



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Technology Blog

FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket

March 4, 2024



Three recent FTC enforcement actions reflect a heightened focus on pervasive extraction and mishandling of consumers' sensitive personal data.

Proposed Settlements with [Avast](#)^[1], [X-Mode](#)^[2], and [InMarket](#)^[3]

In mid February, the FTC announced a proposed settlement to resolve allegations that Avast, a security software company, unfairly sold consumers' granular and re-identifiable browsing information—information that Avast amassed through its antivirus software and browser extensions after telling consumers that Avast's software would protect their privacy, and that any disclosure of their browsing information would only be in aggregate and anonymous form.

In January of this year, the FTC announced proposed settlements with two data aggregators, X-Mode Social and InMarket, to resolve a host of allegations stemming from how those companies handled consumers' location data. Both companies, the FTC alleged, collected precise location data from consumers' phones through the data aggregators' own mobile apps and those of third parties (via software development kits, or "SDKs," provided by the data aggregators). X-Mode, the FTC alleged, sold consumers' location data to private government contractors without first telling consumers or obtaining consumers' consent to do so. And InMarket, the agency alleged, used consumers' location data to sort them into particularized audience segments—like "parents of preschoolers," "Christian church goers," "wealthy and not healthy," etc.—that InMarket then provided to advertisers.

Taken together, these matters reflect several common themes that highlight serious privacy threats imposed on consumers by business models that monetize people's personal information.

Give Feedback

1. Browsing and location data paint an intimate picture of a person's life, including their religious affiliations, health and medical conditions, financial status, and sexual orientation.

The FTC's proposed complaint against Avast alleges that a sample of just 100—of the trillions—of data points maintained by Avast showed visits by people to the following websites: an academic paper on a study of symptoms of breast cancer; Sen. Elizabeth Warren's presidential candidacy announcement; a CLE course on tax exemptions; government jobs in Fort Meade, Maryland with a salary greater than \$100,000; a link (then broken) to the mid-point of a FAFSA (financial aid) application; directions on Google Maps from one location to another; a Spanish-language children's YouTube video; a link to a French dating website, including a unique member ID; and cosplay erotica.

X-Mode, the FTC alleges, ingested more than 10 billion location data points—which the company advertised as being 70% accurate within 20 meters or less—that were linked to timestamps and unique persistent identifiers. Plotting this data on a map reveals each person's movements, and the unique persistent identifiers make it easy to sync up a person's movements with information—like each person's name, email address, etc.—from publicly available sources or other data brokers.

Similarly, the FTC's proposed complaint against InMarket alleges the company collected the precise geolocation information from 100 million unique devices each year from 2016 to the present, and cross-referenced these location histories with points of interest to identify consumers who had visited particular locations.

Browsing and location data are sensitive. Full stop. None of the underlying datasets at issue in the FTC's proposed complaints against Avast, X-Mode, or InMarket are alleged to have contained people's names, social security numbers, or other traditional standalone elements of personally identifiable information (or "PII"). Indeed, the FTC's proposed complaint against Avast acknowledges Avast's use of a proprietary algorithm to find and remove these elements from its users' browsing data before selling it. What makes the underlying data sensitive springs from the insights they reveal and the ease with which those insights can be attributed to particular people.

Years of research shows that datasets often contain sensitive and personally identifiable information even when they do not contain any traditional standalone elements of PII,^[4] and re-identification gets easier every day—especially for datasets with the precision of those at issue in the FTC's proposed complaints against Avast, X-Mode, and InMarket. Accordingly, the FTC's proposed orders would require Avast, X-Mode, and InMarket to treat people's browsing and location information as the sensitive data that it is. These companies, for example, would be subject to bans prohibiting the

disclosure or use of browsing (Avast) and location (X-Mode and InMarket) information in various circumstances, and all three companies must establish and maintain robust privacy programs designed to protect their users' browsing (Avast), location (X-Mode and InMarket), and all other personal (all three) information.

2. People have no way to object to—let alone control—how their data is collected, retained, used, and disclosed when these practices are hidden from them.

Avast, the FTC alleges, claimed its browser extensions and antivirus software would “block[] annoying tracking cookies that collect data on your browsing activities” and “[p]rotect your privacy by preventing [...] web services from tracking your online activity.” But for years, the FTC alleges, Avast sold the very browsing information they promised to protect—often without any notice to users at all. Where Avast did describe its information practices, the FTC’s proposed complaint alleges Avast deceptively promised that any sharing would be in “anonymous and aggregate” form.

The FTC’s proposed complaint against X-Mode alleges in detail how the company misled people by asserting their location data would be used solely for “ad personalization and location-based analytics”—meaning consumers had no way to know that X-Mode also sold their location data to government contractors for national security purposes.

