epsilon
life sciences

CLIENT ALERT

FTC Bans Mobile App Software Developer from Selling Sensitive Data, Requires Data Deletion

The Federal Trade Commission (FTC) recently announced the acceptance (pending final approval) of an agreement and consent order with X-Mode Social, which was rebranded as "Outlogic" in 2021, following a joint venture and transfer agreement. In this article, we will look at the background of the company's business, alleged violations of the FTC Act, and proposed obligations under the agreement and order. This includes takeaways for other organizations to consider in their privacy risk management programs as the FTC's active streak continues in 2024.

Background

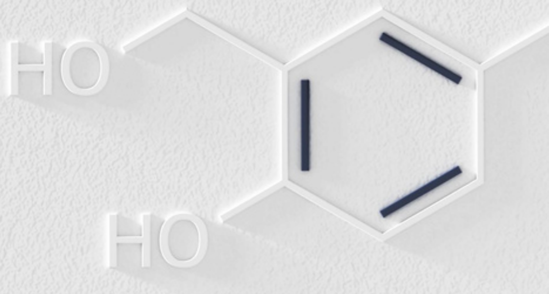
X-Mode's business includes providing a Software Development Kit (SDK) that mobile application developers at other companies could easily incorporate into their products. X-Mode's SDK (branded as "XDK") would collect precise geo-location information from users of apps on which it was installed, and in turn provide the companies publishing those apps with revenue from X-Mode based on the number of daily active users. The geolocation accuracy was described as, "70% accurate within 20 meters or less." X-Mode would enrich the device user and geolocation data with other sources and classifications it developed or purchased separately. This included matching businesses to latitude and longitude to segment users based on the type of places they might have visited. X-Mode would then license (sell) the raw or enriched data to companies for uses such as product development and marketing.

As of January 2021, X-Mode advertised a reach of 60MM monthly active users, representing 25% of the US adult population and up to 10% of users from countries including Canada, Mexico, Brazil, Japan, Australia, Singapore, the U.K., Spain, Italy, and France. In addition to the SDK and data licensing, X-Mode also developed their own apps, which was the company's original business before discovering the value of their location data. These included "Drunk Mode," which was advertised as a tool for inebriated individuals to manage their desired or undesired activities, and "Walk Against Humanity," which prompted users with snarky motivations related to their daily fitness activities.

Specific Allegations

The complaint alleged X-Mode unfairly engaged in the following violations under the FTC Act:

> Selling sensitive data: X-Mode's location data could easily be plotted to sensitive locations using publicly available map programs. This could include identifying specific healthcare facilities, places of worship, welfare organizations, or other locations that could infer sexuality, health conditions, or religious beliefs. Though X-Mode included in their customer terms that the data could not be used "to associate any user, device or individual with any venue that is related to healthcare, addiction, pregnancy or pregnancy termination, or sexual orientation…", the contractual terms were considered insufficient given the availability of additional data and ease of matching that data.



- Failing to honor consumers' privacy choices: Mobile devices include a unique identifier called a Mobile Advertiser ID (MAID). From 2013 – 2021, when Android device consumers enabled an option to "Opt-out of Ad Personalization," the MAID would still be sent to the mobile application but would include a flag that the user had opted out of the use for advertising. From June 2018 until July of 2020, X-Mode allegedly did not honor this flag and provided the data to marketers.
- Inadequate notice regarding collection and use of location data from apps: For certain periods until at least August 2020, X-Mode failed to disclose to users of its own apps (Drunk Mode and Walk Against Humanity) how location data would be used. The privacy notices indicated data would be shared with X-Mode customers for advertising, but did not disclose that the information was also sold to government contractors for national security purposes.
- Failing to validate whether app publishers gathered informed consent: X-Mode's primary mechanism or control for ensuring that third-party app publishers gathered consent was through contractual terms. The FTC considered this insufficient as additional methods for auditing could have been reasonably applied.
- Categorizing consumers based on sensitive characteristics for marketing purposes: X-Mode created custom audience segments based on sensitive data, including health information. In one example, X-Mode was contracted by a clinical research company to develop custom audiences of consumers who visited cardiology, endocrinology, or gastroenterology offices in Columbus, OH, or specific infusion centers and spent 30 minutes to one hour or more at those locations.
- Deceptive failure to disclose use of location data: The omission of the sharing and use of location data with government contractors for national security purposes was deceptive to users who would have otherwise reconsidered their use of the application or provision of consent.
- Providing the means and instrumentalities to engage in deceptive acts or practices: X-Mode primarily collects location data from third-parties who publish the XDK through their applications. This means X-Mode relies on those customers to provide notice and gather consent where required. X-Mode provided suggested language for those app publishers; however, it did not properly disclose how the geo-location data would be used in those templates, including use by government contractors for national security purposes.

