2023033

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of **AVAST LIMITED, a United Kingdom limited liability company,** **AVAST SOFTWARE S.R.O., a Czech Republic limited liability company, and** **JUMPSHOT, INC., a Delaware company.**	**DOCKET NO. C-4805**

COMPLAINT

The Federal Trade Commission, having reason to believe that Avast Limited, a limited liability company, Avast Software s.r.o., a limited liability company, and Jumpshot, Inc., a Delaware company, have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Avast Limited ("Avast Ltd") is a United Kingdom limited liability company with its principal place of business at 100 New Bridge Street, London EC4V 6JA, England. Respondent Avast Ltd is the indirect parent company of Respondent Avast Software s.r.o. and Respondent Jumpshot, Inc.

2. Respondent Avast Software s.r.o. ("Avast Software s.r.o." and, collectively with Avast Ltd, "Avast") is a Czech Republic limited liability company with its principal place of business at Enterprise Office Center, Pikrtova 1737/1A, 140 00 Prague 4, Czech Republic. Respondent Avast Software s.r.o. is a wholly-owned, indirect subsidiary of Avast Ltd.

3. Respondent Jumpshot, Inc. ("Jumpshot") is a Delaware corporation with its principal place of business at Suite 450, 9300 Harris Corners Parkway, Charlotte, NC 28269. Respondent Jumpshot was a wholly-owned subsidiary of Avast Ltd prior to the closing of Jumpshot's operations in January 2020.

4. Respondents Avast Ltd, Avast Software s.r.o., and Jumpshot (collectively, "Respondents") have operated as a common enterprise while engaging in the unlawful acts and practices alleged below. Respondents have conducted the business practices described below through interrelated companies that have common ownership, officers, managers, business functions, employees, and office locations, and that commingled funds. Because the Respondents have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below.

5. As detailed below, from at least 2014 to the present day, Respondents distributed software that they promoted with a variety of privacy claims. During this time period, Respondents have claimed their software 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." In fact, from 2014 through January 2020, Respondents sold the browsing information that they purported to protect, in many instances without notice to users. Furthermore, where they did describe their information practices, Respondents claimed that any sharing of user information would be in "anonymous and aggregate" form. In fact, Respondents sold consumers' browsing data to third parties in non-aggregate, re-identifiable form. Respondents failed to obtain consumers' consent to engage in these practices and deceived consumers about their conduct.

6. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Collection of Browsing Information

7. Since at least 2014, Respondents have collected consumers' browsing information through browser extensions and antivirus software installed on consumers' computers and mobile devices.

8. Browser extensions are software programs that can modify or extend the functionality of consumers' web browsers. Respondents developed and distributed two browser extensions that collected information about consumers' browsing activities: Avast Online Security and AVG Online Security (collectively, "the Avast Extensions"). Respondents also distribute the "Avast Secure Browser," a browser that comes pre-installed with the Avast Online Security browser extension.

9. Antivirus software programs for consumers' computers or mobile devices are designed to identify and address potential risks to consumers' privacy or security, such as malware. Avast Software s.r.o. developed and distributed antivirus software for Windows computers and Android devices that collected information about consumers' browsing activities: Avast Free Antivirus ("Avast Desktop Software") and Avast Antivirus – Mobile Security & Virus Cleaner ("Avast Mobile Software").

10. Ostensibly to provide security and privacy services, Respondents used the Avast Extensions, the Avast Secure Browser, Avast Mobile Software, and Avast Desktop Software (collectively, "Avast Software") to collect browsing information from users of these products

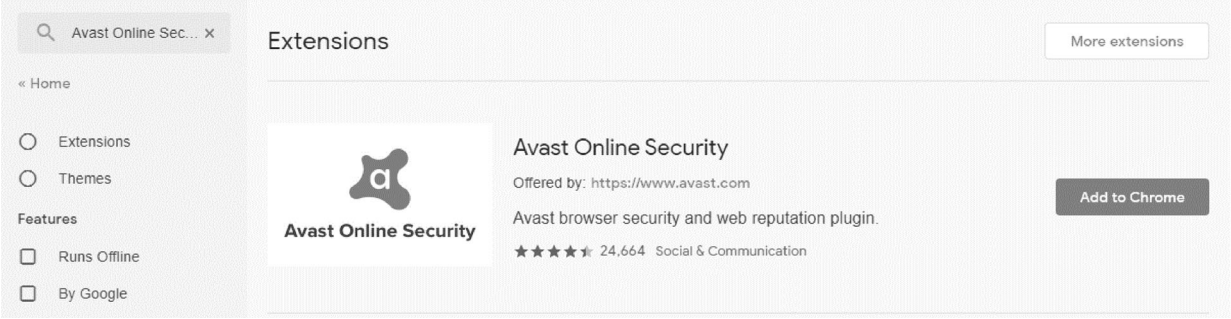
("Avast users"), including: uniform resource locators (URLs) of webpages visited; the URLs of background resources (such as the domains of third parties placing cookies, or of images pulled from domains other than the displayed URL); consumers' search queries; and the value of cookies placed on consumers' computers by third parties.

Representations Regarding the Purpose of Respondents' Products

11. Respondents advertised the privacy and security functionality of the Avast Software on webpages Respondents maintained or controlled, where consumers were able to download the Avast Software.

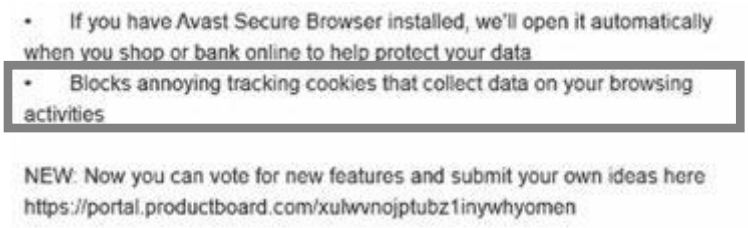
Respondents' Browser Extensions

12. Respondents described the Avast Extensions in the Chrome Web Store as protecting privacy and security. A consumer that searched for "Avast Online Security" in the Chrome Web Store could install the extension without viewing any disclosures about Respondents' collection or sale of browsing information or seeing a link to Avast's privacy policy. The Avast Online Security extension could be installed using the "Add to Chrome" button on the search result page, as shown here:



The description for the AVG Online Security results page was the same as for the Avast Online Security results page.

