Security and Privacy of VPNs Running on Windows 10

WRITTEN BY YAEL GRAUER
TEST TEAM LED BY STEVE BLAIR

Consumer Reports | Digital Lab

Table of Contents

Introduction

Consumers looking for tools for strong data protection and privacy often turn to commercial VPNs, or virtual private networks. VPNs route internet traffic—including users' browsing history and other sensitive information—through their own servers or those they contract, so the privacy and security of these services is important.

Many people turn to VPNs in large part to either avoid risks on untrusted networks or to protect themselves from advertisers and internet service providers (ISPs) that might monitor, disrupt, or even tamper with internet traffic. Unfortunately, some people might not realize that apps and websites may be identifying them even when they're masking their IP addresses. One way to do this, known as digital fingerprinting, involves apps and websites looking at and triangulating characteristics of a computer or mobile device, such as operating systems and models, screen resolutions, and so forth, to uniquely identify individual users. It's also not possible for consumers to know with certainty that any VPN is *not* sharing or even monetizing user data, failing to secure it properly, or sharing it with third parties that may, themselves, be malicious.

However, it *is* possible to conduct a rigorous, objective evaluation of VPNs—to test for different aspects of the service that *are* testable, such as security misconfigurations and leaks and whether strong controls are implemented by default, and to analyze their privacy policies. It's also possible to look for language that might mislead users about the level of protection they can expect from a VPN, and to generally shine a light on both good and harmful practices in the industry. This is what we set out to do.

Selection Process

To begin, we started with a comprehensive list of over 200 VPNs. We narrowed down to a list of 51, choosing VPNs with larger market share and others that had markers of quality, such as public ownership, open source code, public third-party security audits, support for modern protocols, and accurate ad copy. (Indicators of poor quality that disqualified VPNs without significant market share from testing included limited information on their websites, support for the deprecated point-to-point tunneling protocol (PPTP), and hyperbolic ad copy promising "100% security" or "military-grade encryption.") However, it made sense to include popular, well-known VPNs for evaluation even if they didn't meet these standards, as a service for consumers who are already users, often because they've seen these VPNs promoted through marketing or included in lists of top VPN options. We also chose to start with VPNs that were available for Windows, the environment where we ultimately ran all four tests.

We partnered with Digital Lab fellow professor Roya Ensafi and her team from the University of Michigan, using the VPNalyzer test suite they developed. The VPNalyzer tool, a cross-platform desktop tool developed to test the security and privacy features of VPN connections, is just one part of an interdisciplinary research project that aims to analyze the VPN ecosystem through crowdsourced empirical data, large-scale quantitative user studies, and qualitative studies

surveying VPN providers, with the stated goal of advancing the public interest, informing practical regulations and standards, enforcing accountability, and empowering consumers to find more trustworthy VPN products.

For our screening, we looked at a subsection of results from a larger series of tests. Specifically, we were interested in evidence of VPNs manipulating users' network traffic, any DNS leaks, whether kill switches were implemented ineffectively, and good behavior—particularly, VPNs that implemented a DNS proxy to prevent DNS leaks.

Using results from the VPNalyzer tool, we found little evidence of the VPNs we screened manipulating users' networking traffic when testing for evidence of TLS interception. Only one—Turbo VPN—returned abnormal TLS responses for our custom queries, and the VPNalyzer team has reached out to the company for an explanation.

We tested VPNs' kill switches, which—when working correctly—protect a user's traffic by automatically disconnecting the user's device if the VPN connection fails. When testing whether the VPN provider's kill switch was implemented effectively, we found that Le VPN and Speedify both leaked user traffic upon tunnel failure.

There were additional data leaks. If our VPN was turned on properly, which we believe it was, both Hola Free VPN and Psiphon did not tunnel all traffic from the machine by default and leaked any non-browser traffic. And during tunnel failure, HideMyAss and Trust.Zone leaked DNS traffic, which should have been protected using the VPN kill switch feature.