And as the FTC alleges in the proposed InMarket complaint, users of the company’s “CheckPoints” and “ListEase” apps had no way to know InMarket would collect their precise location information (often multiple times per hour) and combine it with data collected from multiple other sources to build extensive profiles for precise ad targeting because the apps’ consent interfaces only told people their data would be used for the app’s functionality:

- “Allow CheckPoints to access your location? This allows us to award you extra points for walking into stores” (CheckPoints app on iOS)
- “Allow Location Permissions to unlock reminders. Get a reminder when you’re in the store so you never forget to grab the items you need!” (ListEase app on Android)

Compounding the problem, the FTC alleges, were X-Mode’s and InMarket’s use of SDKs embedded in other developers’ apps to expand X-Mode’s and InMarket’s reach. When a developer incorporates a company’s code into their app through an SDK, that developer amplifies any privacy risks inherent in the SDK by exposing their app’s users to it. Often, such code may have location and other data tracking capabilities and, because the app developer is not the company that created the SDK, the app developer may not know how their users’ data will ultimately be stored, used, and disclosed. The

developer, however, will know if an SDK requires access to location permissions before they add the SDK to their app.

Purpose matters. Data handling must align with the purposes for which it was collected. Helping people prepare their taxes does not mean tax preparation services can use a person's information to advertise, sell, or promote products or services.^[5] Similarly, offering people a flashlight app does not mean app developers can collect, use, store, and share people's precise geolocation information.^[6] The law and the FTC have long recognized that a need to handle a person's information to provide them a requested product or service does not mean companies are free to collect, keep, use, or share that person's information for any other purpose—like marketing, profiling, or background screening.

The FTC alleges that Avast, X-Mode, and InMarket each ignored this basic principle, and the proposed orders seek to hold them to account. Under the proposed orders, for example, Avast will have to pay \$16.5 million (which the FTC plans to return to affected consumers), and all three companies will have to comply with substantial limits on how they handle people's browsing (Avast) and location (X-Mode and InMarket) data going forward—including provisions ensuring that people are able to actually consent to how their data is collected and used.

3. Any safeguards used to maintain people's privacy are often outstripped by companies' incentives and abilities to match data to particular people.

The value proposition for many data purchasers is often the same thing that exposes people's privacy: ever-more granular data, and the insights and inferences such data convey. Companies that sell or license data sometimes include language in their contracts prohibiting recipients from re-identifying the people in the data, or restricting how recipients use the data they buy. But not all contracts contain such prohibitions. Those that do are often still insufficient to maintain consumers' privacy, even when bolstered by technical safeguards.

As the FTC's proposed complaint against Avast alleges, some of the company's underlying contracts did not prohibit data buyers from re-identifying Avast users. Under one such contract, for example, the FTC alleges that an Avast subsidiary granted a company specializing in identity services a "world-wide license" to use Avast users' browsing information for "targeting, messaging and other data driven marketing activities served to consumers and businesses"—including "ID Syncing Services" and "Data Distribution Services." And even where Avast's underlying contracts included a re-identification prohibition, the FTC alleges that recipients were still permitted to match information with Avast users' browsing data so long as the information was not "personally-identifiable," and Avast never audited or otherwise confirmed that recipients complied with such prohibitions.

While the FTC’s proposed complaint against X-Mode recognizes that the company included some use restrictions in its contracts,^[7] even when paired with technical measures and auditing requirements, such use restrictions may not deter misuse by downstream actors. And at least twice, the FTC alleges, X-Mode sold location data to customers who violated restrictions in their contracts by reselling the data they bought from X-Mode to companies even further downstream.

Companies must do better. Honoring privacy promises and obligations means implementing and adhering to safeguards that actually maintain people’s privacy. Promises and contract clauses are important, but they must be backed up by action. Going forward, the FTC’s proposed orders against Avast, X-Mode, and InMarket seek to ensure these companies comply with the law. In addition to prohibiting Avast, X-Mode, and InMarket from misrepresenting how they handle people’s information—including the extent to which consumers’ browsing (Avast) and location (all three) information is aggregated or anonymized (Avast) or deidentified (X-Mode and InMarket)—the FTC’s proposed orders require these companies to design, implement, maintain, and document safeguards to protect the personal information they handle.

As these actions underscore, the FTC is committed to protecting people from the unlawful collection, retention, use, and disclosure of their information.

1. Browsing and location data are sensitive. Full stop.
2. Purpose matters: Firms do not have free license to market, sell, and monetize people’s information beyond purposes to provide their requested product or service.
3. Companies must do better: Safeguards used to maintain people’s privacy are often outstripped by companies’ incentives and abilities to match data to particular people. Firms should not let business model incentives that focus on the bottom line outweigh the need for meaningful privacy safeguards.

“Across these cases, we have established that businesses by default cannot sell people’s sensitive data or disclose it to third parties for advertising purposes,” Chair Khan emphasized in her statement^[8] accompanying the proposed Avast settlement. Collecting, storing, using, and sharing people’s sensitive information without their informed consent violates their privacy, and exposes them to substantial secondary harms like stigma, discrimination, physical violence, and emotional distress. The FTC will not stand for it. The Commission will use all of its tools to continue to protect Americans from abusive data practices and unlawful commercial surveillance.^[9]

Thank you to the attorneys who led the investigations, and to all who contributed to this post: Andy Hasty, Noam Kantor, Aaron Alva, Elizabeth Averill, Bhavna Changrani, Simon Fondrie-Teitler, Alex Gaynor, Julia Horwitz, Amritha Jayanti, Nick Jones, Kevin Moriarty, Gorana Neskovic, Stephanie Nguyen, Brian Shull, Ben Swartz, Cathlin Tully, David Walko, Ben Wiseman, and Daniel Zhao.

