar.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the attorneys below.

Roxane A. Polidora (bio)
San Francisco
+1.415.983.1976
roxane.polidora@pillsburylaw.com

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Lindsay A. Lutz (bio)
San Francisco
+1.415.983.1255
lindsay.lutz@pillsburylaw.com

Kristen E. Baker (bio)
Washington, DC
+1.202.663.8379
kristen.baker@pillsburylaw.com

Jim Gatto (bio)
Northern Virginia
+1.703.770.7754
james.gatto@pillsburylaw.com

Michael L. Sibarium (bio)
Washington, DC
+1.202.663.9202
michael.sibarium@pillsburylaw.com