epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 1, 2024

Chair Lina M. Khan
Commissioner Rebecca Kelly Slaughter
Commissioner Alvaro Bedoya
Commissioner Andrew Ferguson
Commissioner Melissa Holyoak
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: *Avast, Ltd. et al.*, FTC File No. 202-3033

Dear Chair Khan and Commissioners Slaughter, Bedoya, Ferguson, and Holyoak,

By notice published February 29, 2024, the Federal Trade Commission (FTC) announced its proposed consent order and settlement with Avast Limited, Avast Software s.r.o., and Jumpshot, Inc., (collectively Avast) for Avast's alleged violations of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), prohibiting unfair or deceptive acts or practices.[1] The proposed consent order with Avast is the result of the FTC's complaint alleging that Avast violated the FTC Act in three ways: (1) unfair collection, retention, and sale of consumers' browsing information; (2) deceptive failure to disclose tracking of customers; and (3) misrepresentations regarding aggregation and anonymization.[2]

The Electronic Privacy Information Center (EPIC) submits this letter to applaud the FTC's enforcement efforts in this matter and to provide recommendations to strengthen the proposed Order (and others like it in future cases concerning web browsing data). EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed FTC consent orders and complaints regarding business practices that violate privacy rights.[3]

---

[1] Avast Ltd. et al.; Public Comment, 89 Fed. Reg. 14,839 (Feb. 29, 2024), https://www.federalregister.gov/documents/2024/02/29/2024-04257/avast-limited-et-al-analysis-of-proposed-consent-order-to-aid-public-comment [hereinafter Federal Register Notice].
[2] *Id.*; Complaint, *In the Matter of Avast Ltd. et al.*, FTC File No. 202-3033 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-Avast.pdf.
[3] *See, e.g.*, Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter EPIC Commercial Surveillance Comments]; Comments of EPIC, *In re Blackbaud, Inc.*, FTC File No. 202-3181 (Mar. 2024), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-blackbaud/; Comments of EPIC, *In re InMarket Media LLC*, File No. 202-3088 (Feb. 22, 2024), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-consent-order-with-inmarket-media-llc/; Comments of EPIC,

EPIC commends the Commission for using its authority to investigate and take enforcement actions against companies like Avast engaged in unfair and deceptive practices, especially where companies wrongfully profit from the selling of web browsing data and other sensitive information. Avast exploited users' desire for privacy protections by promising that its software would block tracking technologies that collect browsing information—while selling such data itself. We support the Commission's enforcement action against Avast, and we offer two recommendations to make the final Order even stronger: (1) the Commission should extend the core prohibition of the Order to cover sales or disclosures of browsing data for other purposes, such as sales of data to government contractors for national security purposes; and (2) the Commission should incorporate a comprehensive data minimization framework with express collection, processing, transfer, and retention limits.

As the Commission knows, web browsing data is both highly sensitive in its own right and potentially revealing of other highly sensitive consumer traits, including medical conditions and treatments. EPIC is encouraged to see the Commission recognize that "[r]e-identifiable browsing information is sensitive data."[4] The complaint highlights some of the sensitive traits that can be revealed by browsing information, including a paper on the symptoms of breast cancer, Google Maps directions, and a French dating website.[5] In the aftermath of U.S. Supreme Court's overturning of the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*, the sale of location data poses a special threat to the safety of abortion patients and providers and undermines reproductive privacy.[6] EPIC supports protections for such sensitive information and urges the

---

Demand Progress, & EFF, *In re X-Mode Social, Inc.*, FTC File No. 202-3038 (Feb. 20, 2024), https://epic.org/documents/comments-of-epic-demand-progress-and-eff-in-re-the-federal-trade-commissions-proposed-order-settlement-with-x-mode-social-inc/; Comments of EPIC, *In re BetterHelp, Inc,*, FTC File No. 202-3169 (2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-betterhelp-inc/; Comments of EPIC, *In re CafePress*, File No. 192-3209 (2022), https://epic.org/wp-content/uploads/2022/04/EPIC-comments-in-re-cafepress.pdf; Comments of EPIC, *In re Matter of Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; Comments of EPIC et al., *In re Zoom Video Communications, Inc.*, FTC File No. 192-3167 (2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; Complaint of EPIC, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc.*, FTC File No. 172-3139 (2019), https://epic.org/apa/comments/EPICFTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (2019), https://epic.org/apa/comments/EPIC-FTCCambridgeAnalytica-Sept2019.pdf; EPIC, *Comments on Standards for Safeguarding Customer Information*, Docket No. 2019-04981 (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf.

[4] Complaint, *supra* note 2, at 10.

[5] *Id.*

[6] Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.

Commission to further safeguard browsing data and location data in future enforcement actions in order to protect the privacy and safety of abortion patients and providers.

The deceptive nature of Avast's promises was particularly egregious because those promises capitalized on recent trends of consumers wanting more privacy protection online. Avast claimed its software would block annoying tracking cookies and prevent services from tracking users' online activity.[7] Avast sold the very information it purported to protect.[8] This bait and switch is especially harmful: consumers took steps to protect their privacy by using Avast's software only to have their sensitive browsing information sold to third parties. As consumers have demanded more privacy protections and less tracking in recent years, large data collectors and tech companies have sought to attract new users and differentiate themselves from competitors by making privacy protective promises. EPIC encourages the Commission to continue to hold companies accountable where they lead consumers to falsely believe that their privacy is more protected while engaging in contradictory, invasive data practices.