13. For consumers who clicked past the search results page and viewed the information page for each Avast Extension, Respondents failed to disclose any information about their collection or sale of browsing information. Indeed, Respondents affirmatively represented that the extensions would decrease tracking on the Internet, as shown on the information page for the Avast Online Security extension:

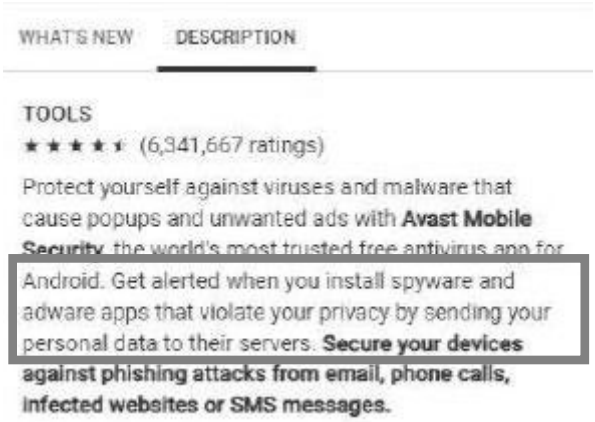


The information page highlights seven features of the extension, including that the product "[b]locks annoying tracking cookies that collect data on your browsing activities." The

information page for AVG Online Security was identical to the information page for Avast Online Security. In fact, as described below at Paragraphs 18–30, the Avast Extensions tracked consumers' browsing activities more extensively than could ordinary tracking cookies.

Respondents' Mobile Software

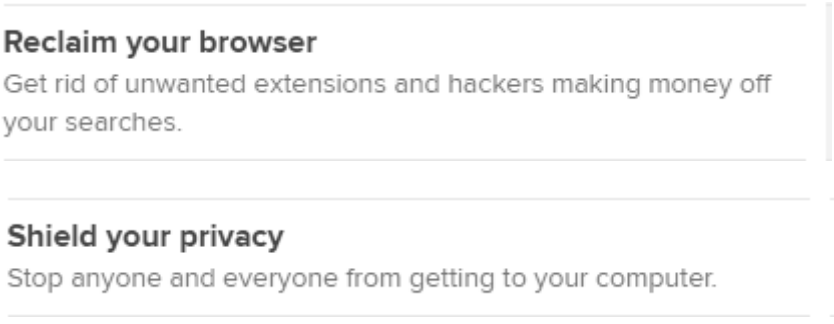
14. The information page for Avast Mobile Software also affirmatively represented that the product would enhance consumer privacy while browsing the Internet:



These disclosures equate apps that are "sending your personal data to their servers" with "spyware and adware," and state that Avast Mobile Software will provide alerts when this occurs. Once installed, as described below at Paragraphs 18–30, the Avast Mobile Software itself sent consumers' personal data to Avast's servers, and some of that data was ultimately sold to third parties.

Respondents' Desktop Software

15. Since at least 2015, on the download page for the Avast Desktop Software, Avast included the following representations, which consumers would view prior to downloading the software:



Avast represented that its software would "[s]hield your privacy. Stop anyone and everyone from getting to your computer." Avast also represented that its software would allow consumers to "[r]eclaim your browser. Get rid of unwanted extensions and hackers making money off your searches." Avast continued to make these claims until February 2017.

16. Beginning in April 2018, Avast began to distribute the Avast Secure Browser, which came pre-installed with an Avast Browser Extension, which was not visible to the consumer and which could not be uninstalled. Avast marketed the Avast Secure Browser for its privacy features, including making the following representations on the download page, which consumers viewed prior to choosing to download the software:

In this image, Avast Software s.r.o. represents 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."

17. Consumers who purchased the premium versions of Avast Software were told that it would "remove ads" or "remove third-party advertising." As discussed below at Paragraphs 18–30, however, Respondents still sold those consumers' browsing information to third parties.

Sale and Use of Browsing Information

18. Prior to its acquisition by Avast Software s.r.o. in 2013, Jumpshot was a competing antivirus company. In early 2014, Avast Software s.r.o. rebranded Jumpshot as an analytics company, which advertised that its "[m]ore than 100 million online consumers worldwide" would give Jumpshot's customers "unique insights to make better business decisions." Jumpshot offered its customers the ability to "[s]ee where your audience is going before and after they visit your site or your competitors' sites, and even track those who visit a specific URL."

19. From 2014 through January 2020, Jumpshot sold browsing information that Avast collected to a variety of clients, including consulting firms, investment companies, advertising companies, marketing data analytics companies, individual brands, search engine optimization firms, and data brokers.

20. Using a proprietary algorithm developed by Avast, Avast and Jumpshot purported to find and remove identifying information prior to each transfer of consumer browsing information to Jumpshot's servers. But this process was not sufficient to anonymize consumers'

browsing information, which Jumpshot then sold, in non-aggregate form, through a variety of different products to third parties.

21. Many of the Jumpshot products (or "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. Most of the data feeds included a unique and persistent device identifier associated with each particular browser ("Jumpshot GUID"), allowing Jumpshot and the third-party buyer to trace individuals across multiple domains over time.

22. Jumpshot data feed products included the "All Clicks Feed" (all URLs clicked during particular consumers' browsing sessions); "Search Plus Click Feed" (consumers' search terms plus the selected results); "Insights Feed" (all commerce "events"—e.g., consumers' searches, adding items to a shopping cart, and purchases on a domain); "Transaction Feed" (details on each purchase event, such as price, brand, seller); "Marketplace Feed" (all consumer interactions with a particular product across multiple domains); and "Cookie Feed" (consumer clickstream data filtered based on cookie values provided by Jumpshot's customers, allowing Jumpshot's customers to assess behavior on domains where the third party was not able to place a cookie directly).