Agreement and Order

The proposed order, pending approval, includes the following obligations which range from restrictions of certain activities, to requirements to develop new internal monitoring programs and processes onto the and deletion of data that is core to the company. The order is effective for 20 years and includes the following requirements:

- Prohibition from misrepresenting how it collects, uses, maintains, shares, and deletes information subject to the complaint, specifically, the extent to which data is de-identified.
- Prohibition from selling or sharing sensitive location data, including information related to health or medical, correctional, religious, labor union, childcare, minor education, racial or ethnic services, or social services facilities.
- Maintain a program to identify and manage where it collects sensitive data to ensure the prior obligations are followed.

- Create policies, procedures, and controls to prevent recipients of X-Mode location data from associating it with locations serving the LGBTQ+ community, social demonstrations, or identifying and individual's home.
- Notify the FTC if it becomes aware a third-party improperly shares location data provided by X-Mode.
- Only collect location data when a user has not opted-out of targeted advertising and maintains a record of consent for the collection. For their own apps' data, a quarterly reminder to users of the collection of location data must be furnished.
- Establish a supplier assessment program to conduct due diligence on new suppliers who install the XDK to ensure consumers are provided consent. This includes keeping records of such assessments and responses.
- Create a process for consumers to request and be informed of any entity, individual, or business with whom their location data has been shared. Alternatively, a method to delete the location data from X-Mode's customer databases with a written confirmation provided.
- Provide a simple process for consumers to withdraw consent and further collection to cease within 15 days of such a request.
- Document, maintain, and adhere to a retention schedule for relevant information. The schedule must be updated prior to collecting and using new information. This probably gives data governance teams heartburn.
- Delete location data unless the organization can demonstrate informed consent was attained or data has been de-identified.
- Establish, implement, and maintain a privacy program. This includes designating a qualified individual to oversee the program, conducting annual risk assessment, conducting effectiveness testing, and annual training and monitoring.
- Maintain records to demonstrate compliance with the order, respond to requests from the FTC, and provide periodic reports and attestations of compliance.

