BEFORE THE
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of)
)
AnchorFree, Inc. Hotspot Shield VPN)
)
)
_____)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Center for Democracy & Technology (CDT)

I. Introduction

1. The Center for Democracy & Technology asks the Federal Trade Commission (Commission) to investigate the data security and data sharing practices of Hotspot Shield Free Virtual Private Network (VPN) services, a product of AnchorFree, Inc. Hotspot Shield Free VPN promises secure, private, and anonymous access to the internet. As detailed below, this complaint concerns undisclosed and unclear data sharing and traffic redirection occurring in Hotspot Shield Free VPN that should be considered unfair and deceptive trade practices under Section 5 of the FTC Act.

II. Parties

2. The Center for Democracy & Technology (CDT) is a nonprofit technology advocacy organization dedicated to preserving the user-controlled nature of the internet. CDT advocates for the protection of democratic values online, with projects on free speech, privacy, security, and internet architecture.

3. Hotspot Shield Free VPN ("Hotspot Shield") is a product offered by AnchorFree, Inc., a privately held corporation headquartered in California with offices in Switzerland. AnchorFree's primary place of business is listed on its website as 155 Constitution Drive,

Menlo Park, CA 94025. The company explains that its mission is to "drive universal online security, privacy and free access to content."[1]

III. Factual Background

4. A Virtual Private Network (VPN) is a technology that enables internet users to privately send and receive data across public networks. VPNs have been marketed as a privacy-protective technology that provide a way for internet users to obscure their personal information, including their web browsing history, from third parties including Internet Service Providers (ISPs) and governments.

5. VPNs have evolved from a technology used mostly in business-to-business transactions to one that has become popular with individual consumers.[2] A desire for more privacy and security online has contributed to a rise in consumer use of VPN services and apps.[3]

6. In March of 2017, Congress enacted a Congressional Review Act (CRA) to repeal privacy rules developed by the Federal Communications Commission that were to go into effect in 2018. The rules would have required ISPs to seek permission from customers for collecting and sharing sensitive personal information such as internet browsing history.[4]

7. In response to the repeal of the rules, public concern has prompted privacy advocates and others to point to VPNs as a viable way to regain some control over their private information.[5] After the repeal, Hotspot Shield VPN directly appealed to this concern in a blog post that said "[a]mong the ways users can protect their web information from being captured by third parties, including their ISPs, the best is arguably a VPN."[6] Since the

---

[1] AnchorFree website, About Page, https://www.anchorfree.com/about/team/ (last visited July 19, 2017).
[2] *See* Katie Young, *4 Things to Know About VPN Users,* GlobalWebIndex (Feb. 2, 2016), http://blog.globalwebindex.net/chart-of-the-day/4-things-to-know-about-vpn-users. The data collection and use practices of ISPs has recently warranted special attention from consumers. As the gatekeepers to internet access, ISPs have broad access to information about their customers' online activities and communications, granting ISPs a unique window into their customers' lives. It is possible to research tremendous insights into human behavior solely by analyzing internet transmission data.
[3] *See* Ariel Hochstadt, *VPN Use and Data Privacy Stats for 2017*, vpnMentor Blog (Jan.1, 2017), https://www.vpnmentor.com/blog/vpn-use-data-privacy-stats/.
[4] *See* Federal Communications Commission, Final Rules, § 64.2004 (Customer Approval), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.
[5] *See* Stephen Nellis & David Ingram, *Vote to Repeal U.S. Broadband Privacy Rules Sparks Interest in VPNs*, Reuters (March 28, 2017), http://www.reuters.com/article/usa-internet-privacy-idUSL2N1H52AA; Laura Hautala, *A VPN can protect your online privacy. But there's a catch*, CNET (Mar. 29, 2017), https://www.cnet.com/news/vpn-protect-online-privacy-its-complicated/.
[6] Chris San Filippo, *Don't Let ISPs Monetize Your Web History: Use Hotspot Shield*, Hotspot Shield Blog (Apr. 8, 2017), http://blog.hotspotshield.com/2017/04/08/dont-let-isps-monetize-web-history-use-hotspot-shield/.

