

February 20, 2024

Chair Lina M. Khan
Commissioner Alvaro Bedoya
Commissioner Rebecca Kelly Slaughter
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: *X-Mode Social, Inc.*, File No. 212 3038

Dear Chair Khan and Commissioners Bedoya and Slaughter,

Free Press writes to support the FTC’s proposed consent order and settlement with X-Mode Social, Inc. and its successor Outlogic, LLC (together, “X-Mode”), arising from X-Mode’s alleged violations of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).¹

The proposed order follows the FTC’s seven-count complaint alleging that X-Mode unfairly sold sensitive data and categorized consumers using sensitive characteristics for marketing purposes; unfairly collected and used consumer location data, including without consent verification; unfairly failed to honor consumers’ privacy choices, including their choices to opt-out of having their location data used for such purposes; deceptively failed to disclose use of consumers’ location data; and provided the means and instrumentalities to engage in deceptive acts or practices.

Free Press commends the FTC’s efforts to address the uniquely sensitive nature of location data; the inadequacies of X-Mode’s notice and consent verification practices, including in its relationships with third parties; and the harms generated by using sensitive characteristics to categorize consumers for targeted marketing. These concerns fall squarely within the FTC’s Section 5 authority to investigate and take enforcement action in order to address unfair or deceptive acts or practices. Each of these activities causes substantial harm to consumers.

¹ X-Mode Social, Inc.; Public Comment, 89 Fed. Reg. 3404 (Jan. 18, 2024), <https://www.federalregister.gov/documents/2024/01/18/2024-00928/x-mode-social-inc-public-comment>; FTC, Press Release, “FTC Order Prohibiting Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data” (Jan. 9, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

Location data is one among many categories of personal data that are routinely collected, used, sold, and bought by commercial entities including software developers, retailers, ISPs, and data brokers. This occurs in a multi-billion dollar market that revolves around persistently tracking consumers, often through mobile applications.² While consumers may consent to having their location data collected and used for clear, specific, and functional purposes – for example, mobile ride-share and mapping applications that require location data to provide their services – disclosures regarding third-party access to such data are often buried in lengthy terms of service or privacy policies that omit material information.³ Consumers may also take steps to avoid having their location data collected through their mobile devices, only for companies like X-Mode to unfairly and deceptively collect, market, and sell that data anyway.⁴

As the FTC notes, location data is often uniquely sensitive. It can convey information about religious and political affiliations; racial, ethnic, and gender identity; even medical conditions and treatments.⁵ It can be used to infer financial difficulties, sexual orientation, pregnancy status, and housing conditions, to name just a few examples.⁶ As a result, the collection, use, and sale of location data have significant implications for people’s civil and constitutional rights, from racial justice and reproductive justice to First Amendment rights of association and protest.

Yet while we understand the reasoning behind the “sensitive locations” definition in the order, and the relationship of that definition to the harmful conduct of X-Mode described by the complaint, Free Press would urge the FTC to consider broadening the definition to include additional examples and broader categories than the proposed order presently enumerates. While the types of locations listed in the order are undoubtedly sensitive, any location data could be sensitive to some individuals or groups. The FTC should empower consumers rather than regulators to determine what types of location data are sensitive in their own view, not necessarily to prevent any and all requested or permitted use of such location data, but to ensure that entities like X-Mode obtain the same affirmative express consent and offer the same protections in all instances.

² Jon Keegan & Alfred Ng, “There’s a Multibillion-Dollar Market for Your Phone’s Location Data,” *The Markup* (Sept. 30, 2021), <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>.

³ Jenna Ruddock, Free Press Action, *Insatiable: The Tech Industry’s Quest for All Our Data* (Oct. 2023) (“*Insatiable*”), https://www.freepress.net/sites/default/files/2023-11/insatiable_the_tech_industry_quest_for_all_our_data_free_press_action_report_final.pdf.

⁴ *In the Matter of X-Mode Social, Inc. and Outlogic, LLC*, File No. 212 3038, Draft Complaint, ¶¶ 20-23 (2022) (the “Complaint”), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf.

⁵ *Id.* ¶¶ 42-44.

⁶ Justin Sherman, “The Location Data Market, Data Brokers, and Threats to Americans’ Freedoms, Privacy, and Safety,” Massachusetts Legislature, Joint Committee on Consumer Protection and Professional Licensure, Hearing on Pending Legislation (June 26, 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Sherman-Justin_WrittenTestimony_MA_Legislature.pdf.

