Privacy & Cybersecurity
Alert

Weil

March 19, 2024

FTC Privacy Fines Are Now Extraterritorial

By Olivia Greer and Alexis Bello

The FTC has fined a UK business $16.5 million over allegations that it – along with its Czech and U.S. subsidiaries – systematically collected and sold consumers' browsing data in direct violation of promises it made to consumers about protecting their data. The order, which also imposes expansive privacy obligations on the remaining businesses, is unique in its extraterritorial reach, as well as in its focus on the potential sensitivity of consumer internet browsing data.

On February 22, 2024, the Federal Trade Commission ("FTC") issued a decision against Avast Limited, a United Kingdom limited liability company ("Avast Ltd"), Avast Software s.r.o., a Czech Republic limited liability company ("Avast Software") and Jumpshot, Inc., a Delaware corporation ("Jumpshot", together with Avast Ltd and Avast Software, "Avast").[1] The Complaint alleges that Avast had, between 2014 and 2020, sold the browsing information of its customers in connection with such customers' use of its software products that were advertised to "block annoying tracking cookies that collect data on your browsing activities" and "protect [their] privacy by preventing . . . web services from tracking [their] online activity."[2] The Decision and Consent Order impose, in addition to the $16.5 million fine, substantial requirements concerning deletion of the data at issue and ongoing obligations with respect to Avast's privacy practices.

Privacy Enforcement Under the FTC Act

Section 5(a) of the Federal Trade Commission Act of 1914 ("FTC Act") empowers the FTC to investigate and take action to prevent unfair or deceptive acts or practices affecting commerce. In recent years, the FTC has been active in using its authority to investigate alleged privacy violations, particularly in instances when companies are viewed as misleading consumers regarding safeguards of their personal information. Since the FTC's landmark 2019 order requiring Facebook, Inc. to pay a $5 billion penalty based on allegations that it deceived users about their ability to control the privacy of their personal information, the FTC has issued more than twenty privacy-related orders.[3] Recently, the FTC issued an order against X-Mode Social, Inc. and its successor Outlogic, LLC, prohibiting them from sharing or selling any sensitive location data after allegations that the company sold precise location data that could be used to track people's visits to sensitive locations without fully informing consumers about such sales and without implementing reasonable or appropriate safeguards around the precise location data it sold.[4]

[1] Decision & Order, *Avast Limited*, *et al.*, FTC File No. 2023033 (Feb. 22, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/D%26O-Avast.pdf [hereinafter Order].

[2] Complaint at *9, *Avast Limited, et al.*, FTC File No. 2023033 (Feb. 15, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-Avast.pdf [hereinafter Complaint].

[3] Federal Trade Commission, "Privacy and Security Enforcement," available at https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited March 12, 2024).

[4] *See* Decision & Order, *X-Mode Social, Inc. and Outlogic, LLC,* FTC File No. 2123038 (Jan. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf.

None of these previous privacy actions have implicated a foreign-based business. However, there appears to be nothing preventing the FTC from enforcing Section 5 of the FTC Act against foreign-based entities. Indeed, "unfair or deceptive acts or practices" explicitly include "such acts or practices *involving foreign commerce* that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States."[5] In this case, although Jumpshot is a Delaware corporation, it is a wholly-owned subsidiary of Avast Ltd, a UK company.

The Avast Complaint and Consent Agreement

Avast distributes software (including browser extensions and antivirus programs) marketed as protecting users' privacy and personal information online.[6] Between 2014 and 2020, according to the Complaint, Jumpshot sold browsing information of Avast users to business customers in an identifiable form that enabled those business customers to track individuals' internet activity across devices over time.[7]

According to the Complaint, the various versions of Avast's privacy policy, until 2018, did not disclose that consumers' browsing information would be shared to third parties (outside a law enforcement or service provider context).[8] In 2018, Avast's privacy policy was revised to state that browsing information would be disclosed to third parties to be used in cross-product direct marketing, cross-product development and trend analytics, but stated (wrongly, according to the Complaint) that such information was pseudonymized and anonymized.[9] In Avast's 2019-revised privacy policy, Avast stated that it shared aggregated, de-identified datasets of Avast user data with Jumpshot, when Jumpshot in fact received granular, non-aggregated browsing information.[10]

The FTC Complaint alleged that Avast (i) unfairly collected consumers' browsing information, storing it in granular form indefinitely and selling it to third parties, without providing adequate notice to or obtaining consent from its customers; (ii) deceptively represented that its software would prevent the collection and sale of consumers' browsing information while itself selling such data through Jumpshot; and (iii) deceptively represented that browsing information would be transferred to Jumpshot and to third parties only in aggregate and anonymous form.