[1] FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay \$16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking (February 22, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over>.

[2] FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (January 9, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

[3] FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (January 18, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data>.

[4] See, e.g., Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, Estimating The Success of Re-Identifications in Incomplete Datasets Using Generative Models, 10 Nature Comm'ns 3069 (2019), available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6650473/>.

[5] Notice of Penalty Offenses Concerning Misuse of Information Collected in Confidential Contexts (Sept. 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/NPO-Misuse-Information-Collected-Confidential-Contexts.pdf .

[6] In the Matter of Goldenshores Technologies, LLC and Erik M. Geidl, FTC File No. 1323087 (2014), <https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3087-goldenshores-technologies-llc-erik-m-geidl-matter>.

[7] For example, purporting to restrict recipients from using “the X-Mode Data (alone or combined with other data) to associate any user, device or individual with any venue that is related to healthcare, addiction, pregnancy or pregnancy termination, or sexual orientation.”

[8] Statement of Chair Lina M. Khan, Joined by Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro M. Bedoya, In the Matter of Avast Limited Commission File No. 202-3033 (February 21, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2024.02.21StatementofChairKhanRegardingAvast.pdf .

[9] FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (January 9, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

Give Feedback

More from the Technology Blog

Technology Blog

[Consumer Facing Applications: A Quote Book from the Tech Summit on AI](#)

Staff in the Office of Technology | April 24, 2024

Technology Blog

[Data and Models: A Quote Book from the Tech Summit on AI](#)

Staff in the Office of Technology | April 17, 2024

Technology Blog

[Security Principles: Addressing Vulnerabilities Systematically](#)

The Office of Technology | April 17, 2024

Technology Blog

[Approaches to Address AI-enabled Voice Cloning](#)

FTC's Office of Technology | April 8, 2024

Give Feedback

Get Business Blog updates

Subscribe



Subscribe to Our Newsletter

Subscribe



ROB BONTA

Attorney General

Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act

Press Release / *Attorney General Bonta Announces Settlement with Sephora as ...*

Wednesday, August 24, 2022

Contact: (916) 210-6000, agressoffice@doj.ca.gov

Marks strong second year of CCPA enforcement with update on enforcement efforts and new investigative sweep of businesses failing to process opt-out request via a user-enabled global privacy control

OAKLAND – California Attorney General Rob Bonta today announced a settlement with Sephora, Inc. (Sephora), resolving allegations that the company violated the California Consumer Privacy Act (CCPA), California's first-in-the-nation landmark privacy law. After conducting an enforcement sweep of online retailers, the Attorney General alleged that Sephora failed to disclose to consumers that it was selling their personal information, that it failed to process user requests to opt out of sale via user-enabled global privacy

controls in violation of the CCPA, and that it did not cure these violations within the 30-day period currently allowed by the CCPA. Today's settlement is part of ongoing efforts by the Attorney General to enforce California's comprehensive consumer privacy law that allows consumers to tell businesses to stop selling their personal information to third parties, including those signaled by the Global Privacy Control (GPC).

“Technologies like the Global Privacy Control are a game changer for consumers looking to exercise their data privacy rights. But these rights are meaningless if businesses hide how they are using their customer's data and ignore requests to opt-out of its sale,” **said Attorney General Bonta**. “I hope today's settlement sends a strong message to businesses that are still failing to comply with California's consumer privacy law. My office is watching, and we will hold you accountable. It's been more than two years since the CCPA went into effect, and businesses' right to avoid liability by curing their CCPA violations after they are caught is expiring. There are no more excuses. Follow the law, do right by consumers, and process opt-out requests made via user-enabled global privacy controls.”

The settlement with Sephora underscores the critical rights that consumers have under CCPA to fight commercial surveillance. Consumers are constantly tracked when they go online. Many online retailers allow third-party companies to install tracking software on their website and in their app so that third parties can monitor consumers as they shop. These third parties track all types of data – in Sephora's case, the third parties could create profiles about consumers by tracking whether a consumer is using a MacBook or a Dell, the brand of eyeliner or the prenatal vitamins that a consumer puts in their “shopping cart,” and even a consumer's precise location. Retailers like Sephora benefit in kind from these arrangements, which allow them to more effectively target potential customers.

Sephora's arrangement with these companies constituted a sale of consumer information under the CCPA, and it triggered certain basic obligations, such as telling consumers that they are selling their information and allowing consumers to opt-out of the sale of their information. Sephora did neither.

Today's settlement requires Sephora to pay \$1.2 million in penalties and comply with important injunctive terms. Specifically, Sephora must:

- Clarify its online disclosures and privacy policy to include an affirmative representation that it sells data;
- Provide mechanisms for consumers to opt out of the sale of personal information, including via the Global Privacy Control;
- Conform its service provider agreements to the CCPA's requirements; and
- Provide reports to the Attorney General relating to its sale of personal information, the status of its service provider relationships, and its efforts to honor Global Privacy Control.