CRA, many major VPN providers have reported a significant increase in downloads, subscriptions, and web traffic from U.S. internet users.[7]

A. Hotspot Shield Makes Strong Privacy and Security Claims That Are Contradicted By Its Privacy Policy

8. Hotspot Shield makes strong claims about the privacy and security of its data collection and sharing practices. CEO David Gorodyansky has stated that "we never log or store user data."[8] The company's website promises "Anonymous Browsing" and notes that Hotspot Shield keeps "no logs of your online activity or personal information."[9] Hotspot Shield further differentiates itself from "...disreputable providers [that] are able to offer free VPN services [ ] because they make their money tracking and selling their users' activities" by claiming that "Hotspot Shield neither tracks nor sells customers' information."[10]

9. These claims are highlighted as key features of the Hotspot Shield VPN mobile application. In iTunes, the application's description states that "Hotspot Shield doesn't track or keep any logs of its users and their activities. You are completely private with Hotspot Shield."[11]

[7] AJ Dellinger, *VPN Services Report Huge Increase In Downloads, Usage Since Broadband Privacy Rules Were Repealed*, International Business Times (Apr. 12, 2017), http://www.ibtimes.com/vpn-services-report-huge-increase-downloads-usage-broadband-privacy-rules-were-2524605.
[8] Shira Weiss, *"Improving the World" Through Internet Security: Chatting with David Gorodyansky, CEO of AnchorFree*, Huffington Post (May 1, 2017), http://www.huffingtonpost.com/entry/5907586ee4b05279d4edbe33.
[9] Hotspot Shield, Homepage, https://www.hotspotshield.com/ (last visited July 24, 2017).
[10] Levent Sapci, *A Beginner's Guide to Hotspot Shield VPN*, Hotspot Shield Blog (Jan. 19, 2016), http://blog.hotspotshield.com/2016/01/19/a-beginners-guide-to-hotspot-shield-vpn/. While Hotspot Shield offers a paid "elite" version of its VPN service that promises an "ad-free browsing experience," it does not state whether it continues to collect and share user information with third parties. *See also* Stephen Cooper, *Review: Hotspot Shield VPN Review 2017 – What's Changed?*, Best VPN (Jul. 19, 2017), https://www.bestvpn.com/hotspot-shield-review/ (finding that while "[t]he company states that advertising is removed for paid subscribers, [ ] that probably just means the display of the company website…hidden advertising structures are written into the software, so most likely continue for paid users").
[11] iTunes Preview Page for AnchorFree, Hotspot Shield VPN Unlimited Privacy Security Proxy iOS app. Retrieved on 7/26/17: https://itunes.apple.com/us/app/hotspot-shield-free-vpn-proxy-wi-fi-privacy/id443369807?mt=8.

Description

Hotspot Shield VPN Proxy is the World's most trusted security, privacy and access app with top performance on speed, stability and security.

GET HOTSPOT SHIELD VPN TO

– Access all websites and apps securely and privately at home, school, work or from anywhere in the world.

– Stay private and anonymous online. Prevent anyone from tracking your IP address, identity, and location from websites and online trackers.
Enjoy complete anonymity.

WHY HOTSPOT SHIELD VPN PROXY

– No Logs Kept: Hotspot Shield doesn't track or keep any logs of its users and their activities. You are completely private with Hotspot Shield.

Screenshots: Hotspot Shield VPN Description in iTunes/iOS App Store

10. Similarly, the description of the Hotspot Shield Free VPN Proxy & WiFi Security app provided in the Google Play Store states that "Hotspot Shield doesn't track or keep any logs of its users and their activities. Your security and privacy are guaranteed!"[12]

