Volume 3, Number 1 January–February 2025

THE JOURNAL OF FEDERAL AGENCY ACTION

fastcase FULL COURT PRESS

The Journal of Federal Agency Action

Volume 3, No. 1 | January–February 2025

THE JOURNAL OF FEDERAL AGENCY ACTION (ISSN 2834-8818 (online)) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Leanne Battle
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

This journal's cover includes a photo of Washington D.C.'s Metro Center underground station. The Metro's distinctive coffered and vaulted ceilings were designed by Harry Weese in 1969. They are one of the United States' most iconic examples of the brutalist design style often associated with federal administrative buildings. The photographer is by XH_S on Unsplash, used with permission.

Cite this publication as:

The Journal of Federal Agency Action (Fastcase)

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF FEDERAL AGENCY ACTION, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in federal agency actions.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at 866.773.2782

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2834-8796 (print)
ISSN 2834-8818 (online)

Federal Trade Commission's Enforcement Action Against Avast Signals Increased Focus on Consumer Web Data

Kirk J. Nahra, Ali A. Jessani, and Amy Olivero*

In this article, the authors summarize the Federal Trade Commission's complaint and final order against Avast Limited and provide some key takeaways from the decision.

The Federal Trade Commission (FTC) has been actively flexing its authority as a privacy regulator in recent months. The agency has been especially focused on identifying data practices it views to be "unfair," thereby essentially creating substantive obligations for how companies are permitted to use data. The FTC's recent enforcement action and order against Avast Limited is one example of this trend.

The FTC recently announced its finalized order prohibiting the sale or licensing of any web browsing data for advertising purposes against Avast and two of its subsidiaries, including Jumpshot Inc. The FTC's case against Avast focused primarily on allegations of misrepresentations about the company's collection, retention, and sale of its consumers' browsing information and insufficient consumer notice regarding the disclosure of consumer data to over 100 third parties.

Through this action, the FTC established that it considers re-identifiable browsing information to be sensitive data. This browsing information can include data such as a user's search queries; the URLs of web pages visited; domains of third-party cookies embedded in ads, videos, or web banners of a user's visited URL; domains of images pulled from visited URLs, and the value of cookies placed on consumers' devices by third parties. In its complaint against Avast, the FTC stated that this browsing information "reveal[s] consumers' religious beliefs, health concerns, political leanings, location, financial status, visits to child-directed content,

The Journal of Federal Agency Action / January–February 2025, Vol. 3, No. 1, pp. 37–43.

ISSN ISSN 2834-8818 (online).

and interest in prurient content." Here, the agency asserted that this information should not have been sold, transferred, or disclosed to third parties without first obtaining affirmative consent from consumers and was thus an "unfair" practice.

This article summarizes the FTC's complaint and final order against Avast and provides some key takeaways from the decision.

Summary of the Complaint

Avast develops and produces cybersecurity software designed to limit and prevent third-party tracking on users' devices. According to the FTC, however, Avast's browser extensions and software also enable it to track users' browsing information with greater detail than ordinary third-party tracking. The FTC alleged three primary violations stemming from Avast's handling of consumers' browsing information and the associated statements, policies, and practices.

Specifically, the FTC stated the following to be an unfair or deceptive practices in violation of Section 5 of the FTC Act.

- *Unfair Collection, Retention, and Sale of Consumers' Browsing Information*

The complaint explained that some of Avast's main products, such as software and browser extensions—which were designed to identify and address potential risks to consumers' privacy and security—also collected eight petabytes of consumer data over a period of approximately six years. The FTC alleges that from 2014 to 2020, Avast, through its subsidiary, Jumpshot, sold large quantities of this data to over 100 third parties via Jumpshot products called "data feeds." These data feeds "provided third-party data buyers with extraordinary detail regarding how consumers navigated the Internet, including each webpage visited, precise timestamp, the type of device and browser, and the city, state, and country." According to the FTC, although Avast sold data feeds in non-aggregate form, many of these feeds included a unique and persistent device identifier that some third parties later used to trace identifiable individuals' browsing activity. Some of the agreements with these third parties allegedly stated directly the recipient's intention to reidentify individuals through re-association

while others contained some contractual limitations but were not monitored or assessed for compliance.

- *Inadequate Disclosure of Consumer Tracking*

The FTC's complaint noted a significant discrepancy between Avast's "marketing hook," which was primarily based on protecting users' privacy and security, and its actual tracking of consumer data and associated privacy statements, for the 2014-2020 period. Moreover, Avast allegedly continued to profit off sales of consumer data (through the sale of Jumpshot data products) without sufficiently informing its users that numerous third parties could "track and target consumers across multiple devices." This included data such as the web pages consumers visited; precise time stamps of the visits; the type of device and browser used; and the city, state, and country of the user. Furthermore, Avast's disclosures were not always triggered by consumer action (e.g., users could download certain Avast products without ever receiving a pop-up notification pertaining to the collection, use, sale, or disclosure of their data of third-party tracking) and/or these disclosures were allegedly hard to find and hard to understand.

- *Misrepresentations Regarding Aggregation and Anonymization of Data*

The FTC's complaint alleges that even where Avast described potential disclosures of consumers' browsing information to third parties, the company misrepresented how it would disclose such data. Until 2018, Avast's privacy policy failed to inform consumers that third parties would have any access to their browsing information outside the law enforcement or service provider context. In its own web forum, Avast even claimed that their aggregation of data prevented the reverse-engineering capable of tracing data back to specific users. Although Avast described certain privacy policies on its own forum, the FTC depicted the forum as a technical-oriented informational site that individuals had to seek out to learn more. The agency also claims Avast's forum made numerous false statements, including that they aggregated all user data when the company allegedly provided Jumpshot with non-aggregate data, which was later re-packaged and sold to additional third parties.