As part of his ongoing efforts to enforce CCPA, Attorney General Bonta also sent notices today to a number of businesses alleging non-compliance relating to their failure to process consumer opt-out requests made via user-enabled global privacy controls, like the GPC. A global privacy control allows consumers to opt out of all online sales in one fell swoop by broadcasting a "do not sell" signal across every website they visit, without having to click on an opt-out link each time. Under the CCPA, businesses must treat opt-out requests made by user-enabled global privacy controls the same as requests made by users who have clicked the "Do Not Sell My Personal Information" link. Businesses that received letters today have 30 days to cure the alleged violations or face enforcement action from the Attorney General. The CCPA's notice and cure provision, which requires businesses to receive notice and opportunity to cure before they can be held accountable by the Attorney General for CCPA violations, will expire on January 1, 2023.

Attorney General Bonta is committed to the robust enforcement of California's groundbreaking data privacy law. Since July 1, 2020, the Attorney General has issued notices to a wide array of businesses alleging noncompliance with the CCPA. Notices to cure have been issued to major corporations in the tech, healthcare, retail, fitness, data brokerage, and telecom industries, among others. New examples of notices to cure are available at oag.ca.gov/ccpa and include:

- An enforcement sweep of businesses operating loyalty programs that offered financial incentives such as discounts, free items, or other rewards, in exchange for personal information without providing consumers with a notice of financial incentive;
- An online advertising business that's privacy disclosures were not understandable to the average consumer and did not include the required information; and
- A data broker whose "Do Not Sell My Personal Information" link worked only on certain browsers and directed consumers to a confusing webpage that required several additional steps to submit CCPA requests.

For more information about the CCPA, visit oag.ca.gov/ccpa. To report a violation of the CCPA to the Attorney General, consumers can submit a complaint online at oag.ca.gov/report. Consumers can also directly notify businesses of potential violations using the Consumer Privacy Tool.

A copy of the complaint is available [here](#). A copy of the settlement is available [here](#).

#





FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data

FTC charges X-Mode and Outlogic with selling raw location data, failing to obtain informed consumer consent

Give Feedback

January 9, 2024 |   

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Big Data](#) | [Online Advertising and Marketing](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

Data broker X-Mode Social and its successor Outlogic will be prohibited from sharing or selling any sensitive location data to settle Federal Trade Commission allegations that the company sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship and domestic abuse shelters.

In its first settlement with a data broker concerning the collection and sale of sensitive location information, the FTC also charged that Virginia-based X-Mode Social and Outlogic, LLC, the successor firm to which X-Mode transferred most of its operations in 2021, failed to put in place reasonable and appropriate safeguards on the use of such information by third parties. Today's action underscores the FTC's strong commitment to restraining the collection, sale, or disclosure of consumer' sensitive location data.

"Geolocation data can reveal not just where a person lives and whom they spend time with but also, for example, which medical treatments they seek and where they worship. The FTC's action against X-Mode makes clear that businesses do not have free license to market and sell Americans' sensitive location data," said FTC Chair Lina M. Khan. "By securing a first-ever ban on the use and sale of

sensitive location data, the FTC is continuing its critical work to protect Americans from intrusive data brokers and unchecked corporate surveillance.”

The raw location data that X-Mode/Outlogic has sold is associated with mobile advertising IDs, which are unique identifiers associated with each mobile device. This raw location data is not anonymized, and is capable of matching an individual consumer’s mobile device with the locations they visited. In fact, some companies offer services that help companies match such data to individual consumers.

X-Mode/Outlogic sells and licenses precise location data that it collects from third-party apps that incorporate its software development kit (SDK) into their apps, from its own mobile apps, and by purchasing location data from other data brokers and aggregators. The company sells consumer location data to hundreds of clients in industries ranging from real estate to finance, as well as private government contractors for their own purposes, such as advertising or brand analytics.

According to the [FTC’s complaint](#) , until May 2023, the company did not have any policies in place to remove sensitive locations from the raw location data it sold. The FTC says X-Mode/Outlogic did not implement reasonable or appropriate safeguards against downstream use of the precise location data it sells, putting consumers’ sensitive personal information at risk.

Give Feedback

The information revealed through the location data that X-Mode/Outlogic sold not only violated consumers’ privacy but also exposed them to potential discrimination, physical violence, emotional distress, and other harms, according to the complaint.

The FTC also says the company failed to ensure that users of its own apps, Drunk Mode and Walk Against Humanity, as well as third party apps that used the X-Mode/Outlogic’s SDK were fully informed about how their location data would be used. For example, X-Mode/Outlogic provided third party apps that use the company’s SDK with sample privacy disclosures that did not fully inform consumers about which entities would receive the data and also failed to ensure these third-party apps obtained informed consumer consent to grant X-Mode/Outlogic access to their sensitive location data.

The company also failed to employ the necessary technical safeguards and oversight to ensure that it honored requests by some android users to opt out of tracking and personalized ads, according to the complaint.

The company's business has also involved creating custom audience segments based on characteristics of consumers. For at least one contract, X-Mode provided a private clinical research company information for marketing and advertising purposes about consumers who had visited certain internal medical facilities and then pharmacies or specialty infusion centers within a certain radius in the Columbus, Ohio area.

The FTC says these practices violate the FTC Act's prohibition against unfair and deceptive practices.