Hotspot Shield Free VPN Proxy & Wi-Fi Security

AnchorFree GmbH Tools 915,719

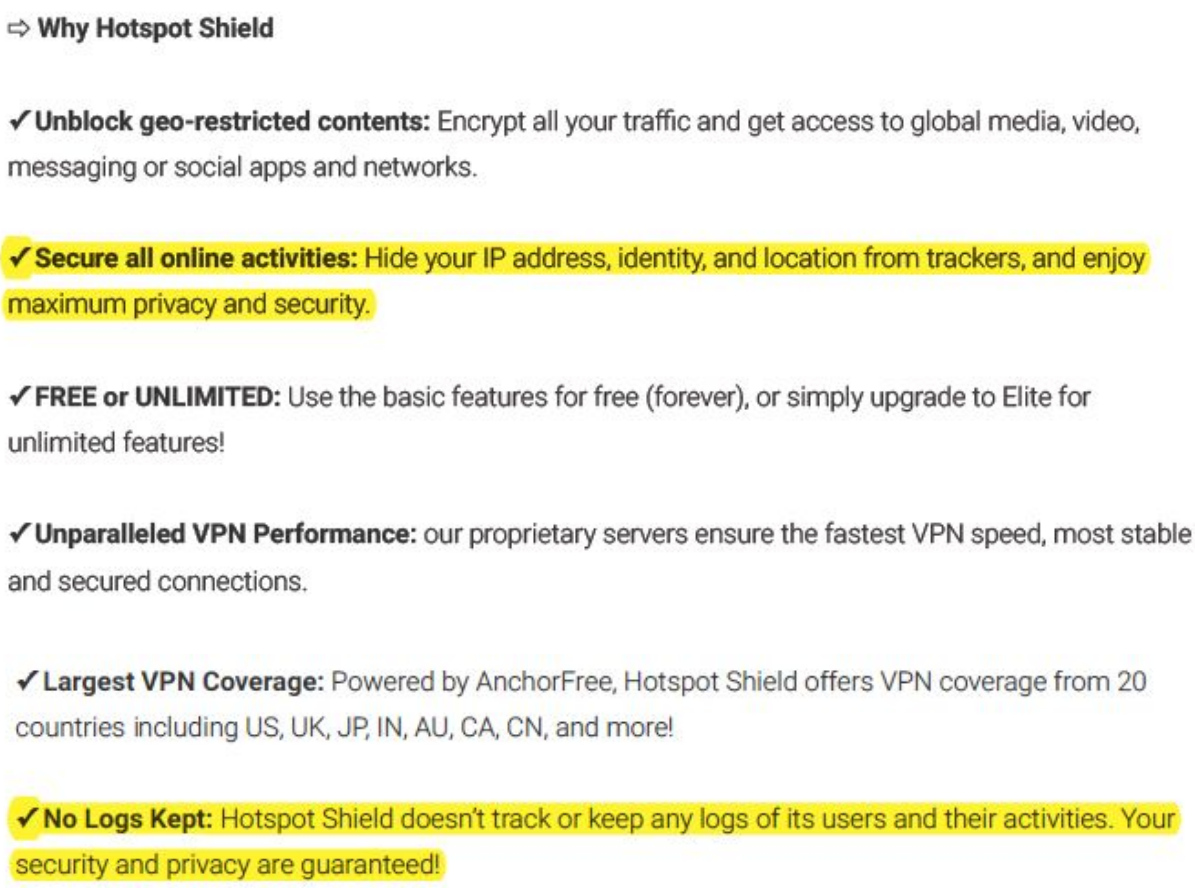
Everyone

Contains ads · Offers in-app purchases

This app is compatible with your device.

Disguise your online identity and access blocked apps and sites with Hotspot Shield, while keeping your mobile activities anonymous, private and secure!

[12] Google Play Store page for AnchorFree, Hotspot Shield Free VPN Proxy & Wi-Fi Security Android app, Retrieved on 7/26/17: https://play.google.com/store/apps/details?id=hotspotshield.android.vpn.



