Proskauer

Data At Issue: FTC Focus on Browsing Information and Location Data

New Media and Technology Law Blog on **March 25, 2024**

Since the start of the year, the Federal Trade Commission (FTC) has brought actions against – and reached proposed settlements with[1] – three business ventures engaged in the collection, use and sharing of certain consumer information.

- *In re X-Mode Social, Inc.*, FTC No. 2123038
- *In re InMarket Media, LLC*, FTC No. 2023088
- *In re Avast Limited*, FTC No. 2023033

Two of the actions involved the collection of location data and the third involved the collection of browsing-related information. These actions, as well as the FTC's ongoing *Kochava* litigation[2] and recent FTC blog posts and statements, suggest that location data and browsing information will be an ongoing FTC focus for the foreseeable future. This intention is clearly expressed in a recent FTC Business Blog post: "Browsing and location data are sensitive. Full Stop"… The Commission will use all of its tools to continue to protect Americans from abusive data practices and unlawful commercial surveillance." [3]

Below, we discuss key points of these enforcement actions and the proposed settlement orders (collectively, the "Orders"). A full discussion of all the details in the Orders would be too extensive for this blog post, but if this topic is relevant to your business, a thorough read of the actual Orders (and related materials)[4] is a must.

Locational Data – X-Mode and InMarket Enforcements

On January 9, 2024, the FTC announced the settlement and proposed consent order with X-Mode Social, Inc. and its successor Outlogic (collectively, "X-Mode") with respect to allegations that the company improperly collected and sold consumers' location data to third parties from various industries (including governmental contractors). (The FTC complaint and proposed consent order are referred to herein as the "X-Mode Complaint" and the "X-Mode Order" respectively.)

Shortly thereafter, on January 18, 2024, the FTC announced the settlement and proposed consent order with InMarket Media, LLC ("InMarket"), also over similar allegations that the company improperly collected and sold location data to third parties for advertising and marketing purposes. (The FTC complaint and proposed consent order are referred to herein as the "InMarket Complaint" and the "InMarket Order" respectively.)

The X-Mode Complaint alleged that X-Mode collected or purchased consumer location data from its own apps, third party apps and other sources and then sold that data to participants in various industries, as well as to private government contractors. According to the FTC, the data X-Mode sold was not anonymized and in fact was generally associated with mobile advertising IDs (MAIDs) such that the recipient of the data could match an individual consumer's mobile device with the exact locations they visited, including sensitive locations such as medical clinics and places of worship. The FTC claimed that X-Mode collected this data with misleading notices and failed to obtain informed consent about the purposes for which their location would be used. In addition, the X-Mode Complaint stated that X-Mode created a software development kit (an "SDK") to collect location data in third-party apps and that X-Mode failed to verify that third-party apps incorporating the SDK obtained informed consent about the location data collection and use.

The InMarket Complaint is similar in many respects to the X-Mode Complaint. Here again, the FTC alleged that location data was collected and purchased from mobile devices via an SDK and from other sources, all without appropriate notice and consent. The FTC alleged that InMarket collected information including locations and movements to and from homes and work and to other sensitive locations, along with several identifiers (including a unique mobile device identifier). The FTC alleged that InMarket subsequently matched that information with other specific details such as users' purchasing histories and demographics to create consumer profiles and offer geofenced ads. The FTC claimed that InMarket failed to notify consumers that their location data would be used for targeted advertising and failed to verify whether the hundreds of third party apps incorporating InMarket's SDK obtained informed consumer consent about the location data collection and use.

Sensitive Locations

Both the X-Mode and InMarket Orders contain restrictive provisions related to "Sensitive Locations" (i.e., various locations that the FTC considers to be of a personal nature) and "Sensitive Location Data" (i.e., locational data associated with Sensitive Locations). However, there is a difference in the way each of the respective Orders define the term "Sensitive Locations." The X-Mode Order's definition, for example, is broader than the definition in the InMarket Order with respect to health-related Sensitive Locations as it includes all "medical facilities" (but, within this category, it includes a long list of specific but non-exclusive types of medical facilities).[5] The InMarket Order definition of Sensitive Locations includes a lengthy – but specific – list of certain types of medical facilities. In addition, the InMarket Order's definition of "Sensitive Locations" includes categories of locations not included in the X-Mode Order's definition (e.g., "locations held out to the public as predominantly providing services to LGBTQ+ individuals" or "locations of public gatherings of individuals during political or social demonstrations, marches and protests").[6]

Remedies

The remedies included in both the X-Mode and InMarket Orders are extensive and not necessarily limited to issues related to Sensitive Location Data. And while many are common across both Orders, there are some differences.

For example, while the X-Mode Order prohibits (subject to certain exceptions) X-Mode from using Sensitive Location Data, the InMarket Order includes not only a similar prohibition on Sensitive Location Data, but also a prohibition on selling or licensing of "Location Data" "in exchange for any valuable consideration."[7]

Both Orders require the respondents going forward to obtain Affirmative Express Consent to the collection and use of location data. Affirmative Express Consent is defined in substantially the same way in both Orders and requires consent following "Clear and Conspicuous disclosure." The Clear and Conspicuous disclosure requirement ("Clear and Conspicuous" is defined in great detail in the Orders) must be "separate from any 'privacy policy,' 'terms of service,' 'terms of service' or other similar document" and not be subverted by an interface that employs dark patterns.