In addition to the limits on sharing certain sensitive locations, the [proposed order](#) requires X-Mode/Outlogic to create a program to ensure it develops and maintains a comprehensive list of sensitive locations, and ensure it is not sharing, selling or transferring location data about such locations. Other provisions of the proposed order require the company to:

- Delete or destroy all the location data it previously collected and any products produced from this data unless it obtains consumer consent or ensures the data has been deidentified or rendered non-sensitive;
- Develop a supplier assessment program to ensure that companies that provide location data to X-Mode/Outlogic are obtaining informed consent from consumers for the collection, use and sale of the data or stop using such information;
- Implement procedures to ensure that recipients of its location data do not associate the data with locations that provide services to LGBTQ+ people such as bars or service organizations, with locations of public gatherings of individuals at political or social demonstrations or protests, or use location data to determine the identity or location of a specific individual;
- Provide a simple and easy-to-find way for consumers to withdraw their consent for the collection and use of their location data and for the deletion of any location data that was previously collected;
- Provide a clear and conspicuous means for consumers to request the identity of any individuals and businesses to whom their personal data has been sold or shared or give consumers a way to delete their personal location data from the commercial databases of all recipients of the data; and
- Establish and implement a comprehensive privacy program that protects the privacy of consumers' personal information and also create a data retention schedule.

Give Feedback

The proposed order also limits the company from collecting or using location data when consumers have opted out of targeted advertising or tracking or if the company cannot verify records showing

that consumers have provided consent to the collection of location data.

The Commission voted 3-0 to issue the proposed administrative complaint and to accept the consent agreement. Chair Khan, joined by Commissioners Rebecca Kelly Slaughter and Alvaro Bedoya, issued a [separate statement](#).

The FTC will publish a description of the consent agreement package in the Federal Register soon. The agreement will be subject to public comment for 30 days after publication in the Federal Register after which the Commission will decide whether to make the proposed consent order final. Instructions for filing comments will appear in the published notice. Once processed, comments will be posted on Regulations.gov.

NOTE: The Commission issues an administrative complaint when it has “reason to believe” that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to \$50,120.

The lead staff attorneys on this matter are Bhavna Changrani and Brian Shull from the FTC’s Bureau of Consumer Protection.

The Federal Trade Commission works to promote competition and [protect and educate consumers](#).

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. Learn more about consumer topics at [consumer.ftc.gov](#), or report fraud, scams, and bad business practices at [ReportFraud.ftc.gov](#). Follow the [FTC on social media](#), read [consumer alerts](#) and the [business blog](#), and [sign up to get the latest FTC news and alerts](#).

Contact Information

Media Contact

[Juliana Gruenwald Henderson](#)

Office of Public Affairs

[202-326-2924](#)



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

FTC Order Will Ban InMarket from Selling Precise Consumer Location Data

Proposed settlement is FTC's second in recent weeks aimed at limiting the collection, use, and sale of consumers' location data

January 18, 2024



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Advertising and Marketing](#) | [Online Advertising and Marketing](#) | [Privacy and Security](#) | [Consumer Privacy](#)

Give Feedback

Data aggregator InMarket Media will be prohibited from selling or licensing any precise location data to settle Federal Trade Commission charges that the company did not fully inform consumers and obtain their consent before collecting and using their location data for advertising and marketing.

Under the [proposed order](#), InMarket will also be prohibited from selling, licensing, transferring, or sharing any product or service that categorizes or targets consumers based on sensitive location data.

"All too often, Americans are tracked by serial data hoarders that endlessly vacuum up and use personal information. Today's FTC action makes clear that firms do not have free license to monetize data tracking people's precise location," said FTC Chair Lina M. Khan. "We'll continue to use all our tools to protect Americans from unchecked corporate surveillance."

Texas-based InMarket collects location information from a variety of sources, including its own apps and from third-party apps that incorporate its software development kit (SDK). InMarket cross-references consumers' location histories with advertising-related points of interest to identify consumers who have visited those locations and then sorts consumers, based on their visits to these

points of interest, into audience segments to which it can target advertising based on their past behavior.

InMarket has maintained nearly 2,000 such audience segment lists that have included such categories as “parents of preschoolers,” “Christian church goers,” and “wealthy and not healthy.” InMarket can display ads based on this information to users of apps that incorporate its SDK and also offers a product that sends ads to consumers based on their location.

In its [complaint](#), the FTC says InMarket failed to obtain informed consent from users of its own apps, shopping rewards app CheckPoints and shopping list app ListEase. For example, when the company requests to use a consumer’s location data, it states that the data will be used for the app’s function, such as to provide shopping reward points or to remind consumers about items on their shopping list, and fails to inform users that the location data will also be combined with other data obtained about those users and used for targeted advertising.

The FTC says that InMarket also failed to ensure that third-party apps that incorporate the company SDK have obtained informed consent. In fact, the company failed to tell third party apps that the location data provided through InMarket’s SDK will be combined with other data to create profiles of consumers, according to the complaint.

The FTC also says that the company’s policy of retaining geolocation data for five years was unnecessary to carry out the purposes for which it was collected and increased the risk that this sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing sensitive information about the consumer.

This is the second case the FTC has brought in recent weeks involving the unfair collection of location data, which can reveal sensitive information about a person’s life. Earlier this month, the FTC [announced a settlement with X-Mode Social and its successor Outlogic](#) over allegations the company sold precise location data that could be used to track people’s visits to sensitive locations such as medical and reproductive health clinics, places of religious worship and domestic abuse shelters.

