CENTER FOR DEMOCRACY & TECHNOLOGY

October 2018

Signals of Trustworthy VPNs – Quick Questions for VPN Services

I. Corporate Accountability & Business Model

1. What is the public facing and full legal name of the VPN service and any parent or holding companies? Do these entities have ownership or economic stakes in in other VPN services, and if so, do they share user information? Where are they incorporated? Is there any other company or partner directly involved in operating the VPN service, and if so, what is its full legal name?

2. Does the company, or other companies involved in the operation or ownership of the service, have any ownership in VPN review websites?

3. What is the service's business model (i.e., how does the VPN make money)? For example, is the sole source of the service's revenue from consumer subscriptions?

II. Privacy: Logging/Data Collection Practices and Responding to Law Enforcement

4. Does the service store any data or metadata generated during a VPN session (from connection to disconnection) after the session is terminated? If so what data? (including data from Client / VPN app, APIs, VPN gateways).

5. Does your company store (or share with others) any user browsing and/or network activity data, including DNS lookups and records of domain names and websites visited?

6. Do you have a clear process for responding to legitimate requests for data from law enforcement and courts?

III. Security Protocols and Protections

7. What do you do to protect against unauthorized access to customer data flows over the VPN?

8. What other controls does the service use to protect user data?

CENTER FOR DEMOCRACY & TECHNOLOGY

October 2018

Signals of Trustworthy VPNs Detailed Overview

Trust is a critical component to a thriving digital ecosystem. While VPN providers are often a tool for users who lack trust in the practices of other online entities, these services must still earn trust from their own users by proving that they adequately obscure individuals' digital footprints and only collect appropriate amounts of information. Specifically, user information should not be sold or shared in unexpected ways, such as web browsing habits being exploited for sale or handed over to law enforcement or other public authorities without proper legal procedures in place. VPN providers should provide users with transparency about basic security practices, company business models, economic incentives, and ownership structures.

Below is a list of questions that a trustworthy VPN service should be able to answer honestly, clearly, and thoroughly, signaling the provider's commitment to earning user trust. The goal of these questions is to improve transparency among VPN services and to provide a way for users to easily compare privacy, security, and data use practices, encouraging VPNs to deploy measures that meaningfully improve the privacy and security of individuals using their services.

Specific technical features and security choices are outside of the scope of this document. While we believe a baseline security standard and clearer privacy commitments are warranted for VPN services, these requirements require further independent auditing infrastructure and technical consensus.

Questions Trustworthy VPNs Should Be Able to Answer (and Why)

I. Corporate Accountability & Business Model

1. What is the public facing and full legal name of the VPN service and any parent or holding companies? Do these entities have ownership or economic stakes in in other VPN services, and if so, do they share user information? Where are they incorporated? Is there any other company or partner directly involved in operating the VPN service, and if so, what is its full legal name?

- VPN ownership can be opaque.[1] A VPN service's public brand name and legal name may be different and a user should know both, as well as any other entities that control or functionally operate the VPN's services and whether they also access any customer data.[2]

2. Does the company, or other companies involved in the operation or ownership of the service, have any ownership in VPN review websites?
    - There is a potential conflict of interest in a company operating both the service and a website reviewing the service. VPN review websites have proven especially susceptible to abuse.[3] Users need to be aware of these relationships so they can determine the trustworthiness of product reviews on websites owned by the same company.
3. What is the service's business model (i.e., how does the VPN make money)? For example, is the sole source of the service's revenue from consumer subscriptions?
    - Individuals should be given detailed information from a VPN provider about how their information is processed. VPN users should expect that their personal data is not being collected, stored, or sold without their consent. VPN providers can monetize user information in ways users may find unexpected.[4] It costs significant resources to deliver a VPN service and understanding the business model and data use practices will enable consumers to make an informed judgement according to their threat model.

II. Privacy: Logging/Data Collection Practices and Responding to Law Enforcement

---

[1] Alex Konrad, *Ex-SoftLayer Chief Lance Crosby's New Startup Acquired Its Way To $200M In Revenue In 2 Years*, Forbes (Jan. 31, 2018), https://www.forbes.com/sites/alexkonrad/2018/01/31/ex-softlayer-chief-lance-crosbys-new-startup-acquired-its-way-to-200m-in-revenue-in-2-years/#6448c15b2967.