Many VPNs have configured their applications to use public DNS services instead of their own DNS resolvers. Astrill VPN, Speedify, Touch VPN, and Windscribe used Cloudflare, a third-party public DNS service. Encrypt.me, Kaspersky, Steganos, Trust.Zone, and Turbo VPN used Google public DNS service. Le VPN and ZoogVPN used the OpenDNS public DNS service, and Le VPN additionally used Google public DNS.

Other VPNs configured their applications to use DNS resolvers hosted in a third-party provider that may or may not be associated with the particular VPN. Anonine (Portlane), AzireVPN (Foilhat), VPN.AC (Leaseweb), VyprVPN (DigitalOcean and Amazon AWS), and ZenMate (M247) all appeared to route the user's DNS queries to a resolver in the mentioned third-party provider, which was in a different network than that of the VPN server to which the user was connected.

However, in the case of Encrypt.me, the DNS queries were additionally being exposed to the user's ISP, which compromised the privacy of the user's browsing activity to their ISP while the user was on the VPN.

We found that some VPNs have configured their network to disable DNS-over-HTTPS (DoH) for Firefox users via the Mozilla Canary Domain, and because this is a deliberate signal to disable DoH for Firefox, doing so without reason is considered poor practice. This was the case for

AirVPN, Cryptostorm, Hide.me, IPVanish, Le VPN, StrongVPN, Unspyable, Windscribe, and ZoogVPN.

We found one instance of DNS manipulation in Betternet, where it returned RFC 6598 carrier-grade NAT addresses for all DNS queries. Though this could be a design choice for optimization, we still labeled it as an unexpected behavior, observed only in Betternet. We also discovered unexpected good behavior by F-Secure Freedome VPN, Hotspot Shield, Private Tunnel, and TunnelBear, which implemented DNS proxy to prevent DNS leaks.

From the findings of the 51 VPNs we ran through VPNalyzer, coupled with an analysis of market share, we chose 16 VPNs for further analysis. Those were Betternet, CyberGhost, ExpressVPN, F-Secure Freedome VPN, Hotspot Shield, IPVanish, IVPN, Kaspersky, Mozilla VPN, Mullvad, NordVPN, Private Internet Access (PIA), Private Tunnel, ProtonVPN, Surfshark, and TunnelBear.

VPN	Location	Owner
Betternet	U.S.	Aura
CyberGhost	Romania	Kape Technologies
ExpressVPN	British Virgin Islands	Kape Technologies
F-Secure Freedome VPN	Finland	F-Secure
Hotspot Shield	U.S.	Aura
IPVanish	U.S.	Ziff Davis
IVPN	Gibraltar	Privatus Limited
Kaspersky VPN	Russia & Switzerland	Kaspersky
Mozilla VPN	U.S.	Mozilla
Mullvad	Sweden	Amagicom AB
NordVPN	Panama	Tefincom S.A.
Private Internet Access (PIA)	U.S.	Kape Technologies
Private Tunnel	U.S.	OpenVPN
ProtonVPN	Switzerland	Proton Technologies AG
Surfshark	British Virgin Islands	Surfshark Ltd.
TunnelBear	Canada	McAfee

We then conducted a comparative privacy and security evaluation guided by the Digital Standard.

Limitations: We did not investigate VPN companies' hosting providers or other third-party partners. We were also unable to determine whether these VPNs have unsafe functions or libraries, or whether the service has settings that can be modified, logged, or manipulated on the server side. We focused specifically on privacy and security, and did not test for

performance. We did not test for torrenting speed or for geoshifting (to watch movies in other countries, for example) or look at monthly fees or the number of devices one can use with each service. We are aware that there are limitations to the information we can find, as there are for any VPN consumer. The fact that we didn't find evidence for providers keeping logs, transmitting data to advertisers, governments, or other third parties, or manipulation of internet traffic, etc., doesn't mean it isn't possible.