Key Provisions from the Final Consent Order

In addition to the $16.5 million fine, the highest monetary remedy for a de novo privacy violation under Section 5(a) of the FTC Act, the FTC imposed several other mandates on Avast, such as the following.

- *A Prohibition on the Sale or Disclosure of Browsing Information*

Avast faces restrictions around the sale, license, transfer, share, and disclosure of browsing information. Avast can no longer engage in disclosure of browsing information derived from any Avast product, even after obtaining consumer consent.

However, the FTC has not completely banned Avast's use or disclosure of browsing information in certain contexts. Avast may disclose browsing information from non-Avast products for advertising purposes upon obtaining affirmative express consent from the consumer. Additionally, the mere use of any browsing information by Avast for advertising purposes cannot be done until after the data subject has given affirmative express consent. The FTC opted for a rather broad definition of "advertising purposes," which further restricted potential Avast efforts to utilize consumer data as a corporate asset. The process of obtaining affirmative express consent may also restrict Avast's ability to profit from browsing information. Avast must provide clear and conspicuous notice detailing if and how browsing information will be used, sold, or otherwise disclosed by both Avast and any third party involved before a user can consent to such action.

- *Data and Model Deletion*

The prohibition on disclosure of browsing information from Avast products applies not only to the data itself but also to the products and services incorporating that information, such as any models or algorithms. The Final Order instructs Avast to delete "the Jumpshot Data and any models, algorithms, or software developed by Jumpshot based on the [their data]." The FTC has recently made efforts for complete disgorgement by requiring companies to destroy any artificial intelligence models that were created using allegedly improperly collected data. To ensure this data can no longer be used for profit, the agency also required Avast to instruct

third parties in possession of Jumpshot data or its by-products to delete or destroy such information. Jumpshot data may only be retained for purposes required by the government or otherwise by law and must be deleted within 30 days after the obligation's expiration.

- *Notice to Consumers*

Avast, a company that once marketed itself primarily based on consumer privacy and security, must provide clear and conspicuous notice to those same consumers that Avast sold their data, without consent, to third parties. The FTC has also required Avast to inform those same consumers of this action against the company. This requirement entails directing consumers to a prewritten notice by providing the linked notice:

1. On the Avast website,
2. On Avast products involved in the collection of browsing information from 2014 to 2020, and
3. In emails sent to any user who purchased an Avast product prior to January 30, 2020.

- *Implement Comprehensive Privacy Program*

Similar to other previous FTC Final Orders, Avast must implement a comprehensive privacy program with biennial third-party assessments for 20 years. The program must be documented in writing, provided to the Avast board of directors or equivalent governing body, and overseen by a designated qualified employee. This provision also requires the installation of safeguards designed to protect covered information based on the amount and sensitivity of covered information at risk.

Key Takeaways

Treat Browsing Information as Sensitive Data and Consider Establishing an Affirmative Express Consent Model Before Collecting

The action against Avast illustrates the FTC's heightened concern around web browsing information and its emphasis that this

data can reveal a great deal of highly sensitive information about a consumer. Under this understanding, browsing information, when aggregated and combined with other data sources, may result in reidentification of the individual consumer. Through the Avast enforcement action, the FTC adds web browsing information to a growing list of what it considers sensitive information that merits heightened protection. (In early 2024, the FTC's enforcement actions against X-Mode and InMarket added health and geolocation data to this list.) Companies should consider obtaining the affirmative express consent from any consumers prior to the disclosure of their browsing information to any third party.

Review Consumer Privacy and Security Claims to Ensure They Accurately Reflect Data Practices and Operations

The FTC's complaint took significant issue with Avast's "marketing hook," which claimed to prevent the exact type of third-party tracking Avast enabled through Jumpshot's sale of data feeds. This focus in the enforcement action illustrates the important of disclosures that accurately inform users how products collect, retain, and use their data. Companies should consistently ensure that any privacy policies, marketing materials, and public statements are in line with the business' legitimate efforts to support privacy and security-related claims.

Exercise Stronger Oversight Over Contractual Provisions Limiting Third Parties' Use of Disclosed Data

Companies should consider performing due diligence assessments to determine whether the third-party companies they enter into contracts with have the capabilities and intentions to comply with any data use limitations written into contracts. Through the Avast action, the FTC has put companies on notice that the agency will hold them accountable for failures to vet third parties who may seek to use a company's data for purposes prohibited by the contract, such as re-identifying users for targeted advertising.

Monitor the FTC's Increasing Fines Against Companies for Privacy Violations

Deceiving consumers by selling their sensitive data without affirmative express consent or sufficient disclosures of the company's intent to sell data may result in significant monetary liability. The agency will seek to provide redress to consumers, especially in situations where it believes companies have viewed consumer data as a windfall for their business. Although certain sensitive data transfers may seem profitable, settlement payments, reputational harm, and mandatory privacy obligations will likely outweigh any short-term gains for your business.

The FTC Will Use Its Enforcement Authority Against Domestic And International Companies for Privacy Violations

The FTC's complaint charges that UK-based Avast and two of its subsidiaries, Czech Republic-based Avast Software and U.S.-based Jumpshot operated as a common enterprise that was subject to FTC authority. Significantly, Jumpshot operations were shut down in 2020, so the current FTC privacy obligations for Avast target its operations outside of the United States. Multinational companies should be aware that data practices outside the United States could still fall within FTC authority.

Note

* The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at kirk.nahra@wilmerhale.com, ali.jessani@wilmerhale.com, and amy.olivero@wilmerhale.com, respectively. Mike Charbonneau, a 2024 summer associate at the firm, assisted in the preparation of this article.