FTC Continues enforcement focus on the sharing of precise geolocation data

On December, 3, 2024, the Federal Trade Commission (FTC) announced settlements with two more data brokers that collected and sold consumers' precise geolocation data, Gravy Analytics and its subsidiary Venntel, and Mobilewalla.



Similar to the FTC's prior cases against InMarket and X-Mode, the FTC found that both Gravy Analytics and Mobilewalla collected and sold precise location information tied to individual consumers or devices that could be used to track consumers to sensitive locations, such as places of worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, political activity, and welfare and homeless shelters. In both cases, the FTC alleged that the companies violated the FTC Act by unfairly collecting and selling consumers' sensitive location data without verifying that consumers consented to such collection and sale, and by categorizing consumers into sensitive audience segments (such as medical conditions, political activities, and religious beliefs) inferred from location data and selling those inferences to third parties or using them for targeted advertising. The FTC also alleged that Mobilewalla violated the FTC Act by collecting consumer data from RTB exchange bidding when it did not have the winning bid, and by retaining consumer location data indefinitely.

The negotiated settlement orders (Orders) prohibit the parties from selling consumers' precise location data associated with a sensitive location, except for national security or law enforcement purposes, and to develop a compliance program to ensure these sensitive locations are excluded from their databases. The parties are also required to implement a supplier assessment program to ensure suppliers obtained consumer consent, provide mechanisms for consumers to exercise privacy rights, including to obtain the identities of third parties to whom the company previously sold the consumer's location data, to withdraw consent for the use or disclosure of location data, or to request deletion of location data. The parties must delete or destroy historic location data and inform third parties to whom historic location data was sold in the past 3 years to delete such data.

In addition, there are three significant take-aways from these recent cases that could have broader implications:

1. It is imperative to conduct adequate due diligence on data suppliers.

In both cases, the FTC found the parties violated Section 5 by unfairly collecting and using consumers' location data without taking reasonable steps to verify that consumers provided informed consent for the consent for the collection, use or sale of the location data.

Gravy and Mobilewalla did not collect location data directly from consumers but obtained most data through third party data aggregators. They made some effort to query their data supplier's collection practices, but the FTC found that neither party's efforts were sufficient to verify that consumers provided informed consent. According to the complaint, Gravy provided a survey to its data suppliers and asked for copies of the consent disclosures presented to consumers but continued to use suppliers who failed to respond or who provided ambiguous or non-responsive responses. Even when Gravy verified that consumers had provided consent for an app to collect and use location data for certain purposes (e.g., consent to collect location data to "locate nearby stores," or "for marketing, ad targeting or predictive modeling and analytics purposes,") the FTC found such consent was not sufficient to verify that consumers were adequately informed that their location data could be used for commercial and government purposes.

The FTC alleged Mobilewalla's verification practices to be similarly lacking. According to the complaint, Mobilewalla



conducted minimal vetting when onboarding a new data supplier; at most, it checked a fraction of a supplier's apps to confirm they disclosed location data sales, but never checked again after onboarding the supplier. Mobilewalla did not contractually require suppliers to obtain consumer consent, merely relying on vague assurances that suppliers' sale of data "complied with applicable law." The company asked suppliers to certify annually that they had obtained the consumers' consent to collect and sell location data, but did not take any steps to verify the accuracy of those certifications. Even when Mobilewalla determined an app did disclose to consumers that the app collected and sold location data, this disclosure was insufficient to verify that consumers consented to the various purposes for which Mobilewalla used location data, including, marketing, commercial, and government purposes.

Under the terms of the Orders, Mobilewalla and Gravy must establish a Supplier Assessment Program. Among other things, this program will include conducting an initial assessment, and annually thereafter, designed to confirm that consumers provide affirmative express consent to the collection, use and disclosure of all data that may reveal a mobile device's or a consumer's precise location.

To quote Commissioner Ferguson, "Data brokers that purchase sensitive information cannot avoid liability by turning a blind eye to the strong possibility that consumers did not consent to its collection and sale."