[2] CNBC, *Facebook promotes a VPN app without disclosing ownership* (Feb. 13, 2018), https://www.cnbc.com/video/2018/02/13/facebook-promotes-a-vpn-app-without-disclosing-ownership.html; *see also* Seth Rosenblatt, *Verizon's VPN: security boon or privacy boondoggle?*, The Parallax (Aug. 2, 2018), https://www.the-parallax.com/2018/08/02/verizon-vpn-security-boon-privacy-boondoggle/.

[3] Sven Taylor, *7 VPN Scams You Need to Avoid, Restore Privacy*, Restore Privacy (June 29, 2017), https://restoreprivacy.com/vpn-scams/; *see also* Beware of False Reviews - VPN Marketing and Affiliate Programs, https://www.reddit.com/r/VPN/wiki/beware_of_false_reviews (last visited Jul. 18, 2018).

[4] Nicolas Deleon, *Phony VPN Services Are Cashing in on America's War on Privacy*, Motherboard (Apr. 4, 2017), https://motherboard.vice.com/en_us/article/xy99ww/phony-vpn-services-are-cashing-in-on-americas-war-on-privacy; Alan Henry, *Hola Better Internet Sells Your Bandwidth, Turning Its VPN into a Botnet*, Lifehacker (May 28, 2015), https://lifehacker.com/hola-better-internet-sells-your-bandwidth-turning-its-1707496872.

4. Does the service store any data or metadata generated during a VPN session (from connection to disconnection) after the session is terminated? If so what data? (including data from Client / VPN app, APIs, VPN gateways).
    - The data logging practices of VPN providers have proven controversial and confusing.[5] Many providers claim to log either a minimal amount of data or no data with respect to the connection logs, which includes logs generated by a VPN server that show session-related events including IP addresses, connection and disconnection timestamps, and the amount of data transferred. However, there are potentially many other points at which user data can collected and stored. Individuals should expect their VPN provider to only store connection logs for purposes relating to the provision of the VPN connection and that any information may be deleted after the connection is terminated. Data retained after the connection may represent a privacy risk to users depending on their requirements.
5. Does your company store (or share with others) any user browsing and/or network activity data, including DNS lookups and records of domain names and websites visited?
    - Activity logs effectively provide a full record of a user's online browsing activities and are potentially far more sensitive than connection logs. Unfortunately, many providers do not explicitly state whether their logging policies or practices apply to connection logs or activity logs. It is possible that a provider is rightly claiming not to log or log a minimal amount of connection logs but still be collecting and storing activity logs. Individuals must be able to easily understand the logging policy for both connection and activity logs in order to evaluate a VPN service.
6. Do you have a clear process for responding to legitimate requests for data from law enforcement and courts?
    - Individuals should expect trustworthy VPN providers to have procedures and processes in place to respond to legal requests from authorities for information they maintain. These procedures should be made available publicly to users and law enforcement, and VPN providers can also

[5] *Compare* Mark Wycislik-Wilson, *FBI uses PureVPN's 'non-existent' logs to track down internet stalker,* Betanews (Oct. 9, 2017), https://betanews.com/2017/10/09/purevpn-logs-fbi/, *with* PureVPN, *Setting the Record Straight: Addressing VPN Privacy and VPN Logs* (Oct. 14, 2017), https://www.purevpn.com/blog/vpn-logs-explained/.

consider transparency reports as a reporting tool.[6] VPN providers should also explain what measures they have in place to protect data in the event of law enforcement gaining physical access to servers.

III. Security Protocols and Protections

7. What do you do to protect against unauthorized access to customer data flows over the VPN?
    - While perfect privacy and security does not exist, VPN users should have the reasonable expectation that trustworthy VPN providers will work to protect customer information through up-to-date protocols and software/hardware hardening. Trustworthy VPN providers will provide information about the technical and administrative procedures they put in place to protect their customers and their businesses.
8. What other controls does the service use to protect user data?
    - VPNs should be encouraged to provide the best privacy and security protections on the market. Additional signals of trust might include independent **security audits**, acceptance of **anonymous payments**, incorporation of **open source code**, **a vulnerability disclosure policy**, and implementation of **bug bounty programs**.

[6] Cyrus Farivar, *Shadowy VPN firm says it has industry's first transparency report*, ArsTechnica (Nov. 5, 2013), https://arstechnica.com/information-technology/2013/11/shadowy-vpn-firm-says-theyve-got-industrys-first-transparency-report/.