Articles + Publications | January 16, 2024

FTC's Sensitive Location Privacy Collection and Sale Expectations: Insights From Data Broker Settlements (and 10 Action Items to Take Now)

WRITTEN BY

James Koenig | Ronald Raether, Jr. | Kim Phan | David N. Anthony | Cindy D. Hanson | Ethan G. Ostroff | Timothy J. St. George | Alan D. Wingfield | Robyn W. Lin

Following several years of investigating the common practices in the space, the Federal Trade Commission (FTC) reached its first settlement with a data broker over the alleged collection and sale of location information that could be used to track people's visits to places of worship, reproductive health clinics, and domestic abuse shelters. Under the proposed order announced on January 9, 2024, X-Mode Social, Inc. and its successor Outlogic, LLC (X-Mode/Outlogic), will be prohibited from sharing or selling such data going forward. Yet, the order provides key lessons for website and mobile app publishers, as well as any company marketing or otherwise using location-based information.

Unfair Use of Sensitive Location Information. X-Mode/Outlogic is a location data broker that sells consumer location data to clients across industries ranging from real estate to finance. Those clients could then use the data for marketing and brand analytics purposes. In its complaint, the FTC alleged that the raw location data sold by X-Mode/Outlogic included unique persistent identifiers for mobile devices called Mobile Advertiser IDs (MAIDs) that could be used to match with the observed mobile device, locations of places the mobile device has visited. In a second step, since the raw data provided by X-Mode/Outlogic contained the location information and timestamps, it was possible for customers who licensed the location data from X-Mode to derive home addresses (where cellphones were located during evening or sleeping hours) and then look up individual or household name information. The FTC also alleged that until at least May 2023, X-Mode/Outlogic did not have any policies or procedures in place to remove places of worship, reproductive health clinics, domestic abuse shelters, and other sensitive locations from the raw location data sets it sold. In addition, the FTC alleged that the company did not implement appropriate safeguards in its contracts with its clients restricting the uses based on sensitive data locations.

Failure to Fully Inform Consumers of Sensitive Location Data Sales and Uses. Further, the FTC also found failure in X-Mode/Outlogic's privacy policy for its own managed websites/apps, as well as the model privacy policy it provided to the website and app publishers from who it obtained location-based information. Specifically, the FTC alleged that the users of X-Mode/Outlogic's own apps, as well as third-party apps that used X-Mode/Outlogic's software development kit (SDK), were not fully informed about how their location data would be used (*e.g.*, the notices did identify collection, sharing, and use of location information for ad personalization and location-based analytics, but did not call out sensitive location collection and use for certain sensitive uses, including selling data to government contractors for national security purposes). Moreover, while the Android mobile phone operating system includes a privacy control that permits users to opt out from marketers using their

©2025 Troutman Pepper Locke

phones' MAIDs to show them personalized ads, the complaint alleged that from at least June 2018 to July 2020, X-Mode/Outlogic failed to employ the necessary oversight to ensure that these privacy choices were honored.

Targeting Consumers Based on Sensitive Characteristics. Finally, X-Mode licensed audience segments, categories of MAIDs based on shared characteristics, for use by third parties (*e.g.*, recently visited "Size Inclusive Clothing Stores," "Firehouses," "Military Bases," and "Veterans of Foreign Wars" establishments). The company also created custom audience segments for customers with special requests, including ones based on sensitive characteristics of consumers (*e.g.*, custom audience segments of consumers who had visited Cardiology, Endocrinology, or Gastroenterology offices and visited a pharmacy or drugstore in the Columbus, OH area, and consumers that had visited a specialty infusion center). The FTC viewed this as an unfair practice.

FTC Order Requirements. Pursuant to the proposed order, X-Mode/Outlogic will be required to:

- Delete all location data previously collected and any products produced from the data unless it obtains consent or ensures the data has been deidentified/rendered non-sensitive.
- Develop a supplier assessment program to ensure that companies that provide location data to X-Mode/Outlogic are obtaining informed consent for the collection.
- Provide a simple way for consumers to withdraw their consent for the collection and use of their location data and for the deletion of any location data that was previously collected.
- Provide a clear means for consumers to request the identity of individuals and businesses to whom their personal data has been sold or give consumers a way to delete their personal location data from the commercial databases of all recipients.
- Establish a comprehensive privacy program that protects the privacy of consumers' personal information and creates a data retention schedule.
- Limit the company from collecting or using location data when consumers have opted out of targeted advertising or tracking, or if the company cannot verify records showing that consumers have provided consent to the collection of location data.

The proposed order will be subject to public comment for 30 days after publication in the *Federal Register* after which the FTC will decide whether to make the proposed consent order final.

Ten Action Items All Companies Should Consider Now. In the wake of the X-Mode order, there are 10 action items that data brokers/resellers, website/app publishers that collect location information, as well as the organizations that use location information for ad targeting, personalization and other purposes, should consider and take action on now:

Action Items – Data Broker:

1. Sensitive Location Data Consent Audit. Data brokers, resellers, and others who sell/license location information that includes sensitive locations, should review all the location data previously collected and any segmentation or targeting products produced from this data to confirm that appropriate consumer consent, in line with the FTC order, was obtained.

2. De-Identify Location Data or Render Nonsensitive. If consent was not obtained or sensitive location information uses not called out, existing databases of location data should be de-identified (by removing latitude, longitude, and specific timestamp information) to prevent deriving home address and individual identities) or rendered nonsensitive (by removing the longitude and latitude and/or other indicators of sensitive locations).