2. Collection and use of consumer location data gathered from RTB exchange is an unfair practice.



In addition to purchasing data from data aggregators, Mobilewalla amassed large quantities of data collected from real time bidding exchanges (RTB exchanges). When Mobilewalla bid to place an advertisement through an RTB auction, it collected and retained the information in the bid request even when it did not have the winning bid, in violation of the contractual terms of the exchange disallowing such collection and retention. Bidstream data often contained a device MAID and precise geolocation data, as well as other personal data, which Mobilewalla combined with other datasets. Mobilewalla used this bidstream data for advertising as well as non-advertising purposes, also in violation of the exchange terms. Specifically, the complaint alleged that Mobilewalla used bidstream data to geofence the home addresses of a customer's employees, health care centers, and to track union organizing. Mobilewalla also sold this data to third parties, in datasets that included the MAID as well as locations associated with that device and the names of the apps from which the data was collected (some of which revealed sexual orientation or other sensitive information). Finding that "Mobilewalla exploited vulnerabilities in digital ad markets to harvest this data at a stunning scale," the FTC found that this practice was likely to cause substantial consumer injury in the form of loss of privacy and increased risk of public or harmful disclosure of sensitive information about consumers' private lives. This case marks the first time the FTC has alleged that the practice of collecting, retaining and using consumer data from the RTB bidstream was an unfair act under Section 5.

As part of the Order, Mobilewalla will be banned from collecting consumer data from online advertising auctions for purposes other than participating in those auctions.

3. Indefinite retention of location data is an unfair practice.

The complaint alleged that Mobilewalla retained sensitive consumer information indefinitely, advertising that it had collected over "50B mobile signals daily" from "2.2B devices" and stores "5+ years of data," and that this indefinite retention of location history exposed consumers to significant harms including stalking, targeted scams, and a variety of reputational harms.

Under the terms of the Orders, both Gravy and Mobilewalla are required to create, implement and publish a data retention schedule, setting forth the purposes for which each type of data is collected or used, the time frame for deletion. The length of the permissible data retention period is not specified by the Orders, other than to state that in no instance should any type of data be retained indefinitely.



Commissioners' statements in location data cases may foreshadow trends for future FTC enforcement

The Republican Commissioners, one of whom is the new FTC Chair, Published Statements (link and link) criticizing certain aspects of these decisions.

The Commissioners appear aligned that the sale of precise geolocation data that reveals visits to sensitive locations without consumers' knowledge and consent is an unfair practice, and broadly agree on the need to conduct sufficient due diligence on data vendors.

But, both Commissioners Ferguson and Holyoak raise doubts as to the illegality of inferring sensitive characteristics derived from location data and using those characteristics for targeted advertising. Ferguson sharply criticized the FTC's "purely subjective" list of so-called "sensitive" characteristics that could embarrass the consumer or expose private information. In Ferguson's view, the FTC should focus on the lawfulness of the initial collection of the data; if the location data was collected with transparency and consumer consent, the FTC should not limit how someone downstream may lawfully acquire that data and what conclusions they may draw from it. Similarly, Holyoak argued, "there is nothing intrinsically unfair about … categorizing consumers based on sensitive characteristics derived from location data," and even expressed her support for certain types of targeting based on sensitive health characteristics, such as targeting pregnant women with ads for pregnancy crisis centers.

Commissioner Holyoak also strongly disagreed with the Mobilewalla count related to the collection of RTB bidding data. She argued that a violation of a commercial contract is not alone sufficient to support a Section 5 claim and criticized the majority for failing to explain how the mere collection of consumer data from the bidstream could cause consumer injury. Holyoak does not go so far as to say that collecting and using bidstream data could never give rise to a violation, one could surmise that Holyoak wants to see more evidence of specific consumer harm before finding a practice to be inherently unfair. Ferguson agreed that a contractual violation is not *per se* unfair, but because these contractual terms protected consumers from the risk of having private data sold without their consent, Mobilewalla's breach of contract exposed consumers to the same substantial risk of injury as the collection of their data without consent, and therefore violates Section 5.

Both Commissioners also strongly disagreed with the indefinite retention count in Mobilewalla, because nothing in Section 5 forms the basis of a standard data retention obligation. Commissioner Holyoak even argued there could be countervailing benefits to justify Mobilewalla's retention of data indefinitely and criticized the majority for failing to conduct that analysis.