Screenshots: Hotspot Shield VPN Description in the Google Play Store

B. Hotspot Shield Engages in Logging Practices and Uses Third-Party Tracking Libraries to Facilitate Targeted Advertisements

11. Hotspot Shield's description for its iOS and Android mobile applications declares a "no logs" policy; however, its Privacy Policy,[13] which covers and includes its Hotspot Shield services, describes more elaborate logging practices.[14]

12. VPN providers generally create two types of logs: connection logs and usage logs. Connection logs include dates and timestamps corresponding to each user's VPN session duration, amount of data transferred, and can sometimes consist of incoming and

[13] Hotspot Shield, Privacy Policy, https://www.hotspotshield.com/privacy/ (last updated Apr. 22, 2015) [hereinafter "HSS Privacy Policy"].
[14] When using a VPN service, a user's internet connections are routed through servers either run by or controlled by the VPN provider. VPN providers may log data about this connection. These VPN logs serve a variety of functions, ranging from operations to delivery of third-party advertising.

outgoing IP addresses.[15] Connection logs are primarily used for troubleshooting technical issues.[16] By contrast, usage logs are much more inclusive. Specifically, usage logs contain software use and browsing history information, including websites accessed and files downloaded.[17]

13. VPN providers typically must engage in some logging either to monitor bandwidth or to enforce restrictions on the number of devices that can access the VPN service.[18]

14. While connection logs can be designed to be minimally privacy-invasive,[19] Hotspot Shield engages in logging practices around user connection data, beyond troubleshooting technical issues. The service uses this information to "identify [a user's] general location, improve the Service, or optimize advertisements displayed through the Service."[20] IP addresses, unique device identifiers, and other "application information" are regularly collected by Hotspot Shield.[21]

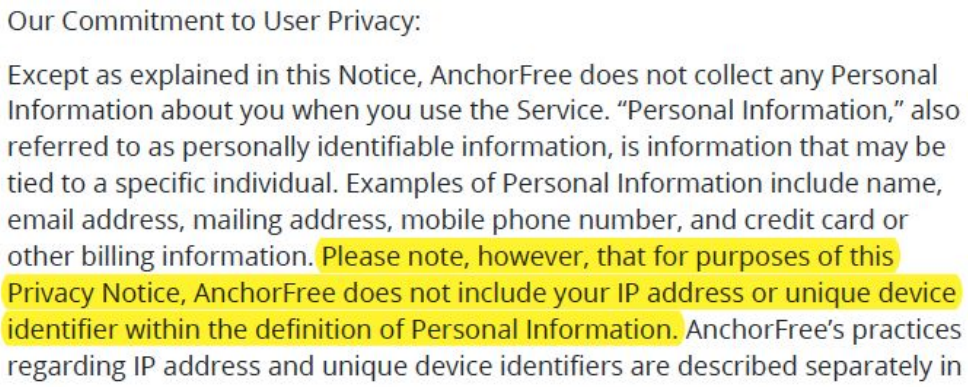
> ***"Automatically Collected" Information.*** When you use our Service, we may automatically record certain information by using different types of proprietary technology (such as cookies), which may include your IP address, unique device ID, or application information installed on your device. For example, we may collect your IP address when you commence your use of the Service; we do not, however, store logs associating your IP address with your online activities that take place when you are using of the Service. The automatically-collected information is used by AnchorFree only in the aggregate, in truncated form, or in order to generate a "hashed" or "virtual" IP Address. AnchorFree may use automatically-collected information to identify your general location, improve the Service, or optimize advertisements displayed through the Service.

Screenshot: Hotspot Shield VPN Privacy Policy

15. Importantly, the Privacy Policy makes clear that neither IP addresses nor unique device identifiers are considered to be personal information by Hotspot Shield.[22]