3. Develop Location Data Supplier Assessment Program – Upstream Audit. Data brokers should develop and roll out a supplier assessment program to ensure that website and app publishers that use an SDK or other means to collect location information and sell it to data brokers, do so by first obtaining consent from consumers for the collection, use, and sale of such data.

4. Draft Contractual Safeguards to Restrict Using Sensitive Location Information. Data brokers should update license agreements and procedures to ensure that recipients of location data do not associate the data with sensitive locations (as identified in the order, "locations that provide services to LGBTQ+ people such as bars or service organizations, with locations of public gatherings of individuals at political or social demonstrations or protests, or use location data to determine the identity or location of a specific individual").

5. Opt Out for/Deletion Mechanism for Location-Based Data Advertising and Other Uses. The FTC is also requiring that consumers have a simple and easy-to-find way for consumers to withdraw their consent for the collection and use of their location data and for the deletion of any location data that was previously collected. This requirement will involve process reviews and potential updates for publishers and location information users as well.

• **Note – Accounting of Disclosures Requirement.** While it is difficult for a data broker to track downstream uses and further sales, the FTC also requested that consumers have access to an accounting of the third parties that receive their location information and for a way to delete their personal location data from the commercial databases of all recipients of the data. Given the industry collaboration necessary to enable these requirements, this will likely evolve through industry associations like the IAB (Interactive Advertising Bureau), 4As (American Association of Advertising Agencies), or other industry groups.

***Action Items – Website and App Publishers Collecting Location Information*:**

6. Review and Update Privacy Policies and Consent Process. Websites and apps that collect location information (or use an API that collects such information), should review and update their privacy notices (including the template language received from data brokers) and consent processes to make sure they fully cover the full range of potential uses and sharing. Given the compliance risk, some publishers may begin reconsidering their practice of selling location information.

• **Note:** This and other action item can be incorporated with the review of privacy policy for compliance with new U.S. state comprehensive privacy law requirements and international law requirements (*e.g.*, EU, China, and

others) as well as privacy impact assessments (PIAs) for the use of new sensitive technologies (*e.g.*, such as location data, based on findings in the FTC's consent decree with Rite Aid released December 19, 2023.

7. Update or Develop Comprehensive Privacy Program and Data Retention Schedule. The FTC has restated its position that companies should establish and implement a comprehensive privacy program that protects the privacy of consumers' personal information, it also called out in the order the expectation that the program also include a data retention schedule.

• **Note:** Data retention schedules can also be updated as part of U.S. state comprehensive privacy laws compliance initiatives.

8. Opt Out for/Deletion Mechanism for Location-Based Data Advertising and Other Uses and Accounting of Disclosures. As noted in number 5 above, the FTC requires that consumers who have access to opt out of location information advertising/uses or delete their location information, and to an accounting of their location data recipients, website, and app publishers collecting location information, as well as the organizations using such information for advertising and other purposes, should keep abreast of industry and technical developments that will enable compliance with such requirements.

Action Items – Organizations Using Location Information for Target Marketing, Personalization, Analytics, and/or Other Uses:

9. Reaffirm Current Location Information Uses. Based on the order, organizations that purchase/license location data are discussing the review and validation of their desire to continue the advertising, personalization, analytics, and other uses involving location information, especially uses that either (i) involve tracking of sensitive locations (including those mentioned in the order — medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters), and/or (ii) derive the individual identity of the cellphone user, and/or derive household address/targeting.

10. Review/Update Program Around Sensitive Location Data Uses, License Agreement Representations, and Consent Audits. Organizations that purchase/license location data should consider a two-prong approach:

• **Develop Model Template License Agreement Representation Regarding Consent and Compliance.** Review licensing agreements (and prepare template language) to ensure data brokers or location-based information resellers have a chain of consent for the full range of intended uses and compliance. Special consideration for targeting based on sensitive location information, uses involving political purposes, and/or government intelligence or surveillance.

• **Location Data Broker Diligence.** Conduct pre-contract diligence or post-contract risk-based compliance audits of the data broker practices.

Location, Location, Location – Our Take.

The FTC's latest order focuses on two areas of recent scrutiny in the privacy world, (1) data brokers, and (2) sensitive data such as sensitive locations consumers visited. Additionally, this settlement mirrors other recent FTC

settlements, which have required a business to delete the personal information at issue in the complaint. Specifically, the FTC is requiring X-Mode/Outlogic to start over and delete sensitive location data (which is defined, but includes medical facilities, religious organizations, correctional facilities, and others) collected before complying with privacy protections the FTC believes needs to be in place.

In an FTC blog post about the settlement, the FTC states that the "status quo is a no go" embracing what has been said previously, namely what the FTC lacks in rulemaking authority, it makes up in settlements. The conduct provisions imposed on the company in the proposed order go far beyond remediating any potentially unfair or deceptive acts or practices, but rather create affirmative obligations that are not articulated in the law, setting the stage for companies to have to anticipate all potential misuses of consumer data by third parties. Simply avoiding engaging in unfair or deceptive acts or practices will no longer be sufficient under the paternalistic approach advocated by the FTC in this enforcement action.

While this is the first-ever settlement by the FTC against a data broker involving sensitive location data, it may be an indication that further scrutiny of the data broker ecosystem will continue in 2024. As we have previously discussed, the Consumer Financial Protection Bureau has proposed expanding rulemaking under the Fair Credit Reporting Act (FCRA) to include data brokers. If promulgated, this rulemaking could impose FCRA obligations upon data brokers, including dispute and reinvestigation obligations. 2023 also saw additional obligations imposed upon certain data brokers as a result of new state laws, such as the California Delete Act, Oregon's new data broker law, and Texas' new data broker law.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Data + Privacy