The pervasiveness of X-Mode’s alleged collection, use, and commercialization of such location data demonstrates the need for these more stringent protections. According to the FTC’s complaint, X-Mode licenses raw location data – including latitude, longitude, and timestamps – tied to unique persistent identifiers called Mobile Advertiser IDs (“MAIDs”). X-Mode collects this data through the company’s own mobile applications as well as through third parties, in particular mobile apps using X-Mode’s software development kit (“SDK”).⁷

As the FTC highlights, such data can easily be used to link a device to an individual. While a device’s presence in one location at an unspecified time might not clearly associate that device with a specific person, data points showing where a device is located at particular times of day or where a device travels over the course of several hours can dramatically narrow down the possible owners of that device.⁸ Data collected from particular locations – such as specialist medical facilities, shelters serving survivors of domestic violence, or houses of worship – can also be used to target individuals or larger groups on the basis of sensitive characteristics such as those described above, as well as others in the FTC’s complaint and proposed order.

The FTC alleges that X-Mode created custom audience segments to enable targeted marketing based on the sensitive characteristics that could be inferred from the precise location data X-Mode collects. In one instance described in the complaint, X-Mode entered into a licensing agreement with a clinical research company, providing it with data on consumers who had visited cardiology, endocrinology, or gastroenterology offices, had stayed for at least 30 minutes, and had subsequently visited a pharmacy, as well as data on consumers that had visited specialty treatment centers and had stayed for at least one hour.⁹ Such granular data relating to sensitive locations enables companies like X-Mode to license consumers’ data, without their knowledge or consent, to facilitate targeted marketing on the basis of this sensitive information – in this case, inferred medical conditions and treatments. Press accounts have further illustrated how data involving the sensitive locations set forth in the FTC’s proposed order in this matter can be exploited: last year, the *Wall Street Journal* described how an anti-abortion organization used location data to target ads containing reproductive health disinformation to people who visited Planned Parenthood locations.¹⁰

The proposed order requires X-Mode to take several actions for already-collected data and data products, including audience segments. The company must delete all historic location data and data products unless it can newly obtain affirmative express consent or it can ensure that retained data is deidentified or otherwise rendered non-sensitive. Critically, this decision correctly places

⁷ Complaint ¶¶ 6-11.

⁸ *Id.* ¶¶ 17-19.

⁹ *Id.* ¶¶ 38-39.

¹⁰ Bryon Tau, “Antiabortion Group Used Cellphone Data to Target Ads to Planned Parenthood Visitors,” *Wall Street Journal* (May 18, 2023), <https://www.wsj.com/articles/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212>.

the burden of compliance on X-Mode, rather than requiring consumers – many of whom are unaware that X-Mode has their sensitive location data in the first place – to take action to have their data deleted or deidentified. As discussed above and in the FTC’s complaint, location data can easily be reidentified if, for example, enough data points are available or if timestamps are attached to that data. Ensuring that X-Mode adequately deidentifies any data or data products that are retained will be critical to ongoing enforcement. Similarly, while the proposed order also requires X-Mode to give consumers a “simple, easily-located” way to withdraw their consent regarding all location data collection and use, the order’s baseline prohibition on future use, sale, licensing, transfer, or disclosure of sensitive location data appropriately places the primary burden on X-Mode to curtail its own activities where sensitive location data is involved. This additional measure is necessary due to the fact that location data can enable targeting on the basis of sensitive characteristics without any additional identifying information, as described above.

The FTC complaint alleges that X-Mode additionally failed to provide information necessary to obtain consumers’ informed consent prior to collecting and using this sensitive location data, and similarly failed to verify that third-party apps incorporating X-Mode’s SDK obtained informed consent prior to granting X-Mode access to consumers’ sensitive location data. As a result, consumers were unaware that their sensitive location data was being used, packaged, and sold to specific categories of third-party buyers for targeting and other such purposes. Like many companies, X-Mode published a privacy notice on its website describing some potential commercial uses of consumers’ personal information.¹¹ That notice, however, was not comprehensive: it failed to notify consumers that X-Mode would be selling their location data to government contractors for self-styled national security purposes.¹² Additionally, X-Mode provided sample consumer consent notices to third-party app publishers that similarly omitted this information.¹³

Free Press has published research documenting how other technology companies similarly bury disclosures in lengthy privacy documents while failing to comprehensively identify potential third-party recipients of consumers’ data – and how these practices routinely inhibit consumers’ ability to give effective affirmative express consent to the collection and use of their data, particularly sensitive data.¹⁴ These kinds of widespread practices highlight the need for FTC intervention in situations like this. X-Mode both unfairly and deceptively collected, used, and licensed this data in ways that caused and are likely to cause substantial harm to consumers’ ability to exercise their constitutional and civil rights; to obtain medical care free from unwelcome scrutiny; or to take advantage of other economic opportunities.

