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.

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 Commc'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.

More from the Technology Blog

Technology Blog

AI and the Risk of Consumer Harm

Staff in the Office of Technology and the Division of Advertising Practices | January 3, 2025

Technology Blog

Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans

Staff in the Office of Technology & the Division of Privacy and Identity Protection | December 13, 2024

Technology Blog

Solving the Traveling Salesman Problem? Not quite, but here are more research questions from the Office of Technology

Staff at the Office of Technology | December 4, 2024

Technology Blog

Unpacking Real Time Bidding through FTC's case on Mobilewalla

Staff in the Office of Technology & Division of Privacy and Identity Protection | December 3, 2024