Published on *The National Law Review* https://natlawreview.com

FTC: Three Enforcement Actions and a Ruling

Article By:

Angela P. Doughty

Mayukh Sircar

In today's digital landscape, the exchange of personal information has become ubiquitous, often without consumers fully comprehending the extent of its implications.

The recent actions undertaken by the Federal Trade Commission (FTC) shine a light on the intricate web of data extraction and mishandling that pervades our online interactions. From the seemingly innocuous permission requests of game apps to the purported protection promises of security software, consumers find themselves at the mercy of data practices that blur the lines between consent and exploitation.

The FTC's proposed settlements with companies like X-Mode Social ("X Mode") and InMarket, two data aggregators, and Avast, a security software company, underscores the need for businesses to appropriately secure and limit the use of consumer data, including previously considered innocuous information such as browsing and location data. In a world where personal information serves as currency, ensuring consumer privacy compliance has never been more critical – or posed such a commercial risk for failing to get it right.

X-Mode and InMarket Settlements: The proposed settlements with X-Mode and InMarket concern numerous allegations based on the mishandling of consumers' location data. Both companies supposedly collected precise location data through their own mobile apps and those of third parties (through software development kits). X-Mode is alleged to have sold precise location data (advertised as being 70% accurate within 20 meters or less) linked to timestamps and unique persistent identifiers (i.e., names, email addresses, etc.) of its consumers to private government contractors without obtaining proper consent. Plotting this data on a map makes it easy to reveal each person's movements over time.

InMarket purportedly utilized location data to cross-reference such data with points of interest to sort consumers into particularized audience segments for targeted advertising purposes without adequately informing consumers – examples of audience segments include parents of preschoolers, Christian church attendees, and "wealthy and not healthy," among other groupings.

Avast Settlement: Avast, a security software company, allegedly sold granular and re-identifiable browsing information of its consumers despite assuring consumers it would protect their privacy.

Avast allegedly collected extensive browsing data of its consumers through its antivirus software and browser extensions while ensuring its consumers that their browsing data would only be used in aggregated and anonymous form. The data collected by Avast revealed visits to various websites that could be attributed to particular people and allowed for inferences to be drawn about such individuals – examples include academic papers on symptoms of breast cancer, education courses on tax exemptions, government jobs in Fort Meade, Maryland with a salary over $100,000, links to FAFSA applications and directions from one location to another, among others.

Sensitivity of Browsing and Location Data

It is important to note that none of the underlying datasets in question contained traditional types of personally identifiable information (e.g., name, identification numbers, physical descriptions, etc.) ("PII"). Even still, the three proposed settlements by the FTC underscore the sensitive nature of browsing and location data due to the insights such data reveals, such as religious beliefs, health conditions, and financial status, and the ease with which the insights can be linked to certain individuals.

In the digital age, the amount of data available about individuals online and collected by various companies makes the re-identification of individuals easier every day. Even when traditional PII is not included in a data set, by linking sufficient data points, a profile or understanding of an individual can be created. When such profile is then linked to an identifier (such as username, phone number, or email address provided when downloading an app or setting up an account on an app) and cross-referenced with various publicly available data, such as name, email, phone number or content on social media sites, it can allow for deep insights into an individual. Despite the absence of traditional types of PII, such data poses significant privacy risks due to the potential for re-identification and the intimate details about individuals' lives that it can divulge.

The FTC emphasizes the imperative for companies to recognize and treat browsing and location data as sensitive information and implement appropriate robust safeguards to protect consumer privacy. This is especially true when the data set includes information with the precision of those cited by the FTC in its proposed settlements.

Accountability and Consent

With browsing and location data, there is also a concern that the consumer may not be fully aware of how their data is used. For instance, Avast claimed to protect consumers' browsing data and then sold that very same browsing information, often without notice to consumers. When Avast did inform customers of their practices, the FTC claims it deceptively stated any sharing would be "anonymous and aggregated." Similarly, X-Mode claimed it would use location data for ad-personalization and location-based analytics. Consumers were unaware such location data was also sold to government contractors.

The FTC has recognized that a company may need to process an individual's information to provide them with services or products requested by the individual. The FTC also holds that such processing does not mean the company is then free to collect, access, use, or transfer that information for other purposes (e.g., marketing, profiling, background screening, etc.). Essentially, purpose matters. As the FTC explains, a flashlight app provider cannot collect, use, store, or share a user's precise geolocation data, or a tax preparation service cannot use a customer's information to market other products or services.

If companies want to use consumer personal information for purposes other than providing the requested product or services, the FTC states that companies should inform consumers of such uses and obtain consent to do so.

The FTC aims to hold companies accountable for their data-handling practices and ensure that consumers are provided with meaningful consent mechanisms. Companies should handle consumer data only for the purposes for which data was collected and honor their privacy promises to consumers. The proposed settlements emphasize the importance of transparency, accountability, meaningful consent, and the prioritization of consumer privacy in companies' data handling practices.

Implementing and Maintaining Safeguards

Data, especially specific data that provide insights and inferences about individuals, is extremely valuable to companies, but it is that same data that exposes such individuals' privacy. Companies that sell or share information sometimes include limitations for the use of the data, but not all contracts have such restrictions or sufficient restrictions to safeguard individuals' privacy.

For instance, the FTC alleges that some of Avast's underlying contracts did not prohibit the re-identification of Avast's users. Where Avast's underlying contracts prohibited re-identification, the FTC alleges that purchasers of the data were still able to match Avast users' browsing data with information from other sources if the information was not "personally identifiable." Avast also failed to audit or confirm that purchasers of data complied with its prohibitions.

The proposed complaint against X-Mode recognized that at least twice, X-Mode sold location data to purchasers who violated restrictions in X-Mode's contracts by reselling the data they bought from X-Mode to companies further downstream. The X-Mode example shows that even when restrictions are included in contracts, they may not prevent misuse by subsequent downstream parties.

Ongoing Commitment to Privacy Protection:

The FTC stresses the importance of obtaining informed consent before collecting or disclosing consumers' sensitive data, as such data can violate consumer privacy and expose them to various harms, including stigma and discrimination. While privacy notices, consent, and contractual restrictions are important, the FTC emphasizes they need to be backed up by action. Accordingly, the FTC's proposed orders require companies to design, implement, maintain, and document safeguards to protect the personal information they handle, especially when it is sensitive in nature.

What Does a Company Need To Do?

Given the recent enforcement actions by the FTC, companies should:

1. Consider the data it collects and whether such data is needed to provide the services and products requested by the consumer and/or a legitimate business need in support of providing such services and products (e.g., billing, ongoing technical support, shipping);
2. Consider browsing and location data as sensitive personal information;
3. Accurately inform consumers of the types of personal information collected by the company, its uses, and parties to whom it discloses the personal information;
4. Collect, store, use, or share consumers' sensitive personal information (including browser and location data) only with such consumers' informed consent;

5. Limit the use of consumers' personal information solely to the purposes for which it was collected and not market, sell, or monetize consumers' personal information beyond such purpose;
6. Design, Implement, maintain, document, and adhere to safeguards that actually maintain consumers' privacy; and
7. Audit and inspect service providers and third-party companies downstream with whom consumers' data is shared to confirm they are (a) adhering to and complying with contractual restrictions and (b) implementing appropriate safeguards to protect such consumer data.

© 2025 Ward and Smith, P.A.. All Rights Reserved.

National Law Review, Volume XIV, Number 131

Source URL:https://natlawreview.com/article/ftc-three-enforcement-actions-and-ruling