¹¹ Complaint ¶¶ 24-25.

¹² *Id.* ¶ 30.

¹³ *Id.* ¶¶ 26-35.

¹⁴ *Insatiable* at 5, 11.

The proposed order requires X-Mode to keep records documenting consumers' affirmative express consent when collecting location data for any individual or device through X-Mode's own mobile applications and, where feasible, when collecting location data through any third parties. The FTC defines "affirmative express consent" as an individual's freely given, specific, informed, and unambiguous consent following a "clear and conspicuous disclosure" that, notably, must (1) describe all types of entities to whom the covered information is disclosed and (2) be separate from a company's privacy policy or terms of service/use. Requiring that these disclosures be made separately from terms of service/use, as well as requiring that these disclosures link to a simple, easily-located means for consumers to withdraw consent, will help clarify for consumers that they do not have to consent broadly to the collection, use, and sale of their sensitive data as a precondition for using a particular mobile app. But ensuring that X-Mode follows the FTC's additional guidance regarding what design elements constitute a "clear and conspicuous" notice and a "simple, easily-located" means to withdraw consent must also be a key part of ongoing enforcement efforts. As the FTC has previously reported, there are many tactics used by companies to trick or manipulate consumers into giving up their privacy, including under the guise of obtaining consent.¹⁵

A notable feature of the data broker marketplace is that consumers often do not interact directly with the many brokers who may be collecting, packaging, and selling consumers' data.¹⁶ This is true for many of the consumers whose data was collected through mobile apps using X-Mode's SDK, as well as by third parties with whom X-Mode has data sharing agreements. The proposed order takes critical steps to address this issue by outlining additional obligations X-Mode has relating to data it collects through third parties. X-Mode must relay the terms of the order to recent X-Mode customers, and then submit those notifications to the FTC; must establish a supplier assessment program to ensure that third parties from whom it collects data are also obtaining affirmative express consent prior to collecting and sharing consumers' location data; and must provide a simple, easily-located means for consumers to request the identity of any third parties to whom their location data has been sold, transferred, licensed, or otherwise disclosed.

Collectively, these requirements help to pierce the consumer-side opacity of the location data broker market, ensuring that X-Mode's obligations do not begin only once the company receives consumers' data or end once the company licenses, shares, or otherwise transfers consumers' data. The requirement to allow consumers proactively to request the identity of any third parties to whom their location data has been sold, transferred, licensed, or otherwise disclosed is a

¹⁵ FTC, Press Release, "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers" (Sept. 15, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers>.

¹⁶ Alfred Ng & Jon Keegan, "Who Is Policing the Location Data Industry?" *The Markup* (Feb. 24, 2022), <https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry>.

critical complement to the requirement that “clear and conspicuous disclosure” include documentation regarding the types of entities to whom X-Mode discloses covered information.

Free Press again commends the FTC’s efforts to address the harms caused by the collection, use, and sale of location data as well as the ways in which the standard notice-and-consent model for privacy disclosures too often fails to adequately inform consumers and also fails to empower consumers to give, withhold, or withdraw their affirmative express consent.

Yet while we support the steps taken in this enforcement action, we would emphasize that exceptions like those made for deidentified data and data retention should be carefully monitored. The FTC’s ongoing role here is crucial, given the inability of consumers to independently verify that their data has been deleted or that it has been rendered incapable of being reidentified. That continued enforcement role is also critical in light of the FTC’s allegations regarding X-Mode’s past handling of sensitive, identifiable location data as well as the company’s disregard for consumers’ clearly expressed privacy preferences.

Respectfully submitted,

Jenna Ruddock, Policy Counsel
Matthew F. Wood, VP of Policy
Free Press

jruddock@freepress.net