23. Jumpshot entered unique contracts with large data buyers to provide a large number of custom data feeds that permitted invasive uses of consumers' browsing information. For example, from May 2017 to April 2019, Jumpshot granted LiveRamp, a data company that specializes in various identity services, a "world-wide license" to use consumers' granular browsing information, including all clicks, timestamps, persistent identifiers, and cookie values, for a number of specified purposes. One specified purpose was "targeting, messaging and other data driven marketing activities served to consumers and businesses." Other terms appear to permit LiveRamp to use Jumpshot's consumer data to track and target consumers across multiple devices.

24. One agreement between LiveRamp and Jumpshot stated that Jumpshot would use two services: first, "ID Syncing Services," in which "LiveRamp and [Jumpshot] will engage in a synchronization and matching of identifiers," and second, "Data Distribution Services," in which "LiveRamp will ingest online Client Data and facilitate the distribution of Client's Data (i.e., data segments and attributes of its users associated with Client IDs) to third-party platforms for the purpose of performing ad targeting and measurement." These provisions permit the targeting of Avast consumers using LiveRamp's ability to match Respondents' persistent identifiers to LiveRamp's own persistent identifiers, thereby associating data collected from Avast users with LiveRamp's data.

25. In August 2018, Jumpshot entered into a contract with Lotame, a data enrichment company, that permitted Lotame to "match[], combin[e], append[], and model[]" Jumpshot's data with Lotame's data, and then "license such Modeled Data to customers of Lotame's products and services." The contract expressly permitted Lotame to use Jumpshot data, combined with its own, "for marketing purposes, including targeting of digital advertisements and digital content." The parties agreed that Jumpshot would receive a share of the revenue that

Lotame earned through the targeting of consumer audiences made up of, or derived from, browsing information held by Jumpshot.

26. In December 2017, Jumpshot entered into a contract with Omnicom, an advertising conglomerate. The contract between Jumpshot and Omnicom stated that Jumpshot would provide Omnicom with an "All Clicks Feed" for 50% of its customers in the United States, United Kingdom, Mexico, Australia, Canada, and Germany. Jumpshot's "All Clicks Feed" ordinarily was limited to clicks associated with a particular domain; for example, an investment company might purchase the "All Clicks Feed" for the domains of a potential investment target. In the Omnicom contract, however, Jumpshot agreed to provide the "All Clicks Feed" for 50% of its entire user base, across all domains. According to the contract, Omnicom was "allowed to map out/translate Jumpshot GUIDs into [data broker Neustar's] Neustar IDs. Customer can also match with LiveRamp." These provisions permitted Omnicom to associate Respondents' data with other sources of data, on an individual user basis. The contract also permitted Omnicom to "transmit, market and sublicense" to its own customers products derived from the raw data. The production fee schedule stated in the first work order to the contract was approximately $2 million per year.

27. Some of the contracts, including the agreement between LiveRamp and Jumpshot, did not prohibit the data buyer from re-identifying Avast users based on data that Jumpshot provided. In other instances, Jumpshot prohibited data buyers from re-identifying Avast users, but those prohibitions were limited. The Jumpshot contracts that did prohibit re-identification defined re-identification as associating personally-identifiable information (such as a consumer's home address) with the browsing information—meaning such data buyers were free to associate non-personally-identifiable information with Avast users' browsing information. Indeed, in some cases, it was clear that the client was purchasing the data to do just that. And Jumpshot failed to audit or otherwise confirm that its data buyers complied with such prohibitions.

28. Respondents, through Jumpshot, sold consumers' browsing information to more than 100 customers, beginning in 2014. Jumpshot earned tens of millions in gross revenues by selling user data collected by the Avast Software, and insights derived from such data, to its customers.

29. After the Commission issued a civil investigative demand, Respondents announced on January 30, 2020, that they would shut down Jumpshot's operations. In an open letter posted on Avast's website explaining the decision, Avast's CEO stated: "I—together with our board of directors—have decided to terminate the Jumpshot data collection and wind down Jumpshot's operations, with immediate effect."

30. Through the entire period that Jumpshot received browsing information from Avast, Jumpshot never deleted any of the data. By January 2020, Jumpshot had more than eight petabytes of browsing information dating back to 2014.

Representations Regarding Disclosure of Browsing Information

31. While Respondents made prominent claims touting the privacy and security features of its products, Respondents in many instances failed to disclose that consumers'

browsing information would be sold to third parties, or misrepresented how such data would be disclosed. For example, until 2018, Respondents' privacy policy did not indicate that consumers' browsing information would be disclosed to third parties outside a law enforcement or service provider context, and when the policy was revised in 2018, the revised policy misrepresented how the data was disclosed, as discussed below.

32. Respondents first provided details about their data sales practices in 2015, but only to individuals who participated in Avast forums, a technically-oriented informational site hosted by Avast for users to exchange information about Avast products. And, even this technically-oriented post misrepresented the privacy protections for consumers' browsing information.

33. In a May 30, 2015, post on Avast's web forum, Avast's Chief Technology Officer highlighted Avast's "recent[] . . . investment in a marketing analytics platform called Jumpshot," and explained:

> To further protect our users' privacy, we only accept websites where we can observe at least 20 users. This ensures that no reverse engineering is possible on the aggregated data—there's nothing that can lead back to a specific user. All aggregated data is then stored . . . on a per-domain and keyword basis. These aggregated results are the only thing that Avast makes available to Jumpshot customers and end users.

In fact, as described above at Paragraphs 18–30, Respondent Jumpshot received from Respondent Avast Software s.r.o., and provided Jumpshot customers with, non-aggregate data. Not only did Jumpshot provide data that could lead back to a specific user, but the entire purpose of some of the Jumpshot products was to enable clients to track specific users or even to associate specific users—and their browsing history—with identifiers known to the Jumpshot customer and in turn to information the Jumpshot customer had associated with that identifier.