After the FTC provided Avast with its draft Complaint, the parties entered into the Consent Agreement, which incorporates the Order.[11] In addition to the $16.5 million fine, Avast is subject to an array of additional requirements and restrictions, including:

A. Deletion of Jumpshot data and models. Avast must delete any data Jumpshot received, as well as all models and algorithms trained on such data, and instruct any third party that has received browsing information, models or algorithms from Jumpshot to delete or destroy the same.[12]

B. Restrictions on data disclosures. Avast is categorically banned from selling or disclosing browsing information from its own products and from selling or disclosing any models or algorithms derived from its own customer browsing information.[13] It is further restricted from selling or disclosing browsing information from a non-Avast product or using its own browsing information for advertising purposes without first obtaining affirmative express consent.[14]

---

[5] 15 U.S.C. § 45(a)(4)(A).

[6] Complaint, *supra* note 2, at *2.

[7] *Id.* at *5.

[8] *Id.* at *9.

[9] *Id.* at *9-10 (Although Avast represented that it had developed an algorithm to remove identifiers from datasets, according to the Complaint, the algorithm was ineffective and the data was sold in identifiable, non-aggregated formats).

[10] *Id.*

[11] Agreement Containing Consent Order, *Avast Limited, et al.*, FTC File No. 2023033 (Feb. 22, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/ACCO-Avast.pdf.

[12] Order, *supra* note 1, at *9.

[13] *Id.* at *8.

[14] *Id.*

C. Implementation of compliant privacy program and practices. Avast is prohibited from providing misleading representations of its privacy practices (including the purpose of the collection, use and disclosure of customer data, the extent to which such data is aggregated or anonymized and how such data is protected).[15] Further, Avast is required to implement a comprehensive privacy program that is documented and regularly evaluated and tested, including by third party experts.[16]

D. Ten years of FTC monitoring. Avast must submit a compliance report, sworn under penalty of perjury, one year following the date of the Consent Agreement. For ten years thereafter, Avast must submit a compliance notice within 14 days of any change to Avast's designated point of contact or corporate structure.[17]

Key Takeaways

While the facts of the Avast matter are somewhat extreme – more than 5 years of allegedly deceptive data practices – there are lessons to be learned for any multinational business that handles consumer information.

- **The FTC's reach is extraterritorial**. The FTC can, and will, enforce Section 5 against an organization based outside the U.S., when the alleged actions of that organization can be found to have an impact in U.S. commerce. Such a finding is likely easy to make where the entity has a U.S. subsidiary with which it shares data.
- **Internet browsing data is sensitive data**. With this action, the FTC has sought to make clear that internet browsing data is sensitive data.[18] Further, where such data is represented to be anonymized or aggregated but can be re-identified, the data remains sensitive and subject to "heightened privacy obligations and a default presumption against its sharing or sale."[19]
- **Algorithmic and data disgorgement is the new normal**. When the FTC finds a business has misled consumers with respect to how and why their data is used, the FTC now regularly orders that the data at issue be deleted, *along with all models and algorithms trained on that data*.[20]
- **Violations can lead to ongoing oversight**. Once the FTC identifies potential privacy violations, a business is likely to stay on the FTC's radar for a significant period of time. Ongoing and regular required reporting is not unusual,[21] and businesses will need to ensure that they continue to comply with the given order, as well as maintain good data hygiene and privacy practices broadly.

* * *

[15] *Id.* at *9.

[16] *Id.* at *9-10.

[17] *Id.* at *16.

[18] Press Release, FTC, Statement from FTC Chairwoman Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro M. Bedoya, *Avast Limited, et al.*, FTC File No. 2023033 (Feb. 21, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2024.02.21StatementofChairKhanRegardingAvast.pdf, ("Because it is intrinsically sensitive, browsing data warrants heightened protection.").

[19] *Id.*

[20] *See, e.g.*, Final Order, *Cambridge Analytica, LLC*, FTC Docket No. 9383 (Dec. 6, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf; Decision & Order, *Everalbum, Inc.*, FTC Docket No. C-4743 (May 7, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf; Stipulated Order, *U.S. v. Kurbo Inc. and WW International, Inc.*, No. 3:22-cv-00946-TSH (N.D. Cal. Mar. 3, 2022); Stipulated Order, *U.S. v. Amazon.com, Inc. and Amazon.com Services, LLC*, No. 2:23-cv-00811-TL (W.D. Wash. Jul. 19, 2023); Stipulated Order, *FTC v. Rite Aid Corp. and Rite Aid Headquarters Corp.*, No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024).

[21] *See, e.g.*, Stipulated Order, *U.S. v. Amazon.com, Inc. and Amazon.com Services, LLC*, No. 2:23-cv-00811-TL at *16 (W.D. Wash. Jul. 19, 2023); Stipulated Order, *U.S. v. Kurbo Inc. and WW International, Inc.*, No. 3:22-cv-00946-TSH at *10 (N.D. Cal. Mar. 3, 2022).

Privacy & Cybersecurity Alert is published by the Privacy & Cybersecurity practice group of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Privacy & Cybersecurity practice group, please speak to your regular contact at Weil or to authors:

Authors

Olivia Greer (NY)	View Bio	olivia.greer@weil.com	+1 212 310 8815
Alexis Bello (NY)	View Bio	alexis.bello@weil.com	+1 212 310 8316