Takeaways

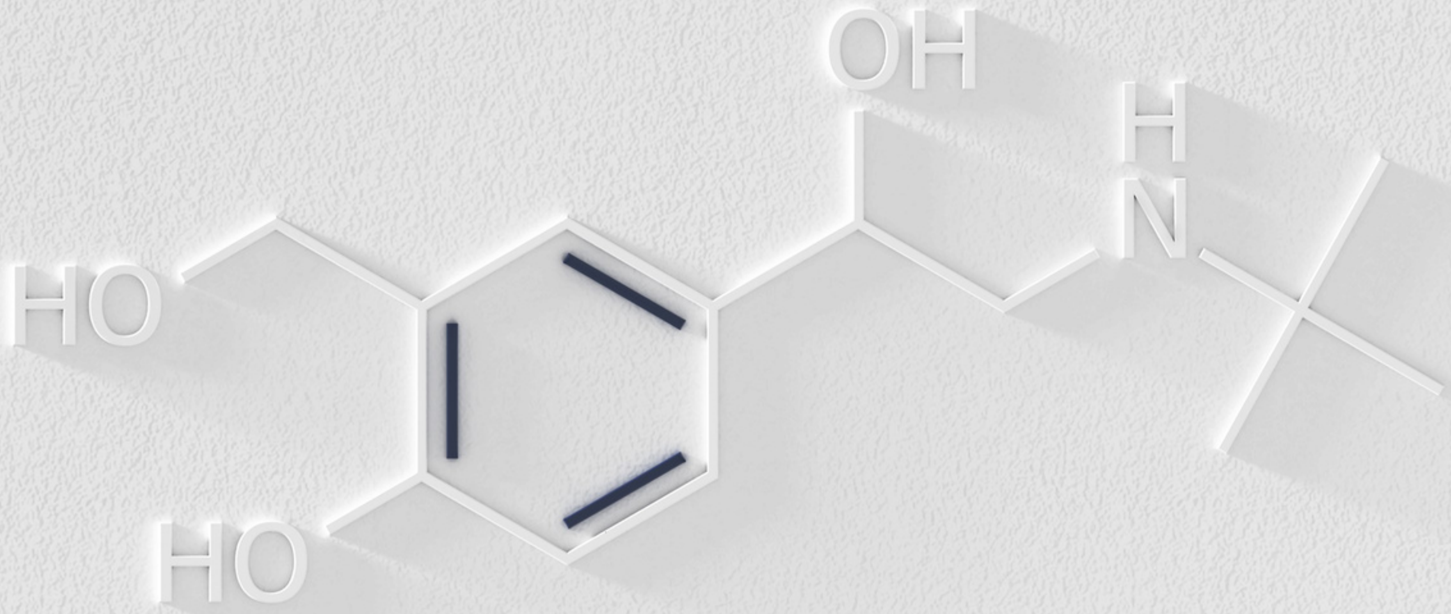
There is a lot to unpack and take away from this case for privacy, legal, compliance, security, product, marketing, and frankly, the C-suite. A few key items that can be applied to most organizations include the following at a minimum:

- The FTC is increasing its understanding of the technical workings of mobile applications, software development kits, and how data is proliferated across organizations. Privacy, security, development, marketing, legal, and compliance teams all need to know what mobile applications they maintain, what components are used to run those applications, and the data they generate and share.
- Geolocation information will likely continue to be a focus for the FTC, as made evident by other cases and statements in recent months. Alerting and educating your teams in product development, research, marketing, and related areas is important to start surfacing where this may need enhanced reviews.
- Know where you claim to be de-identifying data and conduct a thorough review of what practices could be applied to re-engineer identity.
- You cannot rely on contractual terms alone to shift risk. Reasonable auditing and monitoring should be applied.

- The FTC settlement obligations include some equivalent of a data inventory, data subject rights, and retention schedules. These parallels to obligations in the EU under the General Data Protection Regulation (GDPR) are notable and likely signals of U.S. commitment to bolster the transatlantic Data Protection Framework announced last year.
- Simply fixing a data or consent issue once it has surfaced is not the end of the line. Having data deleted from a revenue-generating product, marketing database, training dataset, or research data can be crippling to an organization and such risk should be considered when determining what information to collect and use.

How Epsilon Life Sciences Can Help

Epsilon Life Sciences' data, privacy, and cybersecurity team supports organizations and outside counsel with complex internal or regulatory investigations (e.g., FTC, OCR), class action privacy litigations, and independent monitorships related to data protection orders. The team has extensive experience working with organizations in healthcare, life sciences, technology, and other highly regulated and data-intensive industries to build, mature, and manage data protection programs.



Nick Weil, JD, CIPT
nweil@epsilonlifesciences.com
949.275.4578

Brian Segobiano, CIPP/E
bsegobiano@epsilonlifesciences.com
317.860.8025