epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 20, 2024

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

**Re: *X-Mode Social, Inc.*, FTC File No. 202-3038**

Dear Chair Khan and Commissioners Slaughter and Bedoya,

By notice published January 18, 2024, the Federal Trade Commission (FTC) announced its proposed consent order and settlement with X-Mode Social, Inc. (X-Mode) and its successor, Outlogic, LLC, for X-Mode's alleged violations of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), prohibiting unfair or deceptive acts or practices.[1] The proposed consent order with X-Mode is the result of the FTC's complaint alleging that X-Mode violated the FTC Act in seven ways: (1) unfair sale of sensitive data; (2) unfair failure to honor consumer privacy choices; (3) unfair collection and use of consumer location data; (4) unfair collection and use of consumer location data without consent verification; (5) unfair categorization of consumers based on sensitive characteristics for marketing purposes; (6) deceptive failure to disclose use of location data; and (7) furnishing the means and instrumentalities to engage in deception.[2]

The Electronic Privacy Information Center (EPIC), Demand Progress, and the Electronic Frontier Foundation (EFF) submit this letter to applaud the FTC's enforcement efforts in this matter and to provide recommendations to strengthen the proposed order (and others like it in future cases concerning location data). EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed FTC consent orders and complaints regarding business practices that violate privacy rights.[3] Along with their one million activists, Demand

[1] X-Mode Social, Inc.; Public Comment, 89 Fed. Reg. 3,404 (Jan. 18, 2024), https://www.federalregister.gov/documents/2024/01/18/2024-00928/x-mode-social-inc-public-comment [hereinafter Federal Register Notice].
[2] *Id.*; X-Mode Social, Inc., Complaint, *In the Matter of X-Mode Social, Inc.*, FTC File No. 202-3038 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf [hereinafter Complaint].
[3] *See, e.g.*, Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter EPIC Commercial Surveillance Comments]; Comments of EPIC, *In re BetterHelp, Inc*,, FTC File No. 202-3169 (2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-betterhelp-inc/; Comments of EPIC, *In re CafePress*, FTC File No. 192-3209 (2022), https://epic.org/wp-content/uploads/2022/04/EPIC-comments-in-re-cafepress.pdf; Comments of EPIC, *In re Matter of Support King, LLC (SpyFone.com)*, FTC File No.

Progress fights for a more just balance of corporate power, including fighting monopolies and corporate surveillance. EFF works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF was founded in 1990 and has more than 30,000 members. It is a nonprofit organization that advocates before courts and legislatures to protect the privacy of technology users and consumers from corporations that collect and monetize their personal information.

EPIC, Demand Progress, and EFF commend the Commission for using its authority to investigate and take enforcement actions against companies like X-Mode engaged in unfair and deceptive practices, especially where companies profit off these practices by selling location and other sensitive information (directly or indirectly) to law enforcement and intelligence authorities, who then may use this unlawfully obtained data to target consumers and their communities. As the Commission knows, location data can reveal highly sensitive traits about consumers, including medical conditions and treatments. In the aftermath of the U.S. Supreme Court's overturning of the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*, the sale of location data poses a special threat to the safety of abortion patients and providers and undermines reproductive privacy.[4]

## I. The Prohibition on the Use, Sale, or Disclosure of Sensitive Location Data

We commend the Commission for highlighting the significant harms caused by the use, sale, and disclosure of sensitive location data and for taking action against X-Mode to limit these harms. To provide even greater protection for consumers, we encourage the Commission to strengthen certain provisions before finalizing the consent order. First, the order should not introduce a distinction between "sensitive location data" and other location data, as all location data is inherently sensitive in nature. Second, to the extent that the final order still distinguishes some forms of location data as sensitive location data, that category should at least be broadened to include location data that may reveal an individual's sexual orientation or gender identity, involvement in political public gatherings, or residence. Third, the sensitive location data prohibition should not give X-Mode the option of converting such data into non-sensitive location data or non-location data for subsequent use, sale, or disclosure. And finally, while we applaud the robust requirements for

192-3003 (2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; Comments of EPIC et al., *In re Zoom Video Communications, Inc.*, FTC File No. 192-3167 (2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; Complaint of EPIC, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc.*, FTC File No. 172-3139 (2019), https://epic.org/apa/comments/EPICFTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (2019), https://epic.org/apa/comments/EPIC-FTCCambridgeAnalytica-Sept2019.pdf; EPIC, *Comments on Standards for Safeguarding Customer Information*, Docket No. 2019-04981 (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf.