34. This forum post also described the notice that Respondents would provide during the installation process:

> Avast is committed to protecting its customers on all fronts, which is why we inform our users, even beyond our EULA and Privacy policy, that their browsing information will be collected but stripped of personally identifiable information and will be used to help us better understand new and interesting trends. We actually tried to make this very, very explicit, and that's why we have an extra step in the Avast installer which informs our users in a very straightforward way about what we're doing.

In fact, contrary to this promise, Respondents only provided a pop-up notification during the installation of one of their products—the Avast Desktop Software. No such notification was provided during the installation process for any other product, and no notification was provided to Avast users (including Avast Desktop Software users) who had already downloaded Avast Software, even though Respondents not only sold information collected from those users on a going-forward basis but also information that had previously been collected from those users in

2014. And, at least one version of the pop-up notification for the Avast Desktop Software claimed, incorrectly, that the data collected "is fully de-identified and aggregated."

35. Respondents included a privacy setting that enabled users of the Avast Mobile Software to turn off third-party data sharing (the default setting allowed disclosure of browsing information to third parties). Respondents did not disclose the existence of this setting either before or during the installation process—consumers would have to explore their settings to find it after downloading the software. Even if they did find the setting, the description of the setting indicated incorrectly that data the consumer permitted to be shared with third parties would be anonymized:

36. The online download pages of the Avast Software products contain links to Respondents' privacy policy. Prior to October 2018, Respondents' sale of consumers' browsing information to third parties through Jumpshot was not disclosed in the privacy policy. Privacy policies prior to October 2018 stated that browsing information would be collected only "to ascertain the source of [malware] infection" and that these products "collect no more information than is required in order to provide full functionality." These policies stated that personally identifiable information would be provided to third parties only when required by law or in the context of a service provider.

37. Beginning in October 2018, Respondents stated in their privacy policy for the first time that browsing information, referred to in the policy as "Clickstream Data," would be disclosed to third parties, but indicated that "[w]e pseudonymize and anonymize the Clickstream Data and re-use it for cross-product direct marketing, cross-product development and third party trend analytics." In the same policy, Respondents stated, "[w]e also share statistical data that has been anonymized and aggregated geographically and so cannot be used to identify individuals, with third parties for trend analytics." Respondents' privacy policy defined "anonymized" as "removing or de-identifying all specific identifiers . . . . When we refer to anonymous data, we mean data that cannot be reversed into personal data."

38. In 2019, Respondents revised their privacy policy to indicate that certain data would be disclosed to Respondent Jumpshot:

This statement represents, among other things, that "all that Jumpshot gets is an aggregated, de-identified data set of online trends." In fact, as described above at Paragraphs 18–30, Jumpshot received granular, non-aggregate browsing information from Avast.

39. Respondents removed the "Trend Analytics" language from its privacy policy in December 2019, after Google banned the Avast Extensions for violating the Chrome Web Store's policy, in place since April 2016, which prohibits "[c]ollection and use of web browsing activity . . . except to the extent required for a user-facing feature described prominently in the Product's Chrome Web Store page and in the Product's user interface."

Consumer Harm Related to Browsing Information

40. The vast majority of consumers would not know that the Avast Software would surveil their every move on the Internet or that their browsing information might be sold to more than 100 third parties and stored indefinitely, in granular, re-identifiable form.

41. Re-identifiable browsing information is sensitive data. Among other things, the Avast Extensions and Avast Antivirus Software collected browsing information—including web searches and webpages visited—revealing consumers' religious beliefs, health concerns, political leanings, location, financial status, visits to child-directed content, and interest in prurient content. For example, a sample of just 100 entries out of trillions retained by Respondents showed visits by consumers to the following pages: an academic paper on a study of symptoms of breast cancer; Sen. Elizabeth Warren's presidential candidacy announcement; a CLE course on tax exemptions; government jobs in Fort Meade, Maryland with a salary greater than $100,000; a link (then broken) to the mid-point of a FAFSA (financial aid) application; directions on Google Maps from one location to another; a Spanish-language children's YouTube video; a link to a French dating website, including a unique member ID; and cosplay erotica.

42. Respondents combined this type of information with persistent identifiers—including identifiers created by Respondents that identified each consumer's device uniquely, as well as identifiers collected directly from consumers' devices—as well as coarse location information. The fact that browsing information was linked to an identifier over time increased the likelihood that a consumer could be reidentified.

43. Respondents had direct evidence that many consumers did not want their browsing information to be sold to third parties, even when they were told that the information would only be shared in de-identified form. In 2019, when Avast asked users of other Avast antivirus software to opt-in to the collection and sale of de-identified browsing information, fewer than 50% of consumers did so.

VIOLATIONS OF THE FTC ACT

Count 1
Unfair Collection, Retention, and Sale of Consumers' Browsing Information

44. As described in Paragraphs 7–10 and 18–30, through the Avast Software, Respondents collected consumers' browsing information, stored that information in granular form indefinitely, and sold that information in granular form to third parties, without adequate notice and without consumer consent.

45. These 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. These practices are unfair acts or practices.

Count 2
Deceptive Failure to Disclose Tracking of Consumers

46. In numerous instances, including through the means described in Paragraphs 11–17, Respondents represented, directly or indirectly, expressly or by implication, that the Avast Software would stop the collection and sale of consumers' browsing information.

47. Respondents failed to disclose, or failed to disclose adequately, to consumers that that Respondents, through the Avast Software, collected and sold consumers' browsing information as alleged in Paragraphs 7–10 and 18–30. These facts would be material to consumers in their decision to use Respondents' services.

48. Respondents' failure to disclose or disclose adequately the material information described in Paragraph 47, in light of the representation set forth in Paragraph 46, is a deceptive act or practice.