In addition to the ban on selling or licensing precise location data—a first for the FTC—the proposed order also requires InMarket to take several steps to strengthen protections for consumers. Under the proposed order, the company:

- Must delete or destroy all the location data it previously collected and any products produced from this data unless it obtains consumer consent or ensures the data has

Give Feedback

been deidentified or rendered non-sensitive;

- Must provide a simple and easy-to-find way for consumers to withdraw their consent for the collection and use of their location data for InMarket apps and a mechanism to request deletion of any location data that InMarket previously collected;
- Must notify consumers whose location data was collected through InMarket's apps about the FTC's action against the company and provide them with a way to opt out of data collection or request to delete their data;
- Will be limited from collecting or using location data from InMarket apps unless it obtains consumers' informed consent to the collection of their location data;
- Will be required to create a sensitive location data program to prevent the company from using, selling, licensing, transferring, or otherwise sharing any products or services that categorize or target consumers based on sensitive location data;
- Must develop an SDK supplier assessment program to ensure that companies that provide location data to InMarket via its SDK are obtaining informed consent from consumers for the collection, use and sale of the data or must stop using such information; and
- Establish and implement a comprehensive privacy program that protects the privacy of consumers' personal information and also create a data retention schedule.

Give Feedback

The Commission voted 3-0 to issue the administrative complaint and to accept the proposed consent agreement with InMarket.

The FTC will publish a description of the consent agreement package in the Federal Register soon.

The agreement will be subject to public comment for 30 days after publication in the Federal Register after which the Commission will decide whether to make the proposed consent order final.

Instructions for filing comments will appear in the published notice. Once processed, comments will be posted on Regulations.gov.

NOTE: The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with

respect to future actions. Each violation of such an order may result in a civil penalty of up to \$51,744.

The lead staff attorneys on this matter are Gorana Neskovic, David Walko and Elizabeth Averill from the FTC's Bureau of Consumer Protection.

The Federal Trade Commission works to promote competition and [protect and educate consumers](#).

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize.

Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov. Follow the [FTC on social media](#), read [consumer alerts](#) and the [business blog](#), and [sign up to get the latest FTC news and alerts](#).

Contact Information

Media Contact

[Juliana Gruenwald Henderson](#)

Office of Public Affairs

[202-326-2924](tel:202-326-2924)

Give Feedback



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations

Agency Alleges that Kochava's Geolocation Data from Hundreds of Millions of Mobile Devices Can Be Used to Identify People and Trace Their Movements

Give Feedback

August 29, 2022



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Health Privacy](#)

The Federal Trade Commission filed a lawsuit against data broker Kochava Inc. for selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava's data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. The FTC alleges that by selling data tracking people, Kochava is enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence. The FTC's lawsuit seeks to halt Kochava's sale of sensitive geolocation data and require the company to delete the sensitive geolocation information it has collected.

"Where consumers seek out health care, receive counseling, or celebrate their faith is private information that shouldn't be sold to the highest bidder," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is taking Kochava to court to protect people's privacy and halt the sale of their sensitive geolocation information."

Idaho-based Kochava purchases vast troves of location information derived from hundreds of millions of mobile devices. The information is packaged into customized data feeds that match unique mobile device identification numbers with timestamped latitude and longitude locations. According to Kochava, these data feeds can be used to assist clients in advertising and analyzing foot traffic at their stores and other locations. People are often unaware that their location data is being purchased and shared by Kochava and have no control over its sale or use.

In a [complaint filed against Kochava](#), the FTC alleges that the company's customized data feeds allow purchasers to identify and track specific mobile device users. For example, the location of a mobile device at night is likely the user's home address and could be combined with property records to uncover their identity. In fact, the data broker has touted identifying households as one of the possible uses of its data in some marketing materials.

According to the FTC's complaint, Kochava's sale of geolocation data puts consumers at significant risk. The company's 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. The release of this data could expose them to stigma, discrimination, physical violence, emotional distress, and other harms.

Give Feedback

The FTC alleges that 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. The data sample the FTC examined included precise, timestamped location data collected from more than 61 million unique mobile devices in the previous week. Using Kochava's publicly available data sample, the FTC complaint details how it is possible to identify and track people at sensitive locations such as:

- **Reproductive health clinics:** The data could be used to identify people who have visited a reproductive health clinic and therefore expose their private medical decisions. Using the data sample, it is possible to track a mobile device from a reproductive health clinic to a single-family residence to other places routinely visited. The data may also be used to identify medical professionals who perform, or assist in the performance, of reproductive health services.
- **Places of worship:** The data could be used to track consumers to places of worship, and thus reveal the religious beliefs and practices of consumers. The data sample identifies mobile devices that were located at Jewish, Christian, Islamic, and other religious denominations' places of worship.

- **Homeless and domestic violence shelters:** The data could be used to track consumers who visited a homeless shelter, domestic violence shelter, or other facilities directed to at-risk populations. This information could reveal the location of people who are escaping domestic violence or other crimes. The data sample identifies a mobile device that appears to have spent the night at a temporary shelter whose mission is to provide residence for at-risk, pregnant young women or new mothers. In addition, because Kochava's data allows its customers to track people over time, the data could be used to identify their past conditions, such as homelessness.
- **Addiction recovery centers:** The data could be used to track consumers who have visited addiction recovery centers. The data could show how long consumers stayed at the center and whether a consumer potentially relapses and returns to a recovery center.

