Navigating Recent Enforcement Actions on the Use of Location Data

May 2024

Laura Belmont, Civis Analytics

Marissa Boynton, Latham & Watkins

Section 5(a) of the FTC Act

"unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful"

Deceptive

Involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances

Unfair

Causes or is likely to cause substantial injury to consumers which is not readily avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition

Recent FTC Enforcement Actions

These actions impact data brokers *and* non-data brokers.

Key Allegations

U.S. v. Kochava

- Sold large amounts of data that could be used to track consumers to sensitive locations and homes
- Lack of control on downstream uses of data sold

In re X-Mode Social, Inc.

- Sold data that could be used to track consumers to sensitive locations and homes
- Disregarded opt-outs
- Did not get informed consent
- Targeted consumers based on sensitive characteristics
- Lack of control on downstream uses of data sold

In re InMarket Media, LLC

- Used consumers' precise location data to build sensitive targeting profiles for advertising
- Did not get informed consent
- Did not require app providers to obtain informed consent
- Retained data longer than necessary

Key Provisions in Consent Orders

In re X-Mode Social, Inc. (1/8/2024)

- Banned from using, selling, licensing, disclosing sensitive location data in any product or service
- 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
- Required to develop a supplier assessment program
- Required to establish and implement a comprehensive "sensitive location data program"

In re InMarket Media, LLC (4/29/2024)

- Banned from selling or licensing precise location data in any product or service
- Prohibition on using, selling or licensing products or services that categorize or target consumers based on Sensitive Location Data
- Required to develop a supplier assessment program
- Required to establish and implement a privacy program and "sensitive location data program"

What's Not New

- Transparency
- Respect users' privacy choices
- Opt-ins and opt-outs to processing of sensitive personal data (including location data)
- Implement data retention policies

What's New

- Prohibition on use, sale, and disclosure of sensitive location data (even with transparency)
- Inherent unfairness of the use, sale or disclosure of sensitive location data
- Third-party oversight
- Enforcement based on lack of retention policies

States - Sensitive Data

Personal information that reveals:

- a consumer's precise geolocation
- (generally), a consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, medical conditions, sexual orientation or union membership

FTC - Sensitive Location Data

Location associated with:

(1) sexual and reproductive health care providers, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, psychiatric and substance abuse hospitals, offices of oncologists, and offices of pediatricians; (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations held out to the public as predominantly providing education or childcare services to minors; (6) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; (7) locations held out to the public as predominantly providing services based on racial or ethnic origin; (8) locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (9) locations of public gatherings of individuals during political or social demonstrations, marches, and protests

States Approach to Sensitive Data

Opt-out: Limit to use which is necessary to perform services or what is reasonably expected by consumer

Opt-in: Cannot process sensitive personal data without the consumer's consent

FTC Approach to Sensitive Data

Historically: Separate and apart notice to collection, use, disclosure of sensitive data

Now: Complete ban?

If inherently unfair, will a use, sale or license of sensitive location data ever survive scrutiny?

Compliance Obligations

DSAR requests; Opt-in/opt-out sensitive data requirements (state privacy laws)

Implement data retention policies (state privacy laws/FTC)

Monitoring of vendor's collection of sensitive location data and client's usage of sensitive location data (FTC)

Contracts / Compliance

Vendor Side

- Diligence process / questionnaire for data brokers
- Confirm informed consent for use of data collected

Client Side

- Adequate use restrictions
- Right to audit compliance / certify compliance with use restrictions

Is this just the beginning?

What

Demographic predictive models / list cutting not based on location data

---

Non-sensitive location data

Ad-tech, if browsing and location data is sensitive "full stop"

What should companies start doing today?

Review and enhance existing privacy program controls

Assess whether and how use sensitive location data

Diversify your data strategy