Count 3
Misrepresentations Regarding Aggregation and Anonymization

49. In numerous instances, including through the means described in Paragraphs 31–39, Respondents represented, directly or indirectly, expressly or by implication, that consumers' browsing information would be transferred to Respondent Jumpshot and to third parties only in aggregate and anonymous form.

50. In fact, as set forth in Paragraphs 18–30, Respondents transferred to Respondent Jumpshot, and to third parties, consumers' browsing information in non-aggregate and non-anonymous form. Therefore, the representation set forth in Paragraph 49 is false or misleading.

Violations of Section 5

51. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this **26th** day of **June** 2024, has issued this complaint against Respondents.

By the Commission, Commissioners Holyoak and Ferguson not participating.

April J. Tabor
Secretary

SEAL:

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

2023033

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of
AVAST Limited, a United Kingdom limited liability company,
AVAST SOFTWARE S.R.O., a Czech Republic limited liability company, and
JUMPSHOT, INC., a Delaware corporation.

DOCKET NO. C-4805

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

a. Respondent Avast Limited ("Avast Ltd"), a United Kingdom limited liability company with its principal place of business at 100 New Bridge Street, London EC4V 6JA, England. Respondent Avast Ltd is the indirect parent company of Respondent Avast Software s.r.o. and Respondent Jumpshot, Inc.

b. Respondent Avast Software s.r.o. ("Avast Software s.r.o.," collectively with Avast Ltd, "Avast"), a Czech Republic limited liability company with its principal place of business at Enterprise Office Center, Pikrtova 1737/1A, 140 00 Prague 4, Czech Republic. Respondent Avast Software s.r.o. is a wholly-owned, indirect subsidiary of Avast Ltd.

c. Respondent Jumpshot, Inc. ("Jumpshot"), a Delaware corporation with its principal place of business at Suite 450, 9300 Harris Corners Parkway, NC 28269. Respondent Jumpshot was a wholly-owned, indirect subsidiary of Avast Ltd prior to the closing of Jumpshot's operations in January 2020.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For the purposes of this Order, the following definitions apply:

A. **"Affirmative Express Consent"** means any freely given, specific, informed, and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any "privacy policy," "terms of service," "terms of use," or other similar document, of all information material to the provision of consent. Acceptance of a general or broad terms of use or similar document that contains descriptions of agreement by the individual along with other, unrelated information, does not constitute Affirmative Express Consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute Affirmative Express Consent. Likewise, agreement obtained through a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, does not constitute Affirmative Express Consent.

B. **"Avast Product"** means: (1) any product or service offered by Avast Ltd, Avast Software s.r.o., or Jumpshot, Inc., or any business controlled, directly or indirectly, by Avast Ltd, Avast Software s.r.o., or Jumpshot, Inc., as of September 12, 2022; and (2) any other product or service offered by Respondents after September 12, 2022, that is branded, or marked, advertised, or marketed as provided by, Avast or Jumpshot. For

purposes of Provision IV, Avast Product means: Avast Online Security; AVG Online Security; Avast Secure Browser; Avast Antivirus – Mobile Security & Virus Cleaner; Avast Free Antivirus; and Avast Premium Security.

C. **"Browsing Information"** means, in whole or in part, any uniform resource locators (URLs) of page requests, the URLs of background resources, search queries, form values, and the value of cookies placed on consumers' computers by a Third Party corresponding to the consumers' navigation of the World Wide Web collected from consumers or their devices.

D. **"Clear(ly) and Conspicuous(ly)"** means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made in only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. On a product label, the disclosure must be presented on the principal display panel.

6. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.

7. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

8. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

9. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

E. **"Covered Information"** means information from or about an individual consumer or consumer's device, including: (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) a financial institution account number; (6) credit or debit card information; (7) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; (9) geolocation information; or (9) Browsing Information.

F. **"Deidentified"** means information that cannot reasonably identify, be associated with, or be linked, directly or indirectly, to a particular consumer or consumer's device, provided that Respondents:

1. Have implemented technical safeguards to prevent reidentification of the consumer to whom the information pertains;

2. Have implemented business processes that specifically prohibit reidentification of the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified information; and

4. Make no attempt to reidentify the information.

G. **"Jumpshot Data"** means all Browsing Information that Jumpshot received from Avast.

H. **"Respondents"** means Avast Ltd, a United Kingdom limited liability company, Avast Software s.r.o., a Czech Republic limited liability company, and Jumpshot, Inc., a Delaware corporation, and their successors and assigns, individually, collectively, or in any combination.

I. **"Third Party"** means any individual or entity other than: (1) Respondents; (2) a service provider of Respondents that: (a) uses or receives Covered Information collected by or on behalf of Respondents for and at the direction of Respondents and no other individual or entity, (b) does not disclose the Covered Information, or any individually identifiable information derived from such information, to any individual entity other than Respondents or a subcontractor to such service provider bound to data processing terms no less restrictive than terms to which the service provider is bound, and (c) does not use the data for any other purpose; or (3) any entity that uses Covered Information only as reasonably necessary: (a) to comply with applicable law, regulation, or legal process, (b) to enforce Respondents' terms of use, or (c) to detect, prevent, or mitigate fraud or security vulnerabilities.

Provisions

I. Ban on Sale or Disclosure of Browsing Information

IT IS ORDERED that Respondents, and Respondents' officers, agents, and employees who receive actual notice of this Order must not:

A. Sell, license, transfer, share, or otherwise disclose to or with a Third Party, for Advertising Purposes: (1) Browsing Information from any Avast Product; (2) any information product or service derived from or incorporating Browsing Information from any Avast Product; or (3) any models or algorithms derived from Browsing Information from any Avast Product;

B. Use Browsing Information for Advertising Purposes without first obtaining Affirmative Express Consent; or

C. Sell, license, transfer, share, or otherwise disclose to or with a Third Party, Browsing Information from any non-Avast Product, for Advertising Purposes, without first obtaining Affirmative Express Consent.

