FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Business Blog

Protecting consumers' location data: Key takeaways from four recent cases

By: Bhavna Changrani | December 4, 2024

Since the start of this year, the FTC has announced four groundbreaking cases addressing issues with how businesses collect and, in some cases misuse, people's location data. If your business collects, buys, sells, or uses location data, take a minute to read about the FTC's most recent enforcement actions against data brokers and aggregators — Mobilewalla, Gravy/Venntel, InMarket, and X-Mode/Outlogic — and consider these takeaways:

Location data is sensitive personal information. In all four complaints, the FTC says data aggregators collected billions of location data points linked to unique persistent identifiers and timestamps that could offer insights into people's movements. Unique persistent identifiers make it easy to match someone's movements with other personally identifiable information (PII) — like their name, address, or email address — from publicly available materials or other data brokers. Location data is sensitive personal information. Given the sensitivity, if you collect or sell it, you must protect it carefully.

Certain sensitive location data should never be used or sold. The FTC claims that each of the companies involved in these four complaints unfairly sold location information revealing people's visits to particularly sensitive locations, like medical facilities and places of worship. In Mobilewalla and Gravy/Venntel, the FTC also alleged the companies unfairly targeted people based on sensitive characteristics. Certain location information is so sensitive that it requires heightened protections. This could include information about visits to or stays at the following locations: medical facilities, religious organizations, correctional facilities, labor union offices, locations providing services to LGBTQ+ individuals, locations of political demonstrations, locations providing education or childcare to minors, racial or ethnic organizations, locations providing shelter or social services, and military installations, offices, or buildings. In most instances, businesses should not use or sell this data at all.

Get people's permission and monitor the companies you work with. When it comes to location data, make sure you have consent from every person for every applicable use. Whether you collect consent directly or rely on third parties, you must ensure people provide informed consent before using their location data. Check out the four complaints for methods of obtaining or verifying consent that the FTC alleges were inadequate. For example, you shouldn't get a person's consent to use their data for one purpose, while concealing or conveniently disregarding other purposes for which you intended to use the data. You must verify a person's informed consent for the specific collection of location data for the purpose you will be using their data, even when the person's consent was obtained through a third party. Vague contract provisions with no oversight or monitoring of vendors' compliance does not constitute verification. And think about how you'll monitor the companies you're selling data to, not just the companies you buy data from. Do your contracts include strict restrictions on how recipients of data can use it? How will you use technical means to detect misuse, vigilantly monitor compliance, and terminate relationships for lack of compliance?

Transparency is key. If you collect and sell location data, build trust with consumers through transparency in your business practices. For example, publicly disclose a retention schedule that explains the purposes you're collecting people's information for, your business reasons for keeping the data, and an established, reasonable timeframe for deleting it. Don't forget to provide easy ways for people to withdraw their consent for the collection and use of their location data, to request the deletion of any location data previously collected, and to request the identity of anyone to whom their data has been sold or shared.

Assess your risks, and establish and maintain a robust privacy program designed to protect location data and other personal information. The orders against Mobilewalla, Gravy/Venntel, InMarket, and X-Mode/Outlogic seek to ensure the companies comply with the law. In addition to requiring them to tell the truth about how they handle people's information — including the extent to which location information is deidentified — the orders require the companies to design, implement, maintain, and document safeguards to protect the personal information they handle. If you collect and sell people's data, check out the orders to make sure your own privacy program checks all the boxes. And, while you're at it, ensure you have tools in place to honor people's choices to opt-out or delete location data. Here are some questions to consider as you assess your risks:

- Do you have consent to collect, use, and sell location data?
- Do you filter out visits to sensitive locations?
- Do you disclose how long you keep location data? Do you keep data longer than necessary?

- Do you honor people's opt-out preferences?
- Do you have a robust privacy program?

If the answer to any of these questions is "no," now's the time to right the ship.

Tags: Consumer Protection | Bureau of Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

Comments closed.

More from the Business Blog

Business Blog

Concerned about deceptive earnings claims? So's the FTC, and we want your feedback

Julia Solomon Ensor | January 13, 2025

Business Blog

Look who's covered: the amended TSR and tech support scams

Karen S. Hobbs | December 19, 2024

Business Blog

Food for thought: The FTC's proposed settlement with Grubhub

Julia Solomon Ensor | December 17, 2024

Business Blog

Getting to the bottom line: The FTC's bipartisan Junk Fees Rule and your business

Julia Solomon Ensor | December 17, 2024