DATA PRIVACY & SECURITY | FEBRUARY 23, 2024

FTC Fines Avast Limited for Collection and Sale of Consumer Browsing Data

Kelly Ruane Melchiondo

Avast Limited, a United Kingdom-based company that marketed its browser extensions and antivirus software to protect consumer privacy did just the opposite—storing consumer browsing data indefinitely and selling it without consent to third parties. On February 22, 2024, the FTC fined Avast $16.5 million for a data collection and sale scheme in which Avast and its subsidiaries were engaged from 2014 through 2020.

The FTC initiated an investigation of Avast and its wholly-owned subsidiaries, Avast Software, S.R.O., and Jumpshot, Inc., for violations of Sections 4 and 5 of the Federal Trade Commission Act dating back to at least 2014. The FTC alleged that Avast and its subsidiaries distributed software marketed to "block[] annoying tracking cookies that collect" consumer browser data, and protect consumer privacy by preventing web services from tracking consumers' online activity. Avast's browser extensions, antivirus software and apps collected URLs, search queries and the value of cookies that third parties placed on consumers' computers. According to the FTC, however, not only did Avast and its subsidiaries not protect consumer privacy as advertised, but they sold the "protected" browsing information from 2014 through 2020, without notice to or consent from users.

As alleged in the FTC's **Complaint**, Avast acquired Jumpshot, a competing antivirus company, in early 2014, and rebranded Jumpshot as an analytics company. From 2014 through 2020, Jumpshot sold the browsing information that Avast collected to consulting firms, investment companies, advertising agencies, and data brokers. The data provided buyers with "extraordinary detail regarding how consumers navigated the Internet," including timestamps, and unique device identifiers associated with each browser, which enabled Jumpshot and its buyers to trace individuals across multiple domains over time. Using information purchased from Jumpshot, buyers were able to engage in activities such as targeted messaging to consumers and businesses.

The FTC alleges that the "vast majority of consumers would not know that the Avast Software would surveil their every move on the Internet," and that the information collected revealed consumers' religious beliefs, their health concerns, political affiliations, locations, and other interests. The FTC charged Avast with unfairly collecting, retaining and selling consumer browsing information, deceptively failing to disclose tracking of consumers, misrepresenting that it would anonymize consumer data, and engaging in unfair and deceptive trade practices.

On February 22, 2024, the FTC and Avast agreed to a Consent Order, in which Avast agreed to pay $16.5 million. Avast also agreed not to (1) sell, license, transfer or otherwise disclose to a third party, for advertising purposes, any browsing information collected, without affirmative express consent from consumers, or to (2) misrepresent, expressly or by implication, the purpose of their collection, use, disclosure or maintenance of the information collected, the extent to which Avast anonymizes information. Avast also agreed to delete and destroy any information that Jumpshot had collected within 20 days, and to instruct its buyers to do the same. Avast also agreed that it and its subsidiaries would implement and maintain a comprehensive privacy program to protect the privacy of the information that it collects, and to certify annually that it had established and maintained that privacy program as ordered.

This is the latest FTC enforcement actions to target a company that misused or failed to safeguard sensitive consumer data. In the absence of federal laws protecting consumer privacy, the FTC has taken the laboring oar on using Section 5 of the FTC Act, which prohibits deceptive and unfair trade practices, to impose hefty fines on companies for failing to protect sensitive data such as biometric data, sensitive health information, and now, browsing history. The common thread among all of these enforcement actions and penalties is consumer consent. Companies should always err on the side of clearly communicating their intents for data use and obtaining affirmative consent before using any data collected.

Related People

Kelly Ruane Melchiondo
Partner, Construction, Trial & Litigation