When obtaining Affirmative Express Consent required under this Provision, Respondents must provide notice Clearly and Conspicuously that identifies the Browsing Information that will be used, sold, licensed, transferred, shared, or otherwise disclosed, and each purpose for which Browsing Information will be used, sold, licensed, transferred, shared, or otherwise disclosed, including by any Third Party.

D. For purposes of this Provision, "Advertising Purposes" means:

1. Advertising, marketing, promoting, offering, or selling any products or services on, by, or through Third Party websites, mobile applications, or services.

2. Advertising Purposes shall not include: (a) communications, services, or products requested by a consumer that are sent or provided to the consumer; (b) advertising, marketing, promoting, offering, or selling Respondents' own products or services, and its jointly marketed, co-branded, or white-labeled products or services; (c) reporting or analytics related to understanding advertising or advertising effectiveness, such as statistical reporting, traffic analysis, measuring or understanding the number and type of ads served, or conversion or impression measurement, provided that any Third Party reporting or analytics service is restricted from using any Browsing Information from any Avast Product for any purpose other than to provide the reporting and analytics services to Respondents; or (d) contextual advertising, meaning short-term, transient use of Browsing Information for non-personalized advertising shown as part of a user's current interaction with Respondents provided that the user's Browsing Information is not disclosed to a Third Party and is not used to build a profile about the user or otherwise alter the user's experience outside the current interaction with Respondents. Respondents

shall not be deemed to have disclosed Browsing Information in connection with a user's direct interaction with an advertisement.

II. Prohibited Misleading Representations

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the collection, use, disclosure, or maintenance of Covered Information, must not misrepresent in any manner, expressly or by implication:

A. The purpose of their collection, use, disclosure, or maintenance of Covered Information;

B. The extent to which Covered Information is aggregated or anonymized; or

C. The extent to which they collect, use, disclose, or maintain Covered Information, or otherwise protect the privacy, security, availability, confidentiality, or integrity of any Covered Information.

III. Data Deletion

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, and employees who receive actual notice of this Order must:

A. Within twenty (20) days of the effective date of this Order, delete: the Jumpshot Data and any models, algorithms, or software developed by Jumpshot based on the Jumpshot Data. Respondents must provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information, models or algorithms, and software have been deleted or destroyed.

B. Within twenty (20) days of the effective date of this Order, instruct any Third Party that has received Browsing Information from Jumpshot to delete or destroy such information, models or algorithms derived therefrom, and any software developed to analyze Browsing Information, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that Respondents issued such instructions. Respondents must promptly submit all correspondence, including demand letters, responsive letters, and any written statements required by this Provision, to the Commission pursuant to Provision XII of this Order.

Provided, however, that any Browsing Information that any Respondent is otherwise required to delete or destroy pursuant to this provision may be retained, and may be disclosed, as requested by a government agency or otherwise required by law, regulation, court order, or other legal obligation, including as required by rules applicable to the safeguarding of evidence in pending litigation. In each written statement to the Commission required by this Provision, such Respondent shall describe in detail any Browsing Information that Respondent retains on any of these bases and the specific government agency, law, regulation, court order, or other legal obligation that prohibits Respondent from deleting or destroying such information. Within thirty

(30) days after the obligation to retain the information has ended, Respondent shall provide an additional written statement to the Commission, sworn under penalty of perjury, confirming that Respondent has deleted or destroyed such information.

IV. Notice to Users

IT IS FURTHER ORDERED that on or before twenty-eight (28) days after the effective date of this Order, Respondents must:

A. Post Clearly and Conspicuously on Respondents' websites https://www.avast.com/ and https://www.avg.com a link to an exact copy of the notice attached hereto as Exhibit A ("Exhibit A Notice") for a period of one hundred and eighty (180) days following the date of the issuance of this Order;

B. Post Clearly and Conspicuously a notification on Avast Products which collected Browsing Information between August 1, 2014 and January 30, 2020 that directs consumers to the Exhibit A Notice on a Sub-Provision IV.A website for a period of one hundred and eighty (180) days following the date of the issuance of this order; and

C. Send the Exhibit A Notice to users who purchased or downloaded any Avast Products that collected Browsing Information prior to January 30, 2020, and for whom Respondents possess email contact information obtained between August 1, 2014 and January 30, 2020. The Exhibit A Notice shall be sent through email without any other information, documents, or attachments, with the subject line "Notice of FTC Settlement."

V. Mandated Privacy Program

IT IS FURTHER ORDERED that each Respondent that collects, uses, discloses, or maintains Covered Information must, within sixty (60) days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program (the "Program") that protects the privacy of such Covered Information. To satisfy this requirement, each Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program and evaluations thereof to the Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for the Program at least once every twelve (12) months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months, internal and external risks to the privacy of Covered Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the privacy of Covered Information identified in response to Sub-

Provision V.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information. Such safeguards must also include:

1. Training of all employees, at least once every twelve (12) months, on how to safeguard the privacy of Covered Information;

2. Technical measures to modify Browsing Information to render it Deidentified;

3. Documentation, for each product or service, of the decision to collect, use, share, disclose, or maintain Browsing Information, including by operation of any third-party software within the product or service. Such documentation should include: the name or names of the person or people who made the decision; for what purpose the Browsing Information is being collected, used, shared, or disclosed; the data segmentation controls in place to ensure that the Browsing Information collected is only used for the particular purpose for which it was collected; the data retention limit set and the technical means for achieving deletion; safeguards in place to prevent unauthorized sharing or sale; and the access controls in place to ensure only authorized employees with a need-to-know have access;

F. Assess, at least once every twelve (12) months, the sufficiency of any safeguards in place to address the internal and external risks to the privacy of Covered Information, and modify the Program based on the results;

G. Test and monitor, including by technical means, the effectiveness of the safeguards at least once every twelve (12) months, and modify the Program based on the results;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from each Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy of Covered Information;

