Code: 6750-01-P

FEDERAL TRADE COMMISSION

[File No. 202 3033]

Avast Limited et al.; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Avast Limited, et al.; File No. 202 3033" on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, please mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H-144 (Annex A), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Cathlin Tully (202-326-3644), Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule § 2.34, 16 CFR 2.34, notice is hereby

given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of 30 days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions*.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Avast Limited, et al.; File No. 202 3033," on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website. If you prefer to file your comment on paper, write "Avast Limited, et al.; File No. 202 3033" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H-144 (Annex A), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your

comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule § 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule § 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule § 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule § 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule § 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at *https://www.ftc.gov* to read this document and the news release describing the proposed settlement. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments it receives on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission (the "Commission" or "FTC") has accepted, subject to final approval, an agreement containing consent order from Avast Limited, Avast Software s.r.o., and Jumpshot, Inc. ("Respondents"). The proposed consent order ("Proposed Order") has been placed on the public record for 30 days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

The FTC's proposed complaint ("Proposed Complaint") alleges that Respondent Avast Limited, a United Kingdom limited liability company, together with Respondent Avast Software s.r.o. (collectively, "Avast"), a Czech Republic limited liability company, collected consumers' browsing information through browser extensions and antivirus software ("Avast Software") installed on consumers' computers and mobile devices. Through Respondent Jumpshot, Inc. ("Jumpshot"), Respondents sold this browsing data to third parties in non-aggregate, re-identifiable form.

According to the Proposed Complaint, the Avast Software collected browsing information from consumers, including uniform resource locators (URLs) of webpages visited, the URLs of background resources, consumers' search queries, and cookie values placed by third parties on consumers' computers. Among other things, the Avast Software collected browsing information revealing consumers' religious beliefs, health concerns, political leanings, location, financial status, visits to child-directed content, and interest in prurient content. Respondents combined this information with persistent identifiers, including identifiers created by Respondents that identified each consumer device uniquely, increasing the likelihood that consumers could be reidentified. As alleged in the Proposed Complaint, in many instances Respondents failed to disclose any information

about their collection or sale of browsing information, and affirmatively represented that the Avast Software would "[b]lock[] annoying tracking cookies that collect data on your browsing activities" and "[s]hield your privacy."

The Proposed Complaint alleges that after Avast acquired Jumpshot in 2013, Avast rebranded Jumpshot in 2014 as an analytics company. From 2014 to 2020, the Proposed Complaint alleges, Jumpshot sold browsing information collected by the Avast Software to customers such as consulting firms, investment companies, advertising companies, marketing data analytics companies, individual brands, search engine optimization firms, and data brokers. The Proposed Complaint alleges that, while Respondents purported to remove consumers' identifying information before transferring browsing information to Jumpshot, the proprietary algorithm Avast developed and used to do so was not sufficient to anonymize the data, which Jumpshot then sold in non-aggregate form to its customers through a variety of products. In total, the Proposed Complaint alleges that Respondents sold consumers' browsing information, and insights derived from such data, to more than 100 customers, earning tens of millions in gross revenues. After receiving the FTC's civil investigative demand, Respondents shut down Jumpshot's operations "with immediate effect."

The Commission's three-count Proposed Complaint alleges that Respondents violated section 5(a) of the FTC Act by: (1) unfairly collecting consumers' browsing information, storing that information in granular form indefinitely, and selling that information in granular form to third parties, without adequate notice and without consumer consent; (2) representing that the Avast Software would stop the collection and sale of consumers' browsing information but failing to disclose, or to disclose adequately, that Respondents, through the Avast Software, collected and sold consumers' browsing information; and (3) misrepresenting that consumers' browsing information would be

transferred to Respondent Jumpshot and to third parties only in aggregate and anonymous form.

With respect to the first count, the Proposed Complaint alleges Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. The vast majority of consumers would not know the Avast Software would surveil their every move on the Internet or their browsing information might be sold to more than 100 third parties in granular, re-identifiable form. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

With respect to the second count, the Proposed Complaint alleges Respondents claimed the Avast Software would stop the collection and sale of consumers' browsing information. The Proposed Complaint alleges that, in reality, and as noted above, Respondents' software collected consumers' browsing information which Respondents then sold to third parties. Respondent's failure to disclosure that material information was deceptive under Section 5 of the FTC Act.

With respect to the third count, the Proposed Complaint alleges Respondents claimed consumers' browsing information would be transferred to Respondent Jumpshot and to third parties only in aggregate and anonymous form. The Proposed Complaint alleges that, in reality, and as noted above, consumers' browsing information was transferred to Respondent Jumpshot and sold to third parties in non-aggregate and non-anonymous form. Such representations were, therefore, deceptive under Section 5 of the FTC Act.

Summary of the Proposed Order with Respondents

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future. Part I prohibits Respondents from selling, licensing, transferring, sharing, or otherwise disclosing to third

parties for advertising: (1) browsing information from Avast products; (2) products or services derived from such browsing information; or (3) models or algorithms derived from such data. This provision further requires Respondents to obtain affirmative express consent from consumers before Respondents use browsing data for third-party advertising, and to obtain affirmative express consent from consumers using non-Avast branded products before selling, licensing, transferring, sharing, or otherwise disclosing to third parties browsing information collected by such products for advertising.

Part II prohibits Respondents from misrepresenting: (1) the purpose of their collection, use, disclosure, or maintenance of Covered Information (*i.e.*, information from or about a consumer or their device, including browsing information); (2) the extent to which Covered Information is aggregated or anonymized; and (3) the extent to which they collect, use, disclose, or maintain Covered Information or otherwise protect the privacy, security, availability, confidentiality, or integrity of Covered Information.

Part III requires Respondents to delete all browsing information that Respondent Jumpshot received from the Avast Respondents and related models, algorithms, and software. This provision further requires Respondents to instruct all third parties that received browsing information from Respondent Jumpshot, any models or algorithms derived from such data, and any software developed to analyze such data, to delete or destroy such data, models, algorithms, or software.

Part IV requires that Respondents provide notice about the FTC's complaint and settlement with Respondents to consumers on the Avast websites, within Avast products, and via email to consumers who purchased or downloaded Avast products between 2014 and 2020. Part V requires that Respondents establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

Part VI requires Respondents to obtain initial and biennial privacy program assessments by an independent, third-party professional for 20 years. Part VII requires Respondents to disclose all material facts to the assessor required by Part VI and prohibits Respondents from misrepresenting any fact material to the assessments required by Part VI. Part VIII requires each Respondent to submit an annual certification from a senior officer responsible for compliance with Part V that the Respondent has implemented the requirements of the Proposed Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part IX requires Respondents to pay to the Commission $16,500,000 in monetary relief. Part X describes the procedures and legal rights related to that payment.

Parts XI-XIV are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part XV states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the Proposed Complaint or Proposed Order, or to modify the Proposed Order's terms in any way.

By direction of the Commission.

April J. Tabor,

Secretary.

Statement of Chair Lina M. Khan, Joined by Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro M. Bedoya

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 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

---

[1] Complaint, *In re Avast Limited*, Docket No. C-XXXX (Feb. 15, 2024) ¶¶ 5-17, 31-39, https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-Avast.pdf [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 identifier associated with each particular browser allowing Jumpshot and the third-party buyer to trace individuals across multiple domains over time." *Id.* at ¶ 21.

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

---

[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.

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.

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.

[FR Doc. 2024-04257 Filed: 2/28/2024 8:45 am; Publication Date: 2/29/2024]

---

[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.