Another key point: both Orders require implementation of SDK Supplier Assessment Programs to ensure that consumers have provided Affirmative Express Consent for the collection and use of Location Data obtained from third party apps via an SDK. The Orders also mandate the implementation of Sensitive Location Data Programs overseen by senior officers.[8]

Browser Information – Avast Enforcement

On February 22, 2024, the FTC announced a $16.5 million settlement and proposed consent order with software provider Avast Limited and two subsidiaries including Jumpshot, Inc. (collectively, "Avast"). The FTC claimed that Avast licensed or sold detailed web browsing information to third parties through a variety of products, despite promises that its anti-tracking privacy software would protect consumers from online tracking. (The FTC complaint and proposed consent order with respect to Avast is referred to herein as the "Avast Complaint" and the "Avast Order" respectively.)

The FTC alleged that to the extent Avast did describe its information collection and sharing practices, Avast claimed that any sharing of user information would be in "anonymous and aggregate" form, when, in fact, according to the FTC, Avast sold consumers' browsing information to third parties in non-aggregate, re-identifiable form. The FTC asserted that the Avast products provided data buyers with "extraordinary" detail about consumers' browsing habits (e.g., webpages visited, timestamps, location, and a persistent identifier to allow tracking over time) and included various data insights, such as browsing sessions, search terms, e-commerce shopping events, and transactions.

Remedies

As part of the Avast Order, in addition to the $16.5 million fine, Avast agreed to certain limitations and requirements with respect to future uses of browsing information. Most – but not all – of the remedies in the Avast Order are limitations on the use of such data in the context of "Advertising Purposes." The Avast Order defines "Advertising Purposes" broadly to include much of what one might expect to be intended by such a term; yet, there are significant and potentially important exclusions from that definition (e.g., the use of browsing information for "reporting or analytics related to understanding advertising or advertising effectiveness" is not subject to the Order).

There are, however, a few remedies in the Avast Order that apply outside the context of Advertising Purposes. Most notably, the Order requires Avast to implement an extensive privacy program that protects the privacy of "Covered Information" – generally defined as information from or about an individual or an individual's device including personally identifying information, location data and browsing information. Avast must also undergo periodic outside assessments and annual certifications with respect to the program.

Are Contractual Assurances Enough?

Parsing the language of the Orders, the FTC's position appears to be that contractual practices that facially appear to ensure consumer privacy compliance may be insufficient, if not backed by certain diligence practices to assure proper consumer notice and consent. This is borne out in the agency's commentary on the InMarket Order: "InMarket's primary mechanism for ensuring that consumers have provided appropriate consent is through contractual requirements with its third-party app partners. However, contractual provisions, without additional safeguards, are insufficient to protect consumers' privacy."

The FTC reiterated this point in a blog post on the X-Mode Order when it cautioned that companies should not sell, or buy, outside location data "without proof of informed consumer consent" and that "every participant in the location data marketplace is responsible for complying with the law."

While the FTC orders in these three cases may give participants in the data ecosystem additional concrete diligence items to inquire about in connection with data-related transactions, the reality is that in many cases, the consumer data collection process remains complex and opaque. We will watch to see whether these FTC actions, the result in *Kochava*, and further statements and enforcements from the FTC (in addition to further privacy-related legislation and enforcement at the state and federal level), add any additional transparency to that ecosystem.

---

[1] Each FTC Complaint was coupled with a proposed consent order negotiated by the parties The consent orders are subject to public comment but are generally expected to become final and binding on the respondent parties in each case.

[2] The FTC is involved in an ongoing action against the data broker Kochava, Inc. This FTC enforcement began with an August 2022 complaint against Kochava seeking an order halting Kochava's alleged acquisition and downstream sale of "massive amounts" of precise geolocation data collected from consumers' mobile devices.

[3] In a 2022 FTC blog post, the FTC promised that it would "vigorously enforce the law if we uncover illegal conduct that exploits Americans' location, health, or other sensitive data." Most recently, the FTC, in commenting on the InMarket settlement, titled its Business Blog post, "How 'location, location, location' can lead to 'enforcement, enforcement, enforcement'", and stated that "The FTC will take action to protect consumers against the illegal collection of their location data."

[4] The landing pages for each FTC settlement, which contain links to the relevant documents and commentary, can be found here: X-Mode page; InMarket page; Avast page.

[5] "Sensitive Locations" is defined in the X-Mode Order as follows: "Sensitive Locations" means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; or (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants.

[6] ”Sensitive Locations” is defined in the InMarket Order is as follows: “Sensitive Location” means: (1) sexual and reproductive health care providers, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, psychiatric and substance abuse hospitals, offices of oncologists, and offices of pediatricians; (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations held out to the public as predominantly providing education or childcare services to minors; (6) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; (7) locations held out to the public as predominantly providing services based on racial or ethnic origin; (8) locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (9) locations of public gatherings of individuals during political or social demonstrations, marches, and protests.

[7] “Valuable consideration” is not defined.

[8] For example, under the X-Mode Order, X-Mode is required to notify the FTC any time X-Mode determines that a third party shared location data in violation of a contractual requirement between X-Mode and the third party and the acts taken to remediate the incident. Both orders contain a provision where each Respondent is required to timely respond to written requests from the FTC to submit “additional compliance reports or other requested information.”

View original.

Related Professionals

- **Jeffrey D. Neuburger**