I. Consult with, and seek appropriate guidance from, independent, third-party experts on privacy in the course of establishing, implementing, maintaining, and updating the Program; and

J. Evaluate and adjust the Program in light of any changes to the Respondent's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in Sub-Provision V.D of this Order, or any other circumstances that the Respondent knows or has reason to know may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, each Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order, titled Mandated Privacy Program, each Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessment must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Program; (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment; and (4) will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. The Assessor shall not withhold any such documents on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim, although such documents can be designated for confidential treatment in accordance with applicable law;

B. For each Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission ("Associate Director") with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period:

1. Determine whether each Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy Program;

2. Assess the effectiveness of each Respondent's implementation and maintenance of Sub-Provisions V.A-J;

3. Identify, through technical testing and any other assessment technique, any gaps or weaknesses in, or instances of material noncompliance with, the Program;

4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were identified in any prior Assessment required by this Order; and

5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and technical testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of the Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions

or attestations by the Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by the Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that any Respondent revises, updates, or adds one or more safeguards required under Provision V of this Order in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re Avast Limited et al.*" All subsequent biennial Assessments must be retained by Respondents until the Order is terminated and provided to the Associate Director for Enforcement within 10 days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

VII. Cooperation with Third Party Assessor

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondents' networks and all of Respondents' IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy Program; (2) assessment of the effectiveness of the implementation and maintenance of Sub-Provisions V.A-J; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. Annual Certification

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this order titled Mandated Privacy Program, Respondents shall:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior officer of each Respondent who is responsible for Compliance with Provision V of this Order, that: (1) each Respondent has established, implemented, and maintained a Privacy Program that complies in all material respects with the requirements of Provision V of this Order; and (2) each Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior officer or subject-matter experts upon whom the senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, Respondents must submit all annual certifications to the Commission pursuant to this Order via email to DEBrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re Avast Limited et al.*

C. Respondents must publish all annual certifications Clearly and Conspicuously on a separate page in the "investors" section of Respondents' website (e.g., investors.avast.com).

IX. Monetary Relief

IT IS FURTHER ORDERED that:

A. Respondents must pay to the Commission $16,500,000, which Respondents stipulate their undersigned counsel holds in escrow for no purpose other than payment to the Commission.

B. Such payment must be made within 9 days of the effective date of this Order by electronic fund transfer in accordance with instructions provided by a representative of the Commission.

X. Additional Monetary Provisions

IT IS FURTHER ORDERED that:

A. Respondents relinquish dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission to enforce its rights to any

payment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.

C. The facts alleged in the Complaint establish all elements necessary to sustain an action by or on behalf of the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.

D. All money paid to the Commission pursuant to this Order may be deposited into a fund administered by the Commission or its designee to be used for relief, including consumer redress and any attendant expenses for the administration of any redress fund. If a representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after redress is completed, the Commission may apply any remaining money for such other relief (including consumer information remedies) as it determines to be reasonably related to Respondents' practices alleged in the Complaint. Any money not used is to be deposited to the U.S. Treasury. Respondents have no right to challenge any activities pursuant to this Provision.

E. In the event of default on any obligation to make payment under this Order, interest, computed as if pursuant to 28 U.S.C. § 1961(a), shall accrue from the date of default to the date of payment. In the event such default continues for 10 days beyond the date that payment is due, the entire amount will immediately become due and payable.

F. Each day of nonpayment is a violation through continuing failure to obey or neglect to obey a final order of the Commission and thus will be deemed a separate offense and violation for which a civil penalty shall accrue.

G. Respondents acknowledge that their Taxpayer Identification Numbers (Social Security or Employer Identification Numbers), which Respondents have previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

XI. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For three (3) years after the issuance date of this Order, each Respondent, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees and agents managing conduct related to the subject matter of this Order ; and (3) any business entity resulting from any change in structure as set forth in Provision XII. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XII. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which each Respondent must: (1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, Covered Information collected, used, disclosed, or maintained, the means of disclosing its Covered Information collection, use, disclosure, or maintenance practices, and the involvement of any other Respondent; (4) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. For ten (10) years after the issuance date of this Order, each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:

    1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of any Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,

Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re Avast Limited et al.*

XIII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 10 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondents, in connection with the collection, use, disclosure, or maintenance of Covered Information, must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

D. A copy of each widely disseminated representation by Respondents that describes the extent to which Respondents collect, use, disclose, or maintain Covered Information, or otherwise protect the privacy, security, availability, confidentiality, or integrity of any Covered Information, including any representation concerning a change in any website or other service controlled by Respondents that relates to the privacy of Covered Information;

E. For 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and

F. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIV. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested

information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XV. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioners Holyoak and Ferguson not participating.

April J. Tabor
Secretary

SEAL:

ISSUED: June 26, 2024

Exhibit A

The U.S. Federal Trade Commission, the United States' consumer protection agency, alleges that from August 2014 to January 2020, Avast, misrepresented how it would share browsing information collected from some of its products, specifically how it would share information in a deidentified form with its subsidiary Jumpshot. The FTC further alleges that Jumpshot sold some of that browsing information to over a hundred companies. Avast shut down Jumpshot in January 2020.

The FTC alleges that if you were a user of Avast or AVG software during that period, you may have been deceived by Avast's representations. The FTC further alleges that, in some cases, the data Avast shared with Jumpshot was not aggregated or fully anonymized before Jumpshot sold it, and in some cases, Jumpshot sold the data in a form that could have allowed third parties to link back browsing information to you or your devices.

What are we doing? On [DATE] we entered into a settlement with the FTC to resolve these allegations. You can learn about the case here: [ftc.gov/LINK]. As agreed in that settlement:

- **Avast will delete the Jumpshot data.** We will delete all browsing information from Jumpshot's databases and have reached out to the companies that bought data from Jumpshot, to ask that they do the same.

- **Avast will narrowly limit who it shares your data with.** The settlement with the FTC prohibits Avast from selling or sharing your browsing information for third-party advertising purposes.

How can you learn more? If you have any further questions or concerns, please email [dedicated @Avast.com email address] or call [dedicated 800-number]. We will get back to you within three business days.

Ondrej Vlcek

Avast Director

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 26, 2024

John Davisson
Sara Geoghegan
Chris Baumohl
Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036

Re: *In the Matter of Avast, Ltd., et al.*, File No. 202-3033

Dear Mr. Davisson, Ms. Geoghegan, and Mr. Baumohl:

Thank you for your comment regarding the Federal Trade Commission's ("FTC" or "Commission") proposed consent agreement in the above-titled proceeding against Avast, Ltd., et al. ("Avast"). Your comment discusses important issues, and we have given it serious consideration.

The complaint in this matter alleges that Avast engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges that Avast: (1) unfairly collected consumers' browsing information, stored that information in granular form indefinitely, and sold that information in granular form to third parties, without adequate notice and without consumer consent; (2) represented that the Avast software would stop the collection and sale of consumers' browsing information but failed to disclose, or to disclose adequately, that Avast collected and sold consumers' browsing information; and (3) misrepresented that consumers' browsing information would be transferred to Avast's subsidiary Jumpshot and to third parties only in aggregate and anonymous form.

The Electronic Privacy Information Center's ("EPIC") comment indicates support for the FTC's proposed consent agreement with Avast and praises the FTC for exercising its authority to investigate and take enforcement actions against companies that engage in unfair and deceptive practices. Additionally, your comment provides recommendations to strengthen the proposed order and future data security enforcement actions.

Specifically, your comment supports the proposed order's prohibition on Avast from selling or otherwise disclosing consumers' browsing information for advertising purposes. However, you also raise a concern that the FTC should extend this prohibition to sales or disclosures made for other purposes, such as sales and disclosures to government contractors for national security purposes. Your letter mentions that Avast sold consumers' browsing data to data brokers, who may sell that data to government contractors for national security purposes.

The Commission is committed to vigorously enforcing the proposed order and ensuring that Avast protects the privacy of its consumers' browsing information. The proposed order was crafted to address the allegations in the complaint, which does not include any factual allegations that Respondents or data brokers sold Avast's consumer browsing data to government contractors or any entity for national security purposes. The proposed order, however, includes numerous provisions that provide strong protections for the sale of consumer's browsing information, including to data brokers. For instance, the proposed order's prohibition on the sale of browsing information from Avast's products will prohibit Avast from selling browsing information to data brokers for advertising purposes, thus substantially limiting potential downstream uses of the data for any purpose. Additionally, the proposed order prohibits Avast from misrepresenting the extent to which it discloses consumers' browsing information for any purpose.

Your comment also suggests that the FTC include a comprehensive data minimization framework that incorporates express collection, processing, retention, and transfer limits in the proposed order's Mandated Privacy Program. The Commission agrees that data minimization is a crucial data security principle and is committed to utilizing its available enforcement mechanisms to their fullest extent. Moreover, the Commission has taken recent action to ensure companies prioritize deleting data when it is no longer in use. *See In the Matter of Drizly, Inc.* (Oct. 24, 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf.

The proposed order's Mandated Privacy Program includes several safeguards to mitigate internal and external risks to the privacy of consumers' browsing information. For instance, the proposed order requires Avast to implement technical measures to modify browsing information to render it deidentified. It also requires documentation of the data segmentation controls in place to ensure that browsing information collected is used only for the particular purpose for which it was collected; data retention limits and the technical means for achieving deletion; and safeguards to prevent unauthorized sharing or sale. Avast must also obtain independent third-party assessments that the mandated privacy program has been implemented effectively.

The Commission believes the proposed order offers substantial protections to consumers. The Commission has placed your comment on the public record, pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would best be served by issuing the Decision and Order in the above-titled proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. Thank you again for your comment.

By direction of the Commission, Commissioners Holyoak and Ferguson not participating.

April J. Tabor
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 26, 2024

Anonymous

Re: *In the Matter of Avast, Ltd., et al.*, File No. 202-3033

Dear Anonymous:

Thank you for your comment regarding the Federal Trade Commission's ("FTC" or "Commission") proposed consent agreement in the above-titled proceeding against Avast, Ltd., et al. ("Avast").

The complaint in this matter alleges that Avast engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges that Avast: (1) unfairly collected consumers' browsing information, stored that information in granular form indefinitely, and sold that information in granular form to third parties, without adequate notice and without consumer consent; (2) represented that the Avast software would stop the collection and sale of consumers' browsing information but failed to disclose, or to disclose adequately, that Avast collected and sold consumers' browsing information; and (3) misrepresented that consumers' browsing information would be transferred to Avast's subsidiary Jumpshot and to third parties only in aggregate and anonymous form.

Your comment calls on the FTC to prevent Avast from engaging in these unfair and deceptive practices in the future. The proposed order is specifically designed to address the misconduct alleged in the complaint and help ensure that Avast will not sell consumers' browsing data for advertising purposes nor make misrepresentations regarding the privacy of the browsing data that it collects. In addition, the proposed order requires Avast to implement a privacy program with specific safeguards aimed at addressing internal and external risks to the privacy of consumers' browsing information.

Your comment also suggests that consumers who trusted Avast because it said its products would protect the privacy of consumers' browsing data should be compensated. The FTC's proposed order includes a provision for $16.5 million in monetary relief, which the FTC will use for consumer redress. For additional information on redress, please visit: https://consumer.ftc.gov/consumer-alerts/2024/02/software-provider-avast-will-pay-165-million-compromising-consumers-privacy.

The Commission believes the proposed order offers substantial protections to consumers. The Commission has placed your comment on the public record, pursuant to Rule 4.9(b)(6)(ii) of

the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would best be served by issuing the Decision and Order in the above-titled proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. Thank you again for your comment.

By direction of the Commission, Commissioners Holyoak and Ferguson not participating.

April J. Tabor
Secretary