[4] Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.

obtaining express affirmative consent from consumers, a data minimization framework that limits all out-of-context secondary data uses would be the strongest approach to protect consumers.

First, all precise location data is sensitive information. We urge the Commission not to distinguish between sensitive and non-sensitive location data in the order's definitions or prohibition on the use, sale, or disclosure of sensitive location data. As the Commission has explained, "[a]mong the most sensitive categories of data collected by connected devices are a person's precise location and information about their health."[5] Chair Khan, joined by Commissioners Slaughter and Bedoya, noted in this very case that "[o]f the many types of personal data, location data is among the most sensitive."[6] And in the Commission's First Amended Complaint in *FTC v. Kochava*, the Commission explained that the data broker's "disclosure of precise geolocation data also reveals sensitive information about consumers[.]"[7] We agree. Indeed, leading privacy frameworks typically make no distinction between sensitive and non-sensitive location information. For example, the American Data Privacy Protection Act (ADPPA)—a federal comprehensive privacy bill proposed in 2022—includes precise geolocation information in its "Sensitive Covered Data" definition,[8] and the California Consumer Protection Act includes a consumer's precise geolocation in its "Sensitive Personal Information" definition.[9] We recommend that the final order be harmonized with these privacy frameworks and the Commission's own views this issue: precise geolocation data is sensitive data, regardless of the particular locations it may reveal. The final order should not afford different protections to "sensitive location data" and other location data because that distinction fails to fully protect consumers from the harms associated with the unauthorized disclosure of their location information.

Second, if the Commission concludes it is appropriate to delineate certain categories of location data that deserve heightened protection, those categories should be broadened to cover all types of location data that could reveal sensitive traits. The proposed order's definition of "Sensitive Locations" is too narrow as it does not include, for example, locations that could reveal a person's sexual orientation, gender identity, or sexual preferences. In Section IV, the proposed order requires X-Mode to maintain procedures to prevent recipients of X-Mode's location data from: (i) associating such location data with (a) locations held out as predominantly providing services to LGBTQ+ individuals, or (b) locations of political public gatherings; or (ii) using such location data to determine the location of an individual's home.[10] The final order should, at a minimum, include

---

[5] Kristin Cohen, *Location, Health, And Other Sensitive Information: FTC Committed To Fully Enforcing The Law Against Illegal Use And Sharing Of Highly Sensitive Data*, FTC Bus. Blog (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[6] Statement, *In re X-Mode Social, Inc. and Outlogic, LLC*, FTC, FTC File No. 212-3038 (Jan. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/StatementofChairLinaM.KhanandRKSandAB-final_0.pdf [hereinafter FTC Statement].

[7] Amended Compl., *Fed. Trade Comm'n v. Kochava Inc*., No. 2:22-CV-00377-BLW, 2023 WL 3249809 ¶ 91 (D. Idaho May 4, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf.

[8] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. Sec. 2 § 28(A)(vi) (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[9] Cal. Civ. Code § 1798.140(ae)(C).

[10] X-Mode Social, Inc., Decision & Proposed Order, *In the Matter of X-Mode Social, Inc.*, FTC File No. 202-3038 at 8 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf [hereinafter Proposed Order].

these types of sensitive locations in the "Sensitive Locations" definition, which would in turn bring it under the prohibition on the sale, use, or disclosure of sensitive location data. The Commission has rightly recognized the serious harms that stem from the commercialization of these types of location information and should similarly protect them by prohibiting X-Mode's use, sale, and disclosure of such data under Section II of the proposed order.