---

[15] *See* Sven Taylor, VPN Logs – What You Need to Know, RestorePrivacy (Mar. 27, 2017), https://restoreprivacy.com/vpn-logs/.
[16] *See id. See also VPN Logs*, Torrent VPN Guide, http://www.best-bittorrent-vpn.com/vpn-logs.html.
[17] *See* Taylor, *supra* at 15; Torrent VPN Guide, *supra* at 16.
[18] *See* Taylor, *supra* at 15.
[19] *See id.*
[20] *Id.*
[21] HSS Privacy Policy, *supra* at 13.
[22] HSS Privacy Policy, *supra* at 13. *Cf.* Definition of "Personally identifiable information" under the California Online Privacy Protection Act, which includes any identifier "that permits the physical or online contacting of a specific individual." Cal. Bus. & Prof. Code § 22577(a). The California Attorney General's Office interprets this category to include "information that is collected passively by the site or service, such as a device identifier or geo-location data." Making Your Privacy Practices Public, California Department of Justice (May 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.
This is a clarification that Hotspot Shield added to its latest iteration of its Privacy Policy. Compare HSS Privacy Policy, *supra* at 13, with Hotspot Shield Privacy Policy (last modified Dec. 13, 2011), available via Wayback Machine at https://web.archive.org/web/20150407052832/http://www.anchorfree.com:80/privacy.php.


Our Commitment to User Privacy:

Except as explained in this Notice, AnchorFree does not collect any Personal Information about you when you use the Service. "Personal Information," also referred to as personally identifiable information, is information that may be tied to a specific individual. Examples of Personal Information include name, email address, mailing address, mobile phone number, and credit card or other billing information. Please note, however, that for purposes of this Privacy Notice, AnchorFree does not include your IP address or unique device identifier within the definition of Personal Information. AnchorFree's practices regarding IP address and unique device identifiers are described separately in

Screenshot: Hotspot Shield VPN Privacy Policy

16. Hotspot Shield also monitors information about users' browsing habits while the VPN is in use. While Hotspot Shield claims that "any browsing information or other similar information relating to your online activities transmitted by you to our servers when using Hotspot Shield is ***cleared*** after your VPN 'session' is closed," [23] it also deploys persistent cookies[24] and concedes that it works with unaffiliated entities to customize advertising and marketing messages.[25] It is unclear to what extent records of browsing habits and other usage logs are attached to virtual, proxy IP addresses or other unique identifiers.

17. While insisting that it does not make money from selling customer data,[26] Hotspot Shield promises to connect advertisers to unique users that are frequent visitors of travel, retail, business, and finance websites.[27] Moreover, these entities have access to IP addresses and device identifiers collected via Hotspot Shield. Even if Hotspot Shield only provides "hashed" or "proxy" IP addresses to these partners, third parties can also link information about web-viewing habits while using the Hotspot Shield by cross-referencing cookies, identifiers, or other information.[28]

18. Carnegie Mellon University's Mobile App Compliance System was used to provide researchers with insight into Hotspot Shield's functionality, data sharing, and network connections. Researchers downloaded the Hotspot Shield binary file from the Android

[23] HSS Privacy Policy, *supra* at 13. (emphasis added)
[24] Hotspot Shield notes that the "persistent cookie remains after you close your browser and may be used by your browser on subsequent use of our Service." *Id.*
[25] *See id.*
[26] Zack Whittaker, *Hotspot Shield Co-Founder Explains Why He Doesn't Want Your Data*, ZD Net (Jan. 12, 2016), http://www.zdnet.com/article/hotspot-shield-co-founder-explains-why-he-does-not-want-your-data/.
[27] AnchorFree's Advertising Opportunities Page, https://www.anchorfree.com/advertise/ (last visited Jul. 24, 2017).
[28] Further, Hotspot Shield likely provides little protection against device or browser fingerprinting efforts. *See* Yael Grauer, *The Impossible Task of Creating a "Best VPNs" List Today*, Arstechnica (Jun. 1, 2016), https://arstechnica.com/security/2016/06/aiming-for-anonymity-ars-assesses-the-state-of-vpns-in-2016/.

Play Store, then tested the app without running it, also known as a "static" test.[29] CMU's analysis of Hotspot Shield's Android application permissions found undisclosed data sharing practices with third party advertising networks. While Hotspot Shield's Privacy Policy focuses largely on IP address protections, providing that "[y]our original IP address will not be permanently stored or provided to any third parties by your use of Hotspot Shield,"[30] it discloses other sensitive information, such as names of wireless networks (via SSID/BSSID information), and other unique identifiers such as Media Access Control addresses[31] and device IMEI numbers.