EPIC also commends the Commission for banning Avast from selling or otherwise disclosing customers' web browsing information for advertising purposes. However, EPIC urges the Commission to extend this prohibition to sales or disclosures made for other purposes, such as sales and disclosures to government contractors for national security purposes. While the Commission's complaint does not allege that Avast sold its customers' web browsing data to government contractors, Avast did sell this data to brokers, many of whom may sell that data to government contractors for national security purposes.

EPIC has been encouraged by the Commission's recent work underscoring the sensitivity of particular types of personal data and establishing heightened legal safeguards for this data. As the Commission found in its X-Mode Social order, sale of sensitive data—in that case, location data—to government contractors for national security purposes "would be material to consumers in deciding whether to use or grant location permissions to mobile apps."[9] That same logic applies to consumers using services that collect and sell internet browsing data. As Chair Khan, Commissioner Slaughter, and Commissioner Bedoya emphasized, "[a] person's browsing history can reveal extraordinarily sensitive information[,]" including "everything from someone's romantic interests, financial struggles, and unpopular political views to their weight-loss efforts, job rejections, and gambling addiction."[10] And the sale of internet browsing data to government contractors would be material to consumers deciding whether to use particular services.[11] Therefore, we urge the Commission to

[7] Complaint, *supra* note 2, at 2.
[8] *Id.*
[9] *Id.* at 5.
[10] Statement of Chair Lina M. Khan, *In re Avast Ltd. et al.*, FTC File No. 202-3033 1 (Feb. 21, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2024.02.21StatementofChairKhanRegardingAvast.pdf.
[11] Government agencies and their contractors continue to purchase significant amounts of web browsing data and other internet metadata, often routed through data brokers. *See, e.g.*, Charlie Savage, *N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says*, N.Y. Times (Jan. 25, 2024), https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html; Joseph Cox, *Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data*, Motherboard (Sept. 21, 2022), https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data.

prohibit the specific deceptive practice of selling web browsing data to defense contractors for national security purposes in the final Order and any analogous orders in the future.

As we noted in recent comments, the Commission's "explicit emphasis on the sale of data to government contractors for national security purposes is an encouraging step toward reining in the cottage industry of data brokers and other firms unlawfully trafficking in Americans' most sensitive information."[12] EPIC continues to believe that the Commission's proposed orders in *X-Mode Social* and *Avast* send a strong signal "not only to data brokers [. . .] but to the government agencies underwriting the data broker industry by purchasing location data and other sensitive information about Americans, knowing full well that this information has been obtained through unlawful trade practices."[13]

EPIC commends the Commission for banning the sale and disclosure of web browsing information for advertising purposes, which we hope will severely curtail the downstream sale for other purposes. However, we remain concerned that merely prohibiting the sale of sensitive data for advertising purposes misses other concrete harms, including harms from the sale of this data to government contractors for national security purposes.

With respect to Provisions I.B and I.C of the Order, EPIC believes that the best way to mitigate harms from the collection, use, disclosure, and retention of sensitive personal information like browsing data is a comprehensive data minimization framework instead of a system that relies on each individual user to grant or withhold consent. Under a robust data minimization framework, using browsing data for most advertising purposes or disclosing browsing data obtained from non-Avast products to third parties would constitute an impermissible secondary data use that violates the reasonable expectations of the consumer.[14] Indeed, effective data minimization rules would prohibit *all* harmful, out-of-context secondary data uses. To ensure that Avast's handling of personal information is as limited as possible and conforms to the reasonable expectations of consumers, EPIC recommends that the final Order incorporate express collection, processing, retention, and transfer limits in the Provision V Mandatory Privacy Program.

EPIC commends the Commission again for taking enforcement action against Avast and for protecting consumers from the harmful practices of data aggregators. EPIC encourages the Commission to adopt the Order with two revisions: a broader prohibition on the sale or disclosure of browsing data that includes sales and disclosures to government contractors for national security purposes, and a comprehensive data minimization framework that imposes across-the-board collection, processing, retention, and transfer limits on Avast. Please feel free to reach out to EPIC Counsel Sara Geoghegan at geoghegan@epic.org if you have any questions.

---

[12] Comments of EPIC, Demand Progress, & EFF, *In re X-Mode Social, Inc.*, FTC File No. 202-3038 5 (2024), https://epic.org/wp-content/uploads/2024/02/EPIC-comments-in-re-X-Mode.pdf.
[13] *Id.* at 5; *see also* Letter from Ron Wyden, U.S. Sen., to Avril Haines, Dir. Nat'l Intel. (Jan. 25, 2024), https://static01.nyt.com/newsgraphics/documenttools/0117fa5f9ff7ae33/fe33e1ba-full.pdf.
[14] Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC (May 4, 2023), https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/.

Sincerely,

/s/ John Davisson
EPIC Director of Litigation &
Senior Counsel

/s/ Sara Geoghegan
EPIC Counsel

/s/ Chris Baumohl
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)