CENTER FOR DEMOCRACY & TECHNOLOGY

February 20, 2024
Via regulations.gov

Re: Center for Democracy & Technology Comments in response to the Federal Trade Commission's Proposed Consent Order with X-Mode Social, Inc., and Outlogic, LLC (X-Mode Social, Inc.; File No. 212 3038).

CDT files these comments in response to the Federal Trade Commission's (Commission's) proposed consent Order with X-Mode and Outlogic (hereinafter "X-Mode").[1] CDT is a nonprofit, 501(c)(3) organization dedicated to advancing privacy, consumer, and civil rights for all in the digital age.

CDT supports the Commission's efforts to protect people's privacy, including their location privacy, particularly in connection with data brokers' practices. In the proposed Order with X-Mode, the Commission would, among other things, require X-Mode to seek consent, or ensure third parties have received consent, for collecting and using Location Data, and would preclude X-Mode from using or sharing "Sensitive Location Data," which is Location Data that indicates an individual has visited a Sensitive Location. The Order also would require X-Mode to ensure recipients of its Location Data cannot associate that Location Data with certain locations like LGBTQ+ service providers, political or social demonstrations, and associate an individual with that individual's home. We urge the Commission to adopt this groundbreaking Order.

CDT has two primary concerns with the Order that the Commission should address, including in any future enforcement actions. First, the Commission should remove the exception to the ban on disclosure and use of Sensitive Location Data that allows converting Sensitive Location Data into non-Location Data. Second, the Commission should remove, or at the very least clarify, the security exemption.

I. The Commission should remove the exception to the ban on disclosure and use of Sensitive Location Data that allows converting Sensitive Location Data into non-Location Data.

Section II of the Order bans, among other actions, the disclosure and use of "Sensitive Location Data." The exception in subsection (i)(b), however, permits converting Sensitive Location Data into non-Location Data, at which point, there would be no limits on use of the data. Because this exception would lead to continued privacy harm, the Commission should remove it from this Order, and should not consider adding it to future orders.

The exception for converting data into non-Sensitive Location Data would continue to allow privacy violations. Under the Order, X-Mode would still be allowed to collect Sensitive Location Data, so long as the company converted that data into non-Location Data, such as inferring a

[1] 89 Fed. Reg. 3404, Jan. 18, 2024, https://www.federalregister.gov/documents/2024/01/18/2024-00928/x-mode-social-inc-public-comment (seeking comment on Proposed Decision and Order Re X-Mode Social, Inc., and OutLogic, LLC, https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf).

particular health care use or audience segment without Location Data attached, or associating the individual with a zip code instead of a GPS coordinate.

Converting Sensitive Location Data into non-Location Data can still allow for a variety of harms. Visits to types of sensitive places, even without location attached, is still sensitive information. The fact that a person visited a Planned Parenthood clinic, even without information that they visited a *specific* Planned Parenthood clinic at a specific address, is still private information that companies could use to infer many things about a person, especially pertaining to that person's health. The same is true with visits to, for instance, a church or a Methadone clinic. Information that can be inferred from visits to sensitive places would include, for instance, sexual orientation; religion and religious practices; medical conditions or procedures including substance use disorders, reproductive healthcare, or mental health counseling; parental status; activity in a labor union; and status as a survivor of domestic violence. Invasive uses of such data are not hypothetical, but directly reported, including, most recently, details of how Recrue Media used location data from Near to identify and target advertising to people who had visited 600 Planned Parenthood clinics.[2]

To avoid allowing these harms to continue, the Commission's enforcement orders should not allow data brokers to infer from Sensitive Location Data, and then sell or otherwise use, sensitive information about people. Therefore, the Commission should remove from this Order exception (i)(b) in Section II, and it should not consider including similar language in future orders.[3]

II. The security exemption should be removed, and if not removed, it should be clarified.

The Commission's complaint points out that X-Mode "failed to inform consumers that it would be selling data to government contractors for national security purposes" and that, "[b]y failing to fully inform consumers how their data would be used and that their data would be provided to government contractors for national security purposes, X-Mode failed to provide information material to consumers and did not obtain informed consent from consumers to collect and use their Location Data."[4] It also points out that X-Mode provided sample consumer notices to third-party app publishers that misled consumers about the purposes for which their Location Data might be used because those notices failed to indicate that their location data would be provided to government contractors for national security purposes. It also alleges that X-Mode was aware of that omission in the notices, but did not instruct the third party apps to correct the notices, did not terminate its relationships with those apps, and continued to use the data they

[2] Letter from Senator Ron Wyden to FTC Chair Khan and SEC Chair Gensler (Feb. 13, 2024), https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf.
[3] At the very least, these orders should ensure that any Sensitive Location Data program addresses harms associated with tying a person to a sensitive location, even without the specific address or GPS coordinate of that location being retained or shared. To effectively mitigate privacy harms, programs to selectively redact sensitive places from Location Data must be comprehensively and carefully developed and maintained. Nick Doty, *Selectively Redacting Sensitive Places from Location Data to Protect Reproductive Health Privacy*, CDT (Aug. 25, 2022), https://cdt.org/insights/selectively-redacting-sensitive-places-from-location-data-to-protect-reproductive-health-privacy.
[4] Complaint, X-Mode Social, Inc., and OutLogic, LLC, at 5, https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf.

provided. The Commission should assert jurisdiction to address these deceptive practices even though they relate to national security.