Protecting sensitive consumer data, including geolocation and health data, is a top priority for the FTC. This month, the FTC announced that it is exploring rules to crack down on harmful [commercial surveillance practices](#) that collect, analyze, and profit from information about people. In July, the [FTC warned businesses](#) that the agency intends to enforce the law against the illegal use and sharing of highly sensitive consumer data, including sensitive health data. Last year, the FTC [issued a policy statement](#) warning health apps and connected devices that collect or use consumers' health information that they must notify consumers and others when that data is breached as required by the Health Breach Notification Rule. In 2021, the agency also [took action against the fertility app Flo Health](#) for sharing sensitive health data with third parties.

Give Feedback

The Commission vote authorizing the staff to file the complaint against Kochava was 4-1. Commissioner Noah Joshua Phillips voted no. The complaint was filed in the U.S. District Court for the District of Idaho.

NOTE: The Commission files a complaint when it has "reason to believe" that the named defendants are violating or are about to violate the law and it appears to the Commission that a proceeding is in the public interest. The case will be decided by the court.

The Federal Trade Commission works to promote competition and [protect and educate consumers](#). The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. Learn more about consumer topics at [consumer.ftc.gov](#), or report fraud, scams, and bad business practices at [ReportFraud.ftc.gov](#). Follow the [FTC on social media](#), read [consumer alerts](#) and the [business blog](#), and [sign up to get the latest FTC news and alerts](#).

Contact Information

Media Contact

[Juliana Gruenwald Henderson](#)

Office of Public Affairs

[202-326-2924](tel:202-326-2924)

Staff Contacts

Brian Shull

Bureau of Consumer Protection

[202-326-3734](tel:202-326-3734)

Julia Horwitz

Bureau of Consumer Protection

[202-326-2269](tel:202-326-2269)

Give Feedback



← HOME

Legal Affairs

Privacy

Working Harder Won't Solve Privacy Diligence. It's Time to Work Smarter.



Feb. 01, 2024

By Michael Hahn and Richy Glassberg



Introducing the IAB Diligence Platform

With more than a dozen privacy laws in effect or coming into effect, each of which provides for an opt-out of “sales” and targeted advertising, digital advertising is increasingly becoming a regulated industry. This change in the law must be met with a change in business practices, including how we conduct diligence around privacy in digital ad transactions.

Liability is shifting

One of the fundamental changes in state privacy laws is the inclusion of accountability. There are new requirements around what partners can and cannot do with the personal information you provide them. Indeed, you must take “reasonable and appropriate steps” to make sure that your partner uses that personal information consistent with the law — for example, by including mandatory audit provisions in your contracts.

Perhaps the most significant change is the California Privacy Protection Agency's (CPPA) regulation stating that whether you conduct diligence of your partners with whom you disclose personal information is a material factor in determining whether you will be liable for their wrongdoing. In other words, due diligence and third-party risk management should now be integral aspects of your data privacy program.

Enforcement is getting tougher — and digital advertising will face new scrutiny

Not only is liability shifting, but enforcement is too. Upon the effective dates of the dozen-plus privacy laws, each vests enforcement in its attorney general's office. In California, both the Attorney General's Office and the CPPA each have enforcement powers.

Those enforcers have shown a clear intent to protect consumers under their privacy laws. On January 26, the California Attorney General's announced a sweep of streaming services under the CCPA. The Connecticut Attorney General's Office announced its enforcement priorities for the digital advertising industry at the IAB State Privacy Law Summit on November 15, including setting bright lines on the right to opt-out of the disclosure of personal information to vendors for measurement and frequency capping (where those vendors do not serve as your processors), as well as parameters on the categorizing information as deidentified.

Colorado's Attorney General Phil Weiser has said "Enforcement of the Colorado Privacy Act is a critical tool to protect consumers' data and privacy (...) If we become aware of organizations that are flouting the law or refusing to comply with it, we are prepared to act."

Finally, the CPPA has a fully staffed enforcement division to investigate possible violations, and it's hard to imagine digital advertising won't be one of its key focus areas. Importantly, you can expect announced or unannounced audits to commence soon, particularly: for companies who've had any history of non-compliance with any privacy law; where there are potential violations of the law; or where the subject's "collection or processing of personal information presents significant risk to consumer privacy or security". And there is no longer a mandatory 30-day "cure period" — no guaranteed second chances — under the CCPA.

Companies should not underprice state privacy risk because doing so could become a big — and very costly — mistake.

Industry diligence must improve

Historically, privacy diligence has relied on two things. First, you obtained a representation and warranty in the contract that the business partner would comply with applicable law and then indemnity if it failed to do so. Second, you typically sent out a generic questionnaire.

This approach will no longer do.

For a fully digital industry, diligence is woefully analog and outdated. It's underfunded, understaffed, and in an underdeveloped state. Companies send out and receive dozens of questionnaires monthly in connection with transactions and partnerships. These often ask the same questions in multiple different ways, which makes responding to them a rote exercise of managing answers in spreadsheets and cutting and pasting. Worse, these questionnaires are often generic and out of date, and the majority fail to address the actual uses of personal information contemplated by the business arrangement and the entirety of each state law. Sometimes, the surveys come back incomplete — if they come back at all.

