Navigating Recent Enforcement Actions on Location Data

X-Mode Social, Inc.

The FTC's Complaint

- Announced in in January 2024. Asserted eight claims for violation of Section 5(a) of the FTC Act. Claims asserted against X-Mode and its successor, Outlogic LLC.
- FTC alleged that:
  - X-Mode, a data broker, acquired precise geolocation data of consumer mobile devices.
  - X-Mode processed billions of location signals each day and sold the data to clients.
  - X-Mode's location data, associated with MAIDs, could be used to track consumers to sensitive locations, including medical facilities, places of worship and domestic abuse shelters.
  - Raw data provided to customers was not anonymized—and could be used to track consumers to their home addresses.
  - X-Mode disregarded "flags" issued by Android for consumers who opted out of personalized advertising/tracking on their phones.
  - X-Mode did not obtain informed consent from consumers. Privacy notices provided in X-Mode's own apps did not fully disclose the purposes for which data was being collected (*e*.g., consumers not informed that data would be sold to government contractors for national security purposes).
  - X-Mode targeted consumers based on sensitive characteristics (*e.g.*, licensing location data of consumers who visited cardiology, endocrinology or gastroenterology offices in Ohio).
  - X-Mode exercised minimal control over downstream uses of data that it sold. In some cases, X-Mode sold data to customers who violated contractual restrictions on resale of the data.

In re X-Mode Social, Inc.

The Consent Order

- Entered on January 8, 2024.
- Notable provisions:
  - X-Mode banned from selling, licensing, transferring, sharing, disclosing, or otherwise using sensitive location data in any product or service—the first ban of its kind ever issued by the FTC.
  - X-Mode required to implement policies, procedures, and technical measures designed to prevent recipients of location data from associating the data with LGBTQ+ service organizations or political demonstrations/protests, and from using the data to identify the location of a person's home.
  - X-Mode required to develop a supplier assessment program to ensure that companies that provide location data to X-Mode/Outlogic are obtaining informed consent from consumers.
  - X-Mode required to delete all location data collected from users without their consent—and all audience segments created from that data.
  - X-Mode required to establish and implement a comprehensive "sensitive location data program" designed to prevent the use, sale, licensing, transfer, or disclosure of sensitive location data.

In re InMarket Media, LLC

The FTC's Complaint

- Announced in January 2024. Asserted four claims for violation of Section 5(a) of the FTC Act.
- FTC alleged that:
  - InMarket collected consumer location data through its SDK. InMarket also purchased consumer data from other aggregators.
  - Despite collecting vast amounts of sensitive location data, InMarket did not obtain informed consent from users in its proprietary apps.
  - The consent screens used for InMarket's proprietary apps told consumers that their location would be used for the apps' functionality (earning points and keeping shopping lists), which was misleading.
  - InMarket did not disclose that it collected consumers' precise locations and used that data to build detailed profiles for targeted advertising purposes.
  - InMarket did not require third-party apps to obtain informed consent from users before collecting their location data—general guidelines simply required app developers to "comply with all applicable laws," and maintain a "privacy policy in line with legal requirements."
  - InMarket retained sensitive, precise location data for five years—far longer than necessary to accomplish the stated purpose of collection (to allow users to earn shopping points or make shopping lists). Long retention period significantly increased risk that sensitive data could be disclosed, misused, or linked back to users.

In re InMarket Media, LLC

The Consent Order

- Entered on April 29, 2024.
- Notable provisions:
  - InMarket banned from selling or licensing precise location data in any product or service.
  - InMarket required to establish and implement a privacy program, and a comprehensive "sensitive location data program" designed to prevent the use, sale, licensing, transfer, or disclosure of sensitive location data.
  - InMarket required to obtain express affirmative consent from users—and document that consent—before collecting, using, maintaining or disclosing a consumer's precise location data.
  - InMarket required to delete all historical location data collected from users without their consent—and all audience segments created from that data.
  - InMarket required to provide a simple, easily-located means for consumers to withdraw any affirmative express consent granted in connection with the collection/use of precise location data.
  - InMarket required to provide a simple, easily-located means for consumers to request deletion of precise location data—and to delete/deidentify such data within 30 days if request is made.

US v. Kochava

The FTC's Complaint

- FTC sued Kochova in August 2022; the court dismissed without prejudice. The FTC filed an amended complaint in June 2023.
- The FTC alleged:
  - Kochava sold data based on millions of consumers' mobile devices, including:
    - Past physical locations derived from "precise" geolocation data
    - Names, addresses, mobile advertising IDs, email addresses and phone numbers
    - Personal traits including age, ethnicity and gender
    - Religious and political affiliations as well as education level
    - Marital, parental and economic statuses, including yearly income and "economic stability"
    - "App affinity" (defined as apps installed on consumers' phones) as well as their "interests and behaviors"
  - Kochava's sale of geolocation data puts consumers at significant risk. The data allows purchasers to track people at sensitive locations that could reveal information about their personal health decisions, religious beliefs, and steps they are taking to protect themselves from abusers.
  - Kochava fails to adequately protect its data from public exposure. Until at least June 2022, Kochava allowed anyone with little effort to obtain a large sample of sensitive data and use it without restriction.

Key Takeaways

- FTC not just concerned about data brokers and "selling" of location data
- Move toward complete prohibition on use of sensitive location data (even with disclosures)
- Continued trend of "unfairness" claims
- Necessity of third-party oversight
- Aggregation alone may not be sufficient to protect individuals' privacy

Strategies

- Anonymization/Aggregation
- Transparency

GRAVEYARD

X-Mode Social, Inc.

Background: X-Mode's Business

- X-Mode, a data broker, acquired precise geolocation data of consumer mobile devices.
- Location data was obtained through various channels—using X-Mode's software development kit to collect data from third-party apps; purchasing data from aggregators; collecting data through X-Mode's proprietary apps.
- X-Mode processed billions of location signals each day and sold the data to clients. Clients included advertisers, SaaS companies, analytics firms, research organizations and government contractors.
- Primary products:
  - Data as a Service: delivered raw location data, including unique mobile advertiser IDs ("MAIDs") and timestamped geolocation coordinates.
  - Audience Segments: divided MAIDs into specific categories. Consumers would be categorized by similar interests/other characteristics based on the locations that they visited (*e.g.*, "Size Inclusive Clothing Stores," "Veterans of Foreign Wars").
- X-Mode did not restrict the collection of location data from sensitive locations such as healthcare facilities, churches, and schools. Customer contracts included some restrictions on use of sensitive location data (*e.g.*, prohibiting customers from linking users to venues associated with drug treatment, sexual orientation or pregnancy termination).

InMarket Media, LLC

Background: InMarket's Business Model

- InMarket is a digital marketing platform and data aggregator that collected consumer location data through its software development kit. InMarket also purchased consumer data from other aggregators.
- InMarket obtained data from consumers—including location data, purchasing history, and demographic/socioeconomic information—and used the data to target advertising to consumers on their mobile devices on behalf of clients. Clients included brands and advertising agencies.
- InMarket displayed the targeted advertising using the InMarket SDK, and also categorized consumers into "advertising audiences" for use by clients (*e.g.*, "low-income millennials;" "well-off suburban moms;" "healthy and wealthy;" "wealthy and not healthy").
- InMarket SDK was incorporated into two InMarket apps—CheckPoints, which offered shopping rewards for completing tasks like watching videos—and ListEase, which allowed consumers to create shopping lists.
- InMarket also made its SDK available to third party app developers. App developers received a portion of InMarket's advertising revenue from each ad served through their apps.
- Until the FTC's recent action, InMarket would retain the location data that it collected for up to five years.