WILMERHALE

Latest FTC Privacy Action Looks Carefully at Geolocation Promises

JUNE 23, 2016

A mobile device's geolocation can be passed to apps and ad networks through various application programming interfaces (APIs) provided by Android or iOS, but there are other ways to determine a consumer's location using information collected from a mobile device. Nevertheless, the Federal Trade Commission's latest privacy enforcement action suggests companies should be on notice to honor consumers' location privacy preferences and avoid tracking them without permission. In a complaint and order released on Wednesday, June 22, the FTC alleged that the mobile advertising company InMobi tracked the locations of millions of app users and served them geo-targeted advertising without their knowledge or consent in violation of both Section 5 of the FTC Act and the Children's Online Privacy Protection Act (COPPA).

InMobi provides an advertising platform to app developers using Android or iOS that allows them to sell advertising within their apps by integrating an InMobi software development kit (SDK). Advertisers can then target those app users through a variety of different geo-targeted advertising. This includes ads that are based on a user's current location, past location, or a combination of locations visited over time. Consumers generally choose to share their location information through individual app permissions or by toggling off location sharing on their iOS or Android devices.

Here, the issue for the FTC was that even where consumers had restricted access to their device's location API, InMobi could still track their location and serve them geo-targeted ads. The company allegedly accomplished this by collecting information about the Wi-Fi networks that a consumer's device either connected to or came within range of. On both Android and iOS devices, InMobi allegedly was able to collect network BSSIDs, which are unique identifiers, and other network information. This information was then sent to a geocoder database, which had mapped millions of Wi-Fi networks to their latitude and longitude, and thus, could be used to infer a device's precise location.

InMobi's Marketing Materials and Developer Guides Were Deceptive

According to the FTC's complaint, InMobi made representations to app developers that it tracked user location and served geo-targeted advertising "only if the application developer and the consumer had provided access" to various location APIs, even though the company continued to

collect location data and serve geo-targeted advertising based on Wi-Fi network information. As a result, the FTC alleged that the InMobi SDK integration guide contained representations that were false and misleading, constituting a deceptive act or practice under Section 5 of the FTC Act. The FTC also alleged that marketing materials that stated that InMobi takes "location data on each user, in the form of user opt-in lat/long signals" were deceptive under Section 5 because InMobi's collection of Wi-Fi data was not subject to opt-in consent.

It is worth highlighting that these materials were not directed toward consumers. Instead, this enforcement action highlights that companies can be held liable under Section 5 for potentially misleading statements that are made to other businesses—especially when those representations affect consumers. FTC staff explains that InMobi's collection and use of Wi-Fi network information ultimately allowed the company to sidestep any given app developer's intentions with respect to advertising. As a result of InMobi's alleged deception, app developers were unable to provide their users with accurate information about their advertising practices, and consumers, in turn, lacked facts that would have been material to their decision to install apps using the InMobi SDK.

InMobi's Misrepresented Its Collection of Children's Data and Violated COPPA

The FTC also alleged that InMobi's made deceptive statements about its collection and use of personal information from child-directed applications in violation of Section 5, and that the company's failure to (1) provide sufficient notice on its website or platform of the information it collects from children and how it uses that information; (2) provide direct notice to parents about these practices; and (3) obtain verifiable parental consent were violations of the COPPA Rule.

First, InMobi has represented that it did not collect or use personal information from child-directed applications. However, the company provided an option during its registration process where app developers could indicate that their app was child-directed by checking a box next to the following language: "My property is specifically directed to children under 13 years of age and/or I have actual knowledge that it has users known to be under 13 years of age." Since that option was made available, thousands of app developers using the InMobi SDK had indicated their apps were directed toward children putting InMobi on notice.

Even as InMobi continued to collect and combine BSSIDs used to infer location with other unique device identifiers and other geolocation collected from children, the company provided a separate "COPPA Policy" that stated it did not collect or use information from applications directed to children. As a result, the FTC found that the company had failed either to implement adequate privacy controls to comply with COPPA or to test whether its controls were functioning as intended. Moreover, the FTC alleged that the company's failure to "clearly, completely, or accurately disclose" its information practices around children's data or to obtain parental consent were clear violations of the COPPA Rule.

FTC Imposes $4 Million Penalty and Compliance and Reporting Requirements

As a result of these alleged COPPA violations, InMobi agreed to a $4 million civil penalty (though this amount has been reduced to $950,000). The stipulated order also includes traditional compliance and reporting requirements, and InMobi will be required to implement a comprehensive privacy

program subject to independent audits every other year for the next 20 years.

Finally, the FTC's order provides some detail as to what the FTC considers location information. It defines location information to include more than just information derived from a device's location API, but also any information "that is inferred from any other data collected through an application programming interface, including but not limited to Basic Service Set Identifiers (BSSIDs), with the limited exception of Internet Protocol (IP) addresses used to infer location at no greater accuracy than city-level." In the future, InMobi will be required to obtain affirmative express consent before collecting any of this location information.