UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

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

A person's browsing history can reveal extraordinarily sensitive information. A record of the websites someone visits can divulge everything from someone's romantic interests, financial struggles, and unpopular political views to their weight-loss efforts, job rejections, and gambling addiction.

Aware that internet users may want to protect their browsing history from data brokers and other trackers, some firms now market services to provide privacy protections online. Avast is one such firm. Since at least 2014, Avast has distributed browser extensions that it promoted through promising users enhanced privacy. It claimed, for example, that its products 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." It also stated that any sharing of user information would be in "anonymous and aggregate" form.[1]

The Commission's complaint charges that these statements by Avast were deceptive. The complaint details how Avast collected highly detailed browsing data from millions of users and then, through its subsidiary Jumpshot, sold those browsing records to over a hundred clients, including major advertising firms. Avast also released this data in individualized, re-identifiable form, allowing these browsing histories to be traced back to specific people—in direct contravention of what Avast had promised.[2] While the FTC's privacy lawsuits routinely take on firms that misrepresent their data practices, Avast's decision to expressly market its products as *safeguarding* people's browsing records and *protecting* data from tracking only to then sell those records is especially galling.[3] Moreover, the volume of data Avast released is staggering: the

[1] Complaint, *In re Avast Limited*, Docket No. X (Feb. 15, 2024) ¶¶ 5-17, 31-39, [hyperlink in black] [hereinafter Avast Complaint].
[2] *Id.* at ¶¶ 18-30
[3] For example, the complaint charges that Avast stated that its software would "[s]hield your privacy. Stop anyone and everyone from getting to your computer." It similarly claimed that some of its products would allow users to "[r]eclaim your browser. Get rid of unwanted extensions and hackers making money off your searches." Avast also represented that the Avast Secure Browser is "Anti-Tracking" and "[p]rotects your privacy by preventing websites, advertising companies, and other web services from tracking your online activity." (*Id.* at ¶¶ 16-37). In reality, "many of the Jumpshot products (or 'data feeds') provided third-party data buyers with extraordinary detail regarding how users navigated the Internet, including each webpage visited, precise timestamp, the type of device and browser, and the city, state, and country. Most of the data feeds included a unique and persistent device

complaint alleges that by 2020 Jumpshot had amassed "more than eight petabytes of browsing information dating back to 2014." Indeed, one advertising firm received detailed browsing information on 50 percent of Avast's entire user base world-wide, spanning the United States, United Kingdom, Mexico, Australia, Canada, and Germany.[4]

The FTC charges that Avast's conduct here was not only deceptive, but also an unfair practice, violating Section 5 of the FTC Act. Exposing people's detailed browsing data in ways that can be traced back to them marks an invasion of privacy and is likely to cause substantial injury. Because it is intrinsically sensitive, browsing data warrants heightened protection. Businesses that sell or share browser history data without affirmatively obtaining people's permission may be in violation of the law.

Today's action against Avast further builds out the Commission's work establishing that sensitive data triggers heightened privacy obligations and a default presumption against its sharing or sale. Through a series of cases, the FTC has been expounding on how firms are legally required to safeguard sensitive data. *Kochava*, *X-Mode*, and *InMarket* highlighted the sensitivity of precise geolocation data.[5] In *Rite Aid* and *Alexa*, the FTC highlighted the sensitivity of biometric data, such as facial attributes and voice recordings of children.[6] And in *GoodRx*, *BetterHelp*, and *Premom*, we underscored the heightened sensitivity of people's health information.[7] Today, we underscore the sensitivity of yet another type of information: people's browsing records.

---

identifier associated with each particular browser allowing Jumpshot and the third-party buyer to trace individuals across multiple domains over time." *Id.* at ¶ 21.

[4] *Id*. at ¶ 30.

[5] *See* Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other; Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Press Release, Fed. Trade Comm'n, FTC Order Will Ban InMarket From Selling Precise Consumer Location Data (Jan. 18, 2024), https://www ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data.

[6] *See* Press Release, Fed. Trade Comm'n, Rite Aid Banned From Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without; Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023), https://www ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[7] *See* Press Release, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay $7.8 Million (July 14, 2023), https://www ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; Press Release, Fed. Trade Comm'n, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

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. We have also pursued bright-line bans. In *Rite Aid*, where we alleged that Rite Aid used unfair and discriminatory facial recognition software, we are seeking to ban its use of facial recognition for five years. In a trio of matters, *GoodRx*, *BetterHelp*, and *Premom*—all cases where health apps promised to keep secure users' highly personal health information but then turned around and sold that data to third parties for advertising purposes—we banned those companies from selling consumers' health information for such purposes. Here, we have obtained a similar ban, for the first time, with respect to a non-health service. Today's order also secures $16.5 million in relief—the highest monetary remedy in a *de novo* privacy violation case.

I am very grateful to the Division of Privacy and Identity Protection for their terrific work to protect Americans from privacy invasions and commercial surveillance, especially as it concerns their most sensitive data.

***