Third, we recommend that exception (i) in Section II be eliminated. The proposed order rightfully prohibits the sale, use, or disclosure of sensitive location data but states that these prohibitions "do not apply if Respondents: (i) use Sensitive Location Data to convert such data into data that (a) is not Sensitive Location Data or (b) is not Location Data[.]"[11] This could allow X-Mode to use the sensitive location data at the center of the Commission's complaint in the future in ways that could reveal sensitive information about a consumer. For example, if X-Mode is in possession of sensitive location data which reveals that an individual visited an addiction treatment center, Section II would appear to permit X-Mode to process that data into a non-location (but nevertheless highly sensitive) data point: the fact the individual visited an unspecified addiction treatment center. X-Mode would then be free to use, sell, or disclose that sensitive inference so long as it complied with the other provisions of the order. We recommend that the Commission eliminate this potential workaround in Section II to ensure that the order's prohibition on the use, sale, or disclosure achieves its intended effect of safeguarding consumers from the misuse of certain location data.

Finally, as EPIC has noted previously in filings with the Commission, we believe that the best way to mitigate the harms from the collection, use, and disclosure of personal information is a data minimization framework rather than a system that leans heavily on consumers to grant or withhold consent. In a data minimization framework, the practice of sharing location data—especially "raw location data with persistent identifiers that can be used to connect specific individuals to specific locations"[12]—with other entities would in many cases constitute an impermissible secondary data use that violates the context in which that data was collected.[13] However, to the extent that the order relies on individual consent to limit the location data available to X-Mode for commercial exploitation, we commend the Commission for including strong requirements in its definitions of "Affirmative Express Consent" and "Clear and Conspicuous," as well as in the "Withholding and Withdrawing Consent" and "Obligations When Consent is Withdrawn" provisions of the proposed order.

## II. Exclusion of Precise Location Data Collected Outside the United States

We commend the Commission for emphasizing the specific deceptive practice of selling data to defense contractors for national security purposes. The complaint notes that X-Mode "failed to inform consumers that it would be selling data to government contractors for national security purposes[,]" a fact that "would be material to consumers in deciding whether to use or grant location permissions to mobile apps."[14] As noted above, the proposed order would require X-Mode to provide

[11] Proposed Order, *supra* note 10, at 8.
[12] FTC Statement, *supra* note 6.
[13] Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC (May 4, 2023), https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/.
[14] Complaint, *supra* note 2, at 5.

a clear and conspicuous means of requesting the identity of "any entity, business, or individual to whom their location data has been sold, transferred, licensed, or otherwise disclosed."[15]

EPIC has previously urged the Commission to recognize that the lack of adequate notice of commercial processing of personal data is an unlawful trade practice.[16] Although notice and consent alone cannot legitimize commercial surveillance practices, they "remain essential components of an effective data protection regime[.]"[17] The Commission's explicit emphasis on the sale of data to government contractors for national security purposes is an encouraging step toward reining in the cottage industry of data brokers and other firms unlawfully trafficking in Americans' most sensitive information.[18] We believe that the Commission's proposed order should be a signal not only to data brokers like X-Mode but to the government agencies subsidizing the data broker industry by purchasing location data and other sensitive information about Americans, knowing full well that this information has been obtained through unlawful trade practices.[19]

As noted above, we believe the Commission has taken an important step to protect location data but should do more to ensure that *all* precise location data is adequately protected.[20] In that same vein, we urge the Commission to remove language from its proposed order (and any similar consent orders in the future) that excludes from the definition of location data all "[d]ata that [. . .] is collected outside the United States and used for (a) Security Purposes or (b) National Security purposes conducted by federal agencies or other federal entities."[21]

We urge the Commission to protect Americans by ensuring that the same restrictions apply whether location data is collected inside or outside the United States. The effects on American consumers are twofold. First, excluding location data collected outside the United States could create ambiguities that make it difficult to effectively enforce these restrictions and even invite gamesmanship. In particular, the language of the Commission's proposed order could be ambiguous when it comes to collection. For example, an American consumer may use an app based outside the United States, which then packages and sells that data to a data broker in the United States, who then sells that data to government contractors. As the proposed order is written, it is unclear whether the Commission would consider this data to have been collected "outside the United States" (and therefore beyond the scope of the order's provisions concerning location data). Further, these ambiguities—combined with the industry practice of packaging and repackaging large sets of