Privacy Practice	Third Parties	App Permissions
Demographic Age 3rd Party 1 Segment	com.mopub	INTERNET
Contact E Mail Address 3rd Party 4 Segments	com.mopub	GET_ACCOUNTS, INTERNET
Identifier Mobile Carrier 3rd Party 15 Segments	com.facebook, com.google, com.vungle, com.mopub, com.quantcast, com.tapit	READ_PHONE_STATE, INTERNET
Identifier SSID BSSID 3rd Party 4 Segments	com.facebook	ACCESS_WIFI_STATE, ACCESS_NETWORK_STATE, INTERNET
Identifier Cookie or similar Tech 3rd Party 1 Segment	com.facebook	INTERNET
Identifier MAC 3rd Party 2 Segments	com.adjust, com.vungle	ACCESS_WIFI_STATE, INTERNET
Identifier IMEI 3rd Party 4 Segments	android.support, com.tapit	READ_PHONE_STATE, INTERNET

Screenshot: Carnegie Mellon University Mobile App Compliance System

[29] Specifically, the Mobile App Compliance System downloaded Android Package Kit (APK) files from the Google Play Store and then conducted a static analysis of the downloaded APK. This analysis included extraction of app permissions and evaluation of first and third party use of Android APIs to assess what data types are collected by the app publisher and shared with which third parties.

[30] HSS Privacy Policy, *supra* at 13.

[31] A Media Access Control (MAC) address is a unique hardware address that is installed into a device by the manufacturer. *See* Bradley Mitchell, *Media Access Control (MAC)*, Lifewire (Sep. 13, 2016), https://www.lifewire.com/media-access-control-mac-817973. Because "your phone's MAC address remains the same regardless of the network and transmits even without actually connecting to the Internet," researchers have long warned against the possibility of consumer tracking via MAC addresses. Latanya Sweeney, *My Phone at Your Service*, Tech@FTC Blog (Feb. 12, 2014), https://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service.

19. Contrary to Hotspot Shield's claims, the VPN has been found to be actively injecting JavaScript codes using iframes for advertising and tracking purposes.[32] An iframe, or "inline frame," is an HTML tag that can be used to embed content from another site or service onto a webpage; iframes are frequently used to insert advertising, but can also be used to inject other malicious or unwanted code onto a webpage.[33]

20. Further analysis of Hotspot Shield's reverse-engineered source code revealed that the VPN uses more than five different third-party tracking libraries,[34] contradicting statements that Hotspot Shield ensures anonymous and private web browsing.

C. Hotspot Shield's Apps Redirect User Traffic to Secret VPN Servers

21. Additional research has revealed that Hotspot Shield further redirects e-commerce traffic to partnering domains. For example, when a user connects through the VPN to access specific commercial web domains, including major online retailers like <www.target.com> and <www.macys.com>, the application can intercept and redirect HTTP requests to partner websites that include online advertising companies.[35]

D. Hotspot Employs Insecure and Unreasonable Data Security Practices

22. Consumers have reported instances of credit card fraud after purchasing the "Elite" paid-version of Hotspot Shield VPN. One consumer reported "thousands of dollars" in credit card charges, as well as other suspicious online activity.[36]

23. A static code analysis of Hotspot Shield also reveals that the app does not transmit Mobile Carrier information through an HTTPS connection. This unencrypted transmission can be vulnerable to leaks or outside attacks.

---

[32] Muhammad Ikram et al., *An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps,* Proceedings of the 2016 Internet Measurement Conference (Nov. 14-16, 2016), https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf.
[33] Definition: IFrame, TechTarget, http://whatis.techtarget.com/definition/IFrame-Inline-Frame (last visited Jul. 10, 2017).
[34] Ikram et al., *supra* note 32, at 11.
[35] *Id.*
[36] *See, e.g., Lots of fraudulent activity since purchasing Hotspot Shield Elite,* Reddit (Jan. 2017), https://www.reddit.com/r/vpnreviews/comments/5f9emw/lots_of_fraudulent_activity_since_purchasing/.