However, the proposed Order only partially addresses these problems identified in the complaint because the proposed Order exempts from the definition of location data any information that is collected outside the U.S. and is used for Security Purposes or for National Security purposes (collectively, the "security exemption") conducted by federal agencies and other federal entities.[5] The security exemption turns not on whether the location to which the data pertains is in the U.S., but rather on whether it was "collected" in the U.S. or abroad, and whether it is "used" for Security Purposes or National Security Purposes. This exemption is unclear, will be difficult to implement and is ill-advised. We urge that it be removed. If retained nonetheless, we urge that it be clarified.

The security exemption is unclear and is difficult to implement because the location at which data is collected is often unclear. It will therefore be difficult to determine whether data was collected inside the U.S. or abroad. For example, when a person in the U.S. uses a third party app that is based abroad and that collects the person's location information, is that a collection that occurred inside the U.S. because the person was physically present in the U.S., or did it occur abroad, where the location data was ingested into a database maintained abroad by that app? Moreover, location data seems to flow like a river among brokers of that data. They combine it with other data, repackage it and then sell it to, for example, X-Mode which then makes it available to contractors for national security purposes. Indeed, as the complaint points out, X-Mode gets location data primarily from third parties. Where it was "collected" may be unknown, making the security exemption difficult to implement because it turns on knowledge of where information was collected.

The security exemption is also unclear because it turns as well on whether data is "used" for Security Purposes or National Security Purposes. A particular piece of location data that X-Mode obtains may be used for both security and for non-security purposes. In such a case, does the exemption apply? Moreover, is X-Mode's disclosure of location data to a national security contractor considered to be a "use" of the data that falls within the security exemption, or does the restriction pertain only to X-Mode's own use of the data to service the security needs of federal agencies?

The security exemption is ill-advised because the place where location data was collected is irrelevant to whether X-Mode deceived consumers by failing to inform them that it would be selling the data to government contractors for national security purposes, by providing misleading consumer notices to third party apps, and by failing to instruct them to correct the notices. The relevant question is whether consumers in the U.S. were misled by X-Mode's failures. Every time a consumer in the U.S. read about how their location data was to be used in an X-Mode privacy notice, or in a privacy notice of a third party app that was based on the sample notice X-Mode provided the app, the customer was deceived regardless of whether the location data was collected in the U.S. or abroad. Moreover, even if the collection of the location

[5] The Order pertains, among other things, to Location Data, which is defined to include any data which tends to reveal the precise location of a consumer or of a mobile device. However, it exempts from this definition data "that is collected outside the United States and is used for (a) Security Purposes or (b) National Security Purposes conducted by federal agencies or other federal entities…"

data abroad triggers concern that the deceptive acts would involve "foreign commerce," the Commission still has jurisdiction because the deception caused reasonably foreseeable injury in the U.S.[6]

The security exemption is also ill-advised because it sends a message to people outside the U.S. that the FTC will not police misleading statements about Location Data companies collect outside the United States even when it has jurisdiction to address those misleading statements on account of their impact in the U.S. This sentiment is contrary to the assurances that the Commission has provided European policy makers in connection with the EU-US Data Privacy Framework. In a June 9, 2023 letter to the European Commission, the Chair of the Commission pointed out that the "U.S. privacy landscape" of which the Commission is an enforcer "also protects EU consumers in a number of ways."[7] The letter properly points out that when the Commission acts to address deceptive acts or practices that are reasonably likely to cause foreseeable injury in the U.S., or that involve material conduct in the U.S., remedial action it can take to protect domestic consumers can inure to the benefit of foreign consumers. Exempting the collection abroad of Location Data that is deceptively shared for security purposes from the proposed Order runs counter to the spirit of this assurance.

We urge the Commission to remove the security exemption from the Order and to refrain from including a security exemption in future orders regarding location data when deceptive acts relating to that data are reasonably likely to cause foreseeable injury in the U.S., or involve material conduct in the U.S. If the Commission nonetheless chooses to retain the security exemption, it should clarify the exemption.

Conclusion

CDT supports the Commission's efforts to crack down on the collection, use, and disclosure of location data by data brokers. The proposed Order is worth finalizing, though the Commission should consider, now and in the future, making the changes recommended above.

Respectfully Submitted,

Eric Null
Co-Director, Privacy & Data Project
Greg Nojeim
Senior Counsel and Director, Security & Surveillance Project
Center for Democracy & Technology

[6] 15 U.S.C. § 45(a)(4).
[7] Letter from FTC Chair Khan to Didier Reynders, Commission for Justice of the European Commission, June 9, 2023, at 2, https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.08letter-to-commissioner-reynders.pdf.