Blogs
March 18, 2024
FTC Obtains $16.5M from Avast for Sale of Sensitive Data

The FTC's action against Avast reflects its continued focus on the mass collection and sale of sensitive personal data for advertising purposes.

One month after the February 22, 2024, announcement of enforcement actions against data brokers X-Mode and InMarket Media, the Federal Trade Commission (FTC) announced a complaint and proposed consent order requiring software security company Avast Limited and two subsidiaries, Avast s.r.o. and Jumpshot, Inc. (collectively, Avast), to pay $16.5 million to resolve allegations that they unfairly and deceptively sold granular, reidentifiable web browsing data for advertising purposes. The FTC's action against Avast reflects its continued focus on the mass collection and sale of sensitive personal data for advertising purposes.

Avast Complaint

In its complaint, the FTC alleges that Avast marketed its products, including browser extensions and antivirus software, as tools to protect consumer privacy, such as by blocking third parties from tracking online activity through cookies. The FTC alleges that Avast (via its Jumpshot subsidiary) collected more than eight petabytes of consumer browsing data, such as search queries and the URLs of webpages visited by consumers, via browser extensions and antivirus software marketed as privacy-protective. The FTC alleges that Avast indefinitely retained these browsing records, typically tied to a persistent identifier, in granular form. The FTC further alleges that Avast sold these detailed data feeds to a variety of clients—including advertising, marketing, and data analytics companies and data brokers.

The FTC claims such actions were deceptive. According to the FTC, after advertising to consumers both that its products would protect their privacy by preventing third parties from tracking their online activity and that it would only ever share their browsing data in aggregate and anonymous form, Avast turned around and did the exact opposite. The FTC's complaint alleges that Avast sold granular data that in some cases purchasers were not only free to re-associate with individuals, but in some cases such re-association was the very point of the

purchase.

The FTC also alleges that Avast's collection, retention, and sale of the granular browsing data was unfair. According to the FTC, this data processing was done without adequate notice and consumer consent. More specifically, the FTC alleges that in many instances, Avast's privacy disclosures either did not state that consumers' browsing data would be shared with third parties for advertising purposes or indicated that such data would only be shared in aggregate and anonymous form. Notably, the FTC also characterizes "re-identifiable browsing data" as "sensitive," and alleges that the browsing data collected by the Avast products, such as web searches and websites, reveal consumers' religious beliefs, health concerns, political leanings, location, financial status, visits to child-directed content, and interest in prurient content. According to the FTC, Avast's practice of linking browsing information to device and other identifiers, as well as coarse location data, over time, increased the likelihood that a consumer could be reidentified, which was likely to cause substantial consumer injury.

Consent Order

The proposed consent order generated headlines with the requirement that Avast must pay $16.5 million, The FTC commissioners touted this as "the highest monetary remedy in a *de novo* privacy violation case" brought by the FTC to date, that is, the highest monetary remedy for a privacy violation under Section 5(a) of the FTC Act. The FTC has said that it intends to use this money to provide redress to affected consumers.

The order bans Avast from selling, licensing, or otherwise disclosing web browsing data from Avast products to third parties for advertising purposes. It also requires Avast to obtain affirmative express consent before selling, licensing, or otherwise disclosing web browsing data from non-Avast products to third parties for such purposes.

Similar to the X-Mode and InMarket orders, the order mandates that Avast not only delete the web browsing data that it collected through Jumpshot, but also delete or destroy any models, algorithms, or software developed based on that data. Avast also must instruct any third party that received such data to delete the data and any models or algorithms derived from them or software developed to analyze the data.

In addition, the order subjects Avast to typical FTC privacy order provisions, such as prohibitions on certain privacy-related misrepresentations and the requirement to implement a mandated privacy program with biennial third-party assessments for 20 years.

Takeaways

The FTC's enforcement actions against X-Mode, InMarket, and now Avast signal the agency's continued focus on data brokers and others in the business of aggregating and selling large volumes of what the FTC views as sensitive data for advertising purposes. In a recent blog post, the FTC reinforced common themes across the Avast, X-Mode, and InMarket actions, such as the following:

- First, in a line that has attracted significant attention, the FTC asserts that "Browsing and location data are sensitive. Full stop." While the FTC has long asserted that precise location data is sensitive, it remains to be seen whether its characterization of web browsing data as "sensitive" marks a sustained shift in the FTC's thinking, or if this is a reflection of the specific facts of Avast's alleged practices. In any event, the Avast case makes clear that even data lacking "traditional standalone elements of personally identifiable information" can reveal sensitive information about consumers. And if the risk of such disclosure is likely to cause substantial injury to consumers, it may be unfair.
- Second, the FTC expects companies to be clear about how consumers' personal data will be used, shared, and retained. Without clear notice, "[p]eople have no way to object to—let alone control," how their data is handled.
- Third, the purposes for which data is processed should align with the purposes for which it was collected.

- Fourth, the FTC expressed skepticism about contractual restrictions on data reidentification or misuse where, for example, such restrictions contain loopholes or are not audited or enforced against downstream recipients of data.

Authors

Explore more in

Privacy & Security