Screenshot: Carnegie Mellon University Mobile App Compliance System

24. Hotspot Shield provides a blanket caveat to its claims to security and privacy. Its Privacy Policy states that "[a]s described in our Terms, [ ] we may not provide a virtual IP Address for every web site you may visit and third-party web sites may receive your original IP Address when you are visiting those web sites."[37] The referenced Terms (of Use) further emphasizes that "software is not perfect and due to defects, bugs, or other reasons, or for no reason at all, AnchorFree does not guarantee that the Service will create a VPN or utilize a Proxy IP Address on all websites."[38] This directly contradicts the stated purpose of HotspotShield and defies consumers' reasonable expectations for the functionality of the product.

III. Legal Analysis

25. Section 5 of the FTC Act prohibits unfair and deceptive acts and practices and empowers the Commission to enforce the Act's prohibitions.[39]

26. Misrepresenting the level of privacy and security available to individuals while using the Hotspot Shield VPN application is a deceptive trade practice under Section 5 of the FTC Act, subject to investigation and injunction by the Commission.

27. Hotspot Shield's lack of transparency about its logging, use of third-party tracking libraries, and redirection of user traffic also constitutes an unfair trade practice under Section 5 of the FTC Act, and is also subject to investigation and injunction by the Commission.

A. Hotspot Shield VPN's Claims About Privacy and Security Are Deceptive Trade Practices

28. A company's "representation, omission, or practice" is considered deceptive under Section 5 of the FTC Act if it is likely to mislead a consumer acting reasonably under the

[37] HSS Privacy Policy, *supra* at 13.
[38] AnchorFree, Hotspot Shield Software License & Service Terms, https://www.anchorfree.com/terms-of-service/ (last modified Jul. 22, 2016).
[39] *See* 15 U.S.C. § 45 (2010)

circumstances and is likely to affect a consumer's conduct or decision regarding a product or service.[40]

29. Hotspot Shield's statements to the media, application descriptions that users' "security and privacy are guaranteed!," and Privacy Policy, which begins with the phrase, "Protecting the web for your security, privacy and anonymity!," are misleading and would lead the average user to believe the VPN service is more secure and more privacy-protecting than the reality of Hotspot Shield's data practices.

30. These statements are also important to a consumer's decision to use Hotspot Shield VPN, constituting "material" claims.[41] [42] Hotspot Shield touts "anonymous web browsing," "complete Wi-Fi security," and the ability to "protect [sensitive data] from snoopers" as key benefits of using its VPN.[43] As mentioned above, consumer demand for privacy and security protections predominate the list of reasons why users access and use VPNs.[44] Misrepresenting the functionality of its product makes it difficult for consumers to meaningfully decide how or whether to purchase, download, or use Hotspot Shield VPN.

B. HotSpot Shield's Data Collection and Sharing Practices, and Its Failure to Provide Adequate Security, Are Unfair Trade Practices

31. The Commission may find a company's practice to be unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[45]

32. There are three elements to an unfairness claim: first, the injury suffered by consumers must be "substantial." This generally involves monetary harm. With respect to data security, the Commission has previously found that the failure to "employ reasonable and appropriate measures to protect personal information against unauthorized access" is an

---

[40] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
[41] *Id.*
[42] The Commission has explained that examples of material claims include representations about a product's performance, features, safety, price, or effectiveness. Fed. Trade Comm'n, *Advertising FAQ's: A Guide for Small Business (Apr. 2001), https://www.ftc.gov/tips-advice/business-center/guidance/advertising-faqs-guide-small-business.*
[43] Hotspot Shield, Benefits of VPN, https://www.hotspotshield.com/benefits/.
[44] *See* Paul Gil, *10 Reasons to Use a VPN for Private Web Browsing*, Lifewire (Jul. 21, 2017), https://www.lifewire.com/reasons-to-use-a-vpn-for-private-web-browsing-2483583.
[45] FTC v. Direct Marketing Concepts, Inc., 569 F. Supp. 2d 285 (D. Mass. 2008); FTC v. Seismic Entertainment Productions, Inc., Civ. No.1:04-CV-00377 (Nov. 21, 2006); *see also* FTC Policy Statement on Unfairness (1980) (codified into the FTC Act as 15 U.S.C. § 45(n)).

unfair trade practice.[46] Hotspot Shield's insecure practices present potential monetary harm for paying customers, as well as the potential risk of identity theft and fraud for all users.

