

[Blogs](#)

January 17, 2024

FTC Cracks Down on Collection and Sharing of Sensitive Location Data With Proposed X-Mode Settlement



On January 9, 2024, the Federal Trade Commission (FTC) announced its [complaint](#) and [proposed settlement](#) with location data broker X-Mode Social, Inc. and its successor Outlogic, LLC (collectively X?Mode).

Under the order, X-Mode will be prohibited from sharing or selling any "sensitive location data"—location data that identifies visits to sensitive locations such as medical facilities, religious organizations, and other locations that allow potentially sensitive inferences. The FTC's action reflects the FTC's continued focus on location data, particularly that reflects potentially sensitive information, and is similar to the case it is currently litigating against [Kochava](#) regarding its sales of precise geolocation data.

X-Mode's Business Practices

X-Mode collects precise location data through third-party apps that incorporate its software development kit, as well as directly from consumers who use its mobile apps, Drunk Mode and Walk Against Humanity. X-Mode also licenses such information from third parties. X-Mode then sells both raw location data and the audiences it creates from such data to its customers, which include advertisers, consulting firms, and private government contractors. X-Mode, the FTC alleged, does not restrict the collection of location information from "sensitive" locations such as healthcare facilities, churches, and schools, though it does contractually restrict how its customers may use the location data it sells.

Complaint

The FTC's seven-count complaint hinges on X-Mode 1) selling location data that can be used to identify consumers' visits to sensitive locations; 2) failing to honor consumers' opt-out choices expressed through mobile platform settings; 3) failing to obtain, or ensure that its data sources obtained, sufficient consent to sell location data to third parties, including by providing insufficient or incomplete notices; and 4) targeting consumers based

on sensitive characteristics. The FTC alleges that these practices were both unfair and deceptive and thus violated Section 5 of the FTC Act.

Selling Sensitive Location Data

Similar to the complaint against Kochava, the FTC alleges the raw location data X-Mode provided to others was not anonymized because it is possible to use such information to identify the owners of mobile devices—either by buying data matching the advertising IDs sold by X-Mode to real-life identities or by using timestamped signals to, for example, infer consumers' addresses. Such information can be used to identify consumers' trips to highly sensitive locations such as medical facilities, reproductive health clinics, places that allow inference regarding consumers' religion or sexual orientation, and domestic abuse shelters. While X-Mode imposed certain contractual restrictions on its customers using location data for such purposes, the FTC alleges that it failed to enforce such restrictions or to adopt any technical protections preventing such use. The FTC further alleges that X-Mode failed to take steps to ensure that proper consent was obtained. The FTC alleges that such selling practices are unfair because they are likely to cause substantial injury to consumers that is not outweighed by any countervailing benefits to consumers or competition and could not reasonably be avoided by consumers.

Failure To Honor Opt-Outs

The FTC also alleges that for a period of time, X-Mode ignored opt-outs expressed on consumers' mobile devices and continued to sell the location data and other information of opted-out consumers, which allowed its customers to continue to build profiles and serve personalized ads in contravention of consumers' choices. The FTC alleges that this, too, is an unfair practice.

Notice and Consent

The FTC alleges that X-Mode failed to fully disclose the purposes for which consumers' location data would be used. While X-Mode's disclosure (used both in its own apps and through partner apps) was lengthy, and specifically informed consumers that the apps were supported by collecting and sharing mobile ad IDs with third parties for advertising and analytics purposes, it did not disclose that location information was also sold to government contractors for national security purposes, a disclosure the FTC believes would be material to consumers. The FTC also alleges that X-Mode failed to verify that its partner apps provided informed consent to the collection, use, or sale of their data. The FTC alleges that the collection of location information without informed consent is an unfair practice and that the provision of location data to government contractors for national security purposes without sufficient notice was a deceptive practice because X-Mode's sharing of data to such entities would be material to consumers in deciding whether to grant location permissions.

Sensitive Audiences

Finally, the FTC alleged that X-Mode had created custom audience segments for its customers that were, in some cases, based on sensitive consumer characteristics such as visits to particular healthcare providers. The FTC alleges that the creation of such practices is an unfair practice and not reasonably avoidable by consumers.

Proposed Consent Order

The proposed consent order, which is subject to a 30-day comment period, would require X-Mode to undertake substantial changes, including to cease selling, licensing, transferring, sharing, disclosing, or using "Sensitive Location Data," defined as location data associated with "Sensitive Locations." "Sensitive Locations," are

defined as locations associated with medical facilities, religious organizations, correctional facilities, labor union offices, those providing education and childcare services to minors or services based on racial or ethnic origin, and those providing shelter or social services to unhoused individuals, survivors of domestic abuse, refugees, or immigrants. This obligation is similar to the voluntary [Precise Location Information Solution Provider Voluntary Enhanced Standards](#) recently adopted by the Network Advertising Initiative (NAI). X-Mode would also be required to delete all location data it collected previously or else receive affirmative express consent to continue processing it. The company would also be required to create a Sensitive Location Data program to prevent the use, sale, licensing, transfer, or disclosure of Sensitive Location Data, develop a supplier assessment program that ensures that consumers provide affirmative express consent for the collection, use, and sale of their location data, and to establish, implement, and maintain policies designed to prevent recipients of its data from using it in certain potentially invasive ways, such as associating the data with locations providing services to LGBTQ+ individuals or locations of political or social demonstrations or using such information to determine the identity or location of an individual's home. The company would also be required to provide consumers with quarterly reminders that their location is being collected and disclosed and to provide them with a simple way to turn off location data collection and request the deletion of their information.

Takeaways

While this is the first time the FTC has imposed a ban on the use and sale of Sensitive Location Data, this complaint and order signals that the FTC continues to scrutinize the sale of location data as well as the processing of sensitive information. Businesses that collect location data should take steps to ensure their disclosures accurately reflect their practices, including the third parties that may receive this information and the uses of such information, and that consider steps to avoid processing information about visits to sensitive locations.

Authors

Explore more in

[Privacy & Security](#) [Perkins on Privacy](#)