The industry must solve for privacy diligence, and it can't do so by doubling down on its current approach. Rather, what's needed are standards around privacy diligence that can achieve effectiveness and efficiency so that all industry participants are speaking the same language. We need standardized privacy diligence questions that address both the letter of the law and the specific data flows and business use cases for every vendor and sub-vendor. We also need a more effective and efficient means of managing the diligence process.

It's a digital problem that demands a digital solution.

Introducing the IAB Diligence Platform

To proactively meet the needs of regulators, the IAB convened a Privacy Implementation and Accountability Taskforce (PIAT), composed of publishers, advertisers, agencies and ad tech companies. The group highlighted the need for an effective and efficient solution: the IAB Diligence Platform.

The Platform provides a privacy diligence solution that is purpose-built for the digital advertising industry. This solution will combine new industry vertical business questions with US state law assessments in one collaborative platform to make the diligence workflow effective and efficient for both sides of the partnership.

Leading industry privacy lawyers and law firms are collaborating in the PIAT initiative to draft the right business and privacy questions of each digital advertising use case and vendor type. We know that the right questions that a publisher should ask an SSP aren't the right questions for

an advertiser or its agency to ask a DSP. These questions will be complemented by questions specifically tailored to assess compliance with each state privacy law.

The IAB Diligence Platform will be built on the SafeGuard Privacy Platform, which features robust state law assessments and a vendor compliance hub. Users will be able to complete the diligence questionnaire once and share it with the partners on the platform as they engage in digital ad transactions. By moving the industry towards use of the Platform, there will be a strong network effect to drive efficiency and improve deal speed. In fact, IAB members that are already on the SafeGuard Privacy platform are seeing 80%+ efficiency gains by managing multiple laws concurrently and automating vendor compliance. They have a single source of truth for members to handle their diligence efficiently, and they're saving dozens of FTE hours a month.

The solution provides:

- Standardized privacy questions that will be leveraged by the industry.
- Ability to fill out assessments and questionnaires once and easily share with partners many times.
- Ability to update compliance as new laws come online or existing laws and regulations evolve.

It's better for vendors. Automated sharing means significant time and labor savings for vendors — they answer the right set of questions once and share everywhere. Deals close faster when there are no overlapping, inappropriate, out of date, and repetitive questions to wrestle with.

It's better for accountability. It's auditable, fully accountable, and provides a clear record of compliance: companies that are audited can show the actions they've taken to ensure that control and privacy of company data was assured. The combination of SafeGuard Privacy assessments and IAB PIAT (Privacy Implementation & Accountability Task Force) questionnaires delivers what the heightened regulatory landscape calls for.

Of inertia, lack of budgets, and finger-pointing

The first challenge is for the industry to overcome inertia. We must recognize that we are now becoming a regulated industry, and expect that regulators will do their job diligently. What worked in the past will not work in the future.

Despite this, few budgets have a line item for a diligence platform. This must change.

Company leaders must not allow this to devolve into finger-pointing about which budget this should come from — especially since nobody's going to point at their own budget first.

This needs to be a priority driven by top management, with real effort to find the resources and get a real solution in place. The good news is, the cost is lower than it might appear — and certainly lower than the financial and reputational cost of an enforcement action arising from your partner failing to properly process personal information you provided to it.

Additionally, the costs of the industry's current approach are high, but largely hidden. Every hour that employees spend sending out questionnaires, working with vendors to fill in the inevitable gaps, and chasing down vendors who are too overwhelmed to reply has a hard-dollar cost. This is to say nothing of the opportunity cost of executives stepping in to push through contracts that have been held up in the process.

What to do now

We encourage everyone to understand the new legal landscape, and prepare for smarter diligence. If you're not already a member of IAB PIAT (Privacy Implementation & Accountability Task Force), you can email michael.hahn@iab.com. You can also contact SafeGuard Privacy [here](#) to see a demo of the IAB Diligence Platform.

The new regulations are real, and we expect them to be enforced. The most important thing to do is to start today to prepare for new state privacy law diligence requirements.

Related Content

[The Intersection of Sensitive Personal Data, Privacy Laws, and Marketing](#)

[Privacy Tech Workshop for Lawyers and Cross-Functional Privacy Teams – D.C.](#)

[Video Privacy Protection Act \(VPPA\) Litigation Preparation & Defense Toolkit](#)

Authors

AUTHOR

Michael Hahn

Executive Vice President, General Counsel
at IAB & IAB Tech Lab

Show Bio 

AUTHOR

Richy Glassberg

Co-Founder & CEO
at SafeGuard Privacy

Show Bio 

Related Content

**The Intersection of Sensitive
Personal Data, Privacy Laws, and
Marketing**



**Privacy Tech Workshop for Lawyers
and Cross-Functional Privacy Teams
– D.C.**



Video Privacy Protection Act (VPPA)

Wiretapping Claims Litigation



[About IAB](#) [Annual Report](#) [Contact Us](#) [Statements & Press](#) [IAB Careers](#)

[Privacy Policy](#) [Terms of Use](#) [Your Ad Choices](#) [Antitrust Principles & Compliance](#)

Copyright 2016 Interactive Advertising Bureau