VPN Version Info:

Betternet	6.13.1
CyberGhost	8.2.5.7817
ExpressVPN	10.3.0.23
F-Secure Freedome VPN	2.42.736.0
Hotspot Shield	10.14.3-plain-773-plain
IPVanish	3.6.5.0
IVPN	3.3.10
Kaspersky VPN	ksec21.36.0.391en_25096
Mozilla VPN	2.3.0 (2.202105270956)
Mullvad	2021.3
NordVPN	6.37.5.0
Private Internet Access (PIA)	2.9.0+06393
Private Tunnel	3.01(664)
ProtonVPN	1.20.4.0
Surfshark	2.8.4
TunnelBear	4.4.5

Tools	Function
Virtual Box	container
Windows 10 image	test OS
Wireshark	USB/NW communication gathering
Sysinternals Procmon	local/system files/PID
Strings	binary ASCII/unicode check
NetMiner	PCAP (NW) analysis
AstroGrep	PCAP/file keyword analysis
https://www.dnsleaktest.com	DNS leak check
https://ipv6leak.com	IPv6 leak check
https://browserleaks.com/webrtc	RTC IPv4 leak check
https://gf.dev/hsts-test	TLS/downgrade attack check
custom page w/no end tags	ad injection check

NMAP	port scan/service check
VPNalyzer (https://vpnalyzer.org)	VPN test software

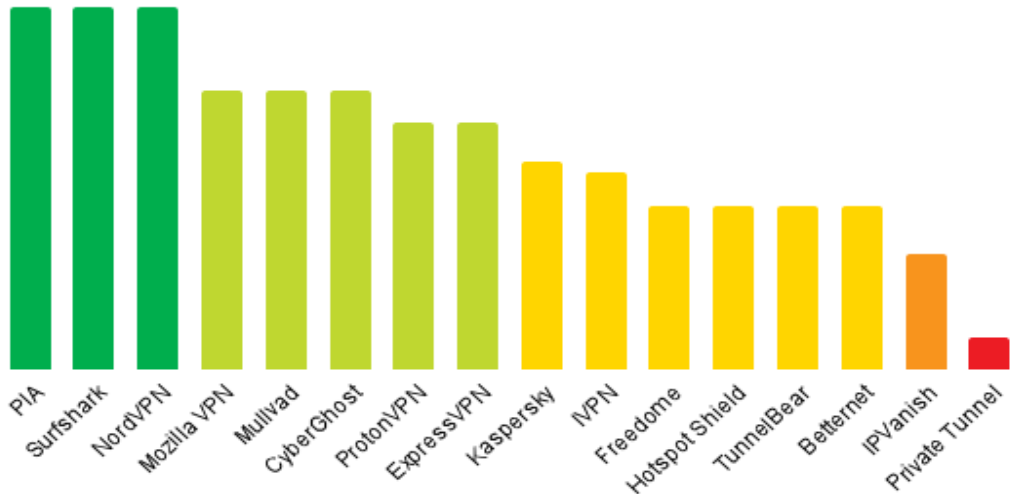
Security Evaluation

Data Security

We broke down our tests into two overarching categories: data security and data privacy.

Data security is a measure of how well the VPN and its service provider protect a user's data with respect to authentication, encryption, software updates, resistance to known exploits, etc. We based our score on inspection of VPN features, analysis of network traffic, and publicly available documentation.

Build Quality: Best Build Practices



We tested for best build practices in a variety of categories.

Effectively Implemented Safety Features

Using the VPNalyzer tool, we looked for VPNs whose DNS resolvers support QNAME minimization (a feature that improves DNS privacy) and found that nine VPNs did not have them. Separately, we looked for secure configuration and protocols, and proven implementations of cryptographic primitives. For each protocol, we looked at the variant used,

giving a lower score to VPNs with poor IPsec or OpenVPN configurations, preshared keys, or PPTP. VPNs could get partial credit for good or no IPsec and OpenVPN configurations and no preshared keys, even if WireGuard support wasn't offered. We also gave partial credit for use of other modern, open source protocols that have not been formally verified.