[15] Proposed Order, *supra* note 10, at 13.
[16] EPIC Commercial Surveillance Comments, *supra* note 3, at 153.
[17] *Id.*
[18] *See, e.g.*, Alfred Ng, *A company tracked visits to 600 Planned Parenthood locations for anti-abortion ads, senator says*, Politico (Feb. 13, 2024), https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172 (revealing that a company ran an anti-abortion ad campaign using location data obtained through Near Intelligence, a firm that had previously sold data to U.S. government intelligence agencies); Joseph Cox, *Broker That Sold Abortion Clinic Data Contracted with Air Force for 'Targeting'*, 404 Media (Feb. 13, 2024), https://www.404media.co/safegraph-abortion-clinic-data-contracted-with-air-force-for-targeting/ (reporting that SafeGraph, which had previously sold location data about abortion clinics, contracted with the U.S. Air Force to improve "targeting cycle and decisions" in "contested geographies[.]"
[19] Letter from Ron Wyden, U.S. Sen., to Avril Haines, Dir. Nat'l Intel. (Jan. 25, 2024), https://static01.nyt.com/newsgraphics/documenttools/0117fa5f9ff7ae33/fe33e1ba-full.pdf.
[20] *See supra* Section I.
[21] Proposed Order, *supra* note 10, at 7.

location data—may have the perverse effect of incentivizing data brokers to engage in a shell game of various data sets to circumvent these protections.

Second, the FTC's proposed consent order provides insufficient protections to the millions of Americans and other U.S.-based consumers—including service members and their families—who travel or live outside the United States.[22] For example, a user of Muslim Pro, a prayer app with over 98 million downloads whose data was sold through X-Mode, would have no notice or expectation that their data would be sold to government contractors for national security purposes.[23] The Commission correctly prohibits X-Mode from using, selling, or disclosing sensitive location data like this collected inside the United States, finding that such sale "poses an unwarranted intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers."[24] However, if that same person travels outside the United States, X-Mode (under the proposed order) may still collect and sell their precise location data—where they visit family, where they pray, and whether they work on a military installation. Indeed, X-Mode has a presence around the globe and claims to be one of the largest providers of location data in the UK.[25]

The surveillance model espoused by data brokers like X-Mode targeting consumers in the United States does not stop at the water's edge; neither should the protections for those consumers. Just as with location data collected inside the United States, the fact that a data broker sells precise location data collected outside the United States to government contractors for national security purposes is material to an American consumer's decision to grant or revoke location permissions to various apps when traveling or living outside the United States (and indeed, material to the decision to use those apps in the first place). We urge the Commission to apply consistent rules to consumers' sensitive personal information that is collected and sold to government agencies and their contractors, regardless of where that information is collected.

### III. Conclusion

EPIC, Demand Progress, and EFF commend the Commission for taking enforcement action against X-Mode and for protecting consumers from the harmful practices of location data brokers. Additionally, we encourage the Commission to revise the order to remove the distinction between sensitive and non-sensitive location data or, at a minimum, to broaden the scope of location data deemed sensitive; to remove exception (i) in Section II to tighten the prohibition on the use, sale, or disclosure of sensitive location; to rely on data minimization requirements rather than individual consent; and to ensure that consumers' location and other sensitive information is protected consistently, regardless of where that information is collected. Please feel free to reach out to EPIC Counsel Sara Geoghegan at geoghegan@epic.org if you have any questions.

---

[22] U.S. Dep't of State, *Consular Affairs by the Numbers*, https://travel.state.gov/content/dam/travel/CA-By-the-Number-2020.pdf (last updated Jan. 2020), (estimating 9 million Americans lived overseas as of FY 2019).

[23] *See* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[24] Complaint, *supra* note 2, at 8; *see* Proposed Order, *supra* note 10, at 8.

[25] Allison Schiff, *X-Mode Acquires Location Data Assets From UK-Based Location Sciences*, AdExchanger (Jan. 15, 2020), https://www.adexchanger.com/mobile/x-mode-acquires-location-data-assets-from-uk-based-location-sciences/.

Sincerely,

Electronic Privacy Information Center (EPIC)
Demand Progress
Electronic Frontier Foundation (EFF)