Finally, Commissioner Holyoak criticized "the Majority's continued efforts to deem targeted advertising an unfair practice under Section 5." Holyoak offered a general defense of the digital advertising industry, enumerating examples of where audience segmentation or behaviorally targeted ads can offer pro-consumer benefits.

These views could reflect a new direction in enforcement priorities once Commissioners Ferguson and Holyoak are in the majority.

FTC turns to vehicle telematics data



Continuing with the precise geolocation theme, the FTC announced a negotiated settlement with General Motors (GM) and its affiliate OnStar in January 2025 for allegedly failing to obtain affirmative express consent from drivers prior to collecting, using, and selling the driver's precise geolocation data and driving behavior data from GM vehicles enrolled in OnStar programs. According to the allegations in the complaint, GM did not adequately disclose to consumers the type of information that would be collected through the OnStar programs, nor that the data would be compiled and sold to third parties. Once enrolled, GM collected and sold precise geolocation and movement data to a third party for transportation planning, infrastructure construction and advertising analytics. GM also sold location and driving behavior insights derived from vehicle telematics (such as hard braking and speeding events) to consumer reporting agencies and insurance carriers. The FTC alleged that this practice has led to consumers being denied auto insurance coverage or having their insurance premiums increased.

Under the terms of the Order, GM is banned from disclosing driver data to consumer reporting agencies for 5 years. Further, GM must obtain the consumer's affirmative express consent prior to collecting, using or disclosing driver data to any third party, with limited exceptions for emergency response services among others. The consent must include providing a clear disclosure of the categories of data that will be collected, the names or categories of third parties receiving the information, and the purposes for which the data is collected or used. GM must obtain affirmative express consent for each separate, unrelated service or feature that collects or uses driving data and must provide an easy mechanism to allow a consumer to withdraw consent. GM must also develop and implement a data retention schedule (similar to the relief in Mobilewalla and Gravy Analytics cases), develop a mechanism for consumers to request to access or request deletion of their driver data, and must allow consumers to disable the collection of location data from the vehicle.

In other news:

- **FTC continues to pursue artificial intelligence (AI) enforcement cases, primarily under deceptive advertising theories.** In December 2024, the FTC entered a settlement order against Intellivision, a company that sells facial recognition software used in home security systems and smart home solutions. According to the complaint, the company allegedly lacked substantiation to support its marketing claims touting the product's high accuracy rates, lack of gender bias, protection against spoofing, and the size of the dataset used for training. This is not the first time the FTC has used the deceptive practices prong of Section 5 to exert limits on the AI industry, and it certainly won't be the last. Companies offering AI tools should avoid exaggerating what AI products can do, and ensure there is competent, reliable support for all advertising claims made about the efficacy of the technology.
- **Unfair advertising and promotional practices for children and teens (13-18).** Even in the absence of Federal Children's Online Safety law, the FTC continues to penalize companies for engaging in unfair business practices when dealing with teens 13-18. The FTC's $20M settlement with game developer Cognosphere, maker of "Genshin Impact" in January 2025, penalized the company for collecting data from children under 13 in violation of the Children's Online Privacy Protection Act (COPPA), and for unfairly aggressive marketing techniques and dark patterns (including the use of count-down timers, false scarcity, and loot boxes) directed to children and teens under 18. The settlement order requires, among other things, the operator to obtain affirmative parental consent before "early teens" age 13-15 can make purchases in the app.

This is at least the third case the FTC has pursued against an operator for unfair and deceptive practices involving teens and minors over the COPPA age cut-off. The case against NGL Labs (July 2024) found the company unfairly marketed its anonymous messaging app to teens because of the likelihood it could cause substantial injury in the form of cyberbullying, harm to mental health, etc. In 2022, the FTC found that Epic Games allegedly engaged in unfair practices by allowing real-time voice and text communications for kids and teens as a default setting, and that its in-app purchase practices allowed kids and teens to accrue unauthorized charges violated ROSCA.

- **Data Clean Rooms: separating fact from fiction blog post (**link**)**. In a November 2024 blog post, the FTC warned that data clean rooms and other privacy-enhancing technologies "alone can't protect privacy and even if they address some privacy risks, they can contribute to others."

Authors



Emily Tabatabai
Partner
Orrick



Sundeep Kapur
Partner
Orrick