Updates
September 06, 2022
FTC Sues Data Broker for Alleged Unfair Act of Selling Precise Geolocation Data

The Federal Trade Commission (FTC) filed a lawsuit on August 29, 2022, against data broker Kochava Inc., alleging that the company's sale of precise geolocation data is an unfair act or practice that violates Section 5 of the FTC Act. The case follows an FTC blog post warning that the agency would be vigilant in protecting consumers' location and health information in the wake of *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022), as well as its recent Advanced Notice of Proposed Rulemaking focused on what it calls "commercial surveillance," which it defines to include practices in which Kochava engages—the "collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."

According to the complaint, Kochava allegedly sells, licenses, or "otherwise transfers" the "precise geolocation data" of consumers' mobile devices." Kochava provides this location data in customized data feeds to assist its customers with "advertising and analyzing foot traffic at stores or other locations." This location data allegedly includes "timestamped latitude and longitude coordinates" for a mobile device's location. Each pair of coordinates is tied to a unique identifier associated with a consumer's mobile device. One of Kochava's customized data feeds was allegedly available for free in an online data marketplace to any purchaser, whether business or individual. This free sample consisted of "a rolling seven-day period," with one day containing "over 61,803,400 unique mobile devices."

The FTC asserts that Kochava's data can be used to "track consumers to sensitive locations," such as abortion clinics, places of religious worship, places that may be used to infer LGBTQ+ identification, domestic abuse shelters, and addiction recovery centers. According to the FTC, the identification of consumers' sensitive and private characteristics from the location data sold and offered by Kochava threatens to "expose consumers to stigma, discrimination, physical violence, emotional distress, and other harms."

The FTC alleged that this location data was not anonymized because, for example, there were typically "multiple timestamped signals" associated with a unique identifier, which could be plotted to locations on a map, and

through which an individual's home address could be inferred and then matched to public or other records to identify the individual's name or identity. Moreover, the FTC asserts that Kochava lacked any "meaningful controls" over who accessed the location data, which was publicly available, including a free sample data feed.

The lawsuit is noteworthy for several reasons. First, the FTC does not allege that Kochava misled consumers or its clients, that any choice mechanisms did not work as described, or otherwise that the company acted in a deceptive manner, but rather simply that its practices are unfair, i.e., that they "cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). The complaint, however, does not identify any consumers who have actually been harmed by Kochava's practices and focuses on how the practices *could* lead to the revelation of sensitive locations. It is also notable that rather than being resolved through a consent order, as is typical for privacy and data security cases, this case went straight to litigation (with Kochava filing a separate declaratory judgment action against the FTC in advance of the FTC's filing, *Kochava Inc. v. FTC*, No. 2:22-cv-00349-BLW (D. Idaho Aug., 12, 2022)). This may reflect that the FTC, during possible pre-suit negotiations, not only advanced more aggressive legal theories than it has typically used in the past, but also sought more exacting settlement terms.

Finally, and perhaps most importantly, this action reflects the heightened scrutiny the FTC is bringing to bear on precise location data following the *Dobbs* decision. While the FTC for years has said that precise location data (even if, as in this case, there is no name or traditional identifier attached to it) is sensitive and deserving of enhanced protection, it has never brought a case alleging that selling such data is an unfair practice because it may reveal sensitive locations. Of course, many apps and services use precise location data and may disclose that data to others for valid purposes. At minimum, the complaint suggests the importance of having some safeguards and guardrails on who can access such data, as the complaint suggests that the wide availability of the location data sold by Kochava without such restrictions was key to the FTC's unfairness theory.

Takeaways

Businesses that collect and share precise geolocation information should consider whether they have adequate safeguards regarding access to such data, particularly to the extent it could reveal sensitive locations, such as reproductive and other healthcare facilities. It remains to be seen whether the complaint portends even more aggressive scrutiny of location data or whether the FTC would advance similar theories even for companies that do have such controls.

Authors

Explore more in

Privacy & Security | Technology Transactions & Privacy Law | Communications | Technology & Communications | Digital Media & Entertainment, Gaming & Sports

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law