33. While emotional impacts and other more subjective types of harm do not ordinarily make a practice unfair,[47] the Commission has also suggested that consumers can be unfairly harmed by the sharing of information for undisclosed purposes in ways that betray consumer trust.[48] It is thusly unfair for Hotspot Shield to present itself as a mechanism for protecting the privacy and security of consumer information, while profiting off of that information by collecting and sharing access to it with undisclosed third parties. Consumers who employ Hotspot Shield VPN do so to protect their privacy, and Hotspot Shield's use of aggressive logging practices and third-party partnerships harm its consumers' declared privacy interests.

34. Second, "the injury must be one which consumers could not reasonably have avoided." Companies may not withhold from consumers "critical price or performance data," which would leave consumers unable to make informed comparisons.

35. The Commission's use of its enforcement authorities are designed to promote the "free exercise of consumer decision making,"[49] and Hotspot Shield's practices unfairly limit consumers' ability to make meaningful free market decisions.

36. Hotspot Shield users could not have avoided the harm at issue here. While there are other VPNs on the market, consumers lack any meaningful way of making comparisons among different providers. Reading user reviews of VPN services, for example, may not provide accurate information; they are frequently manipulated by hired affiliates to VPN service. [50] As users have pointed out, "[a]lthough there are multiple 'top VPN' lists available online, they are often riddled with affiliate links, making it hard to ascertain their accuracy."[51]

---

[46] Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D.N.J. June 26, 2012).
[47] FTC Policy Statement on Unfairness (1980) (codified into the FTC Act as 15 U.S.C. § 45(n)).
[48] Statement of Chairman Pitofsky and Commissioners Anthony and Thompson, In the Matter of Touch Tone Information, Inc., File No. 982-3619 (1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-majoritystatement.htm.
[49] FTC Policy Statement on Unfairness (1980).
[50] Grauer, *supra* at 28.
[51] *See id. See also* Violet Blue, *Good Luck Finding a Safe VPN*, Engadget (Apr. 7, 2017), https://www.engadget.com/2017/04/07/good-luck-finding-a-safe-vpn/ (finding that many articles purporting to explain and review VPNs are "are profit-seeking endorsements for affiliate VPN services").

37. Third, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces." Consumers do not derive a countervailing benefit from policies and procedures that compromise the privacy and the integrity of their information, particularly for a product that presents itself as a tool to protect users' security and privacy. While an ad-supported VPN may be beneficial in certain instances, it should not be paired with a product or service that tells users that it ensures anonymity, privacy, and security.

IV. Grounds for Relief

38. CDT seeks to ensure that technologies marketed to consumers as privacy protective provide clear and accurate disclosures about data collection and third party data sharing of user information.

39. CDT urges the Commission to conduct an investigation pursuant to its regulatory authority into the data collection and sharing practices of Hotspot Shield VPN.

40. Based upon Hotspot Shield's unfair and deceptive trade practices, CDT specifically asks the Commission to: 1) Initiate an investigation into the data security practices of Hotspot Shield, as well as the application's data collection and sharing practices; 2) Order Hotspot Shield to cease misrepresenting its privacy and security practices in its advertising materials, Terms of Service, and Privacy Policy; 3) Order Hotspot Shield to provide consumers with more clear, accurate, and accessible information about Hotspot Shield's advertising practices; 4) Order Hotspot Shield to implement a comprehensive privacy and security program, including an independent third-party audit of the technical security features of its VPN applications; 5) Order Hotspot Shield to provide consumers with refunds where appropriate; and 6) Provide such other relief as the Commission finds necessary and appropriate.

Respectfully submitted,

Michelle De Mooy
Director, Privacy and Data Project
Center for Democracy & Technology

Joseph Jerome
Policy Counsel, Privacy and Data Project
Center for Democracy & Technology

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu