

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Avast Limited, Avast Software s.r.o., and Jumpshot, Inc.,

File No. 2023033

The Federal Trade Commission (the “Commission” or “FTC”) has accepted, subject to final approval, an agreement containing consent order from Avast Limited, Avast Software s.r.o., and Jumpshot, Inc. (“Respondents”).

The proposed consent order (“Proposed Order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

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

According to the Proposed Complaint, the Avast Software collected browsing information from consumers, including uniform resource locators (URLs) of webpages visited, the URLs of background resources, consumers’ search queries, and cookie values placed by third parties on consumers’ computers. Among other things, the Avast Software collected browsing information revealing consumers’ religious beliefs, health concerns, political leanings, location, financial status, visits to child-directed content, and interest in prurient content. Respondents combined this information with persistent identifiers, including identifiers created by Respondents that identified each consumer device uniquely, increasing the likelihood that consumers could be reidentified. As alleged in the Proposed Complaint, in many instances Respondents failed to disclose any information about their collection or sale of browsing information, and affirmatively represented that the Avast Software would “[b]lock[] annoying tracking cookies that collect data on your browsing activities” and “[s]hield your privacy.”

The Proposed Complaint alleges that after Avast acquired Jumpshot in 2013, Avast rebranded Jumpshot in 2014 as an analytics company. From 2014 to 2020, the Proposed Complaint alleges, Jumpshot sold browsing information collected by the Avast Software to customers such as consulting firms, investment companies, advertising companies, marketing data analytics companies, individual brands, search engine optimization firms, and data brokers. The Proposed Complaint alleges that, while Respondents purported to remove consumers’ identifying information before transferring browsing information to Jumpshot, the proprietary algorithm Avast developed and used to do so was not sufficient to anonymize the data, which Jumpshot then sold in non-aggregate form to its customers through a variety of products. In total, the Proposed Complaint alleges that Respondents sold consumers’ browsing information, and

insights derived from such data, to more than 100 customers, earning tens of millions in gross revenues. After receiving the FTC's civil investigative demand, Respondents shut down Jumpshot's operations "with immediate effect."

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

With respect to the first count, the Proposed Complaint alleges that Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. The vast majority of consumers would not know 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 in granular, re-identifiable form. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

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

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

Summary of the Proposed Order with Respondents

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

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

advertising, and to obtain affirmative express consent from consumers using non-Avast branded products before selling, licensing, transferring, sharing, or otherwise disclosing to third parties browsing information collected by such products for advertising.

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

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

Part IV requires that Respondents provide notice about the FTC's complaint and settlement with Respondents to consumers on the Avast websites, within Avast products, and via email to consumers who purchased or downloaded Avast products between 2014 and 2020.

Part V requires that Respondents establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

Part VI requires Respondents to obtain initial and biennial privacy program assessments by an independent, third-party professional for 20 years.

Part VII requires Respondents to disclose all material facts to the assessor required by **Part VI** and prohibits Respondents from misrepresenting any fact material to the assessments required by **Part VI**.

Part VIII requires each Respondent to submit an annual certification from a senior officer responsible for compliance with **Part V** that the Respondent has implemented the requirements of the Proposed Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

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

Parts XI-XIV are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance.

Part XV states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

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