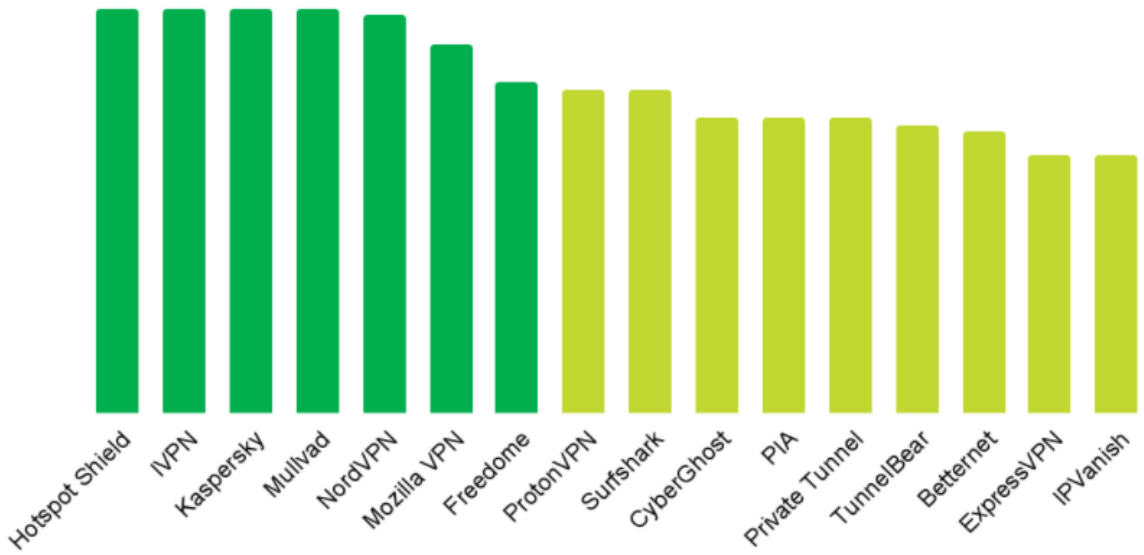
CyberGhost, Mozilla VPN, Mullvad, NordVPN, PIA, and Surfshark scored highest for protocols, and IPVanish, Kaspersky, and Private Tunnel scored lowest. IPVanish was using the deprecated point-to-point tunneling protocol (PPTP). (We previously stated that Kaspersky used PPTP as well based on third party data, but after publication, a Kaspersky spokesperson said it never used the protocol.) Only CyberGhost, IVPN, and Private Tunnel were lacking kill switch support. (IVPN offers a kill switch in the form of an always-on firewall option.)

Open and Reproducible Software

We looked for open source software with reproducible builds, which allows researchers to confirm that the code used in the distributed product is identical to the source code, and allows us to verify whether the software is what it claims to be.

IVPN, Mozilla VPN, Mullvad, PIA, and ProtonVPN were the only VPNs we analyzed that are open source. We found matching hashes when comparing the packets and source code for all five.

Authentication



For VPNs that have account information including email addresses or other personal data, we checked to see whether multifactor authentication (MFA) was available. (Mullvad doesn't have MFA or even passwords, but the user ID is not linked with any user information, which is

arguably better than collecting a lot of private data and securing it with MFA, so we did not dock points for that.)

We looked for default passwords, multiple points of authentication, requirements for strong passwords, input sanitation, and the ability to detect and throttle brute force or denial of service (DOS) attacks.

We found that all VPNs either sanitized their input and allowed the use of password managers, or didn't require passwords.

Betternet, CyberGhost, ExpressVPN, IPVanish, Private Tunnel, Surfshark, and TunnelBear do not offer MFA, even when personal information is associated with the account.

For VPNs that require users to set a password, we looked at both password length and password complexity.

For password length, we looked for a requirement of eight characters. This is one area where ProtonVPN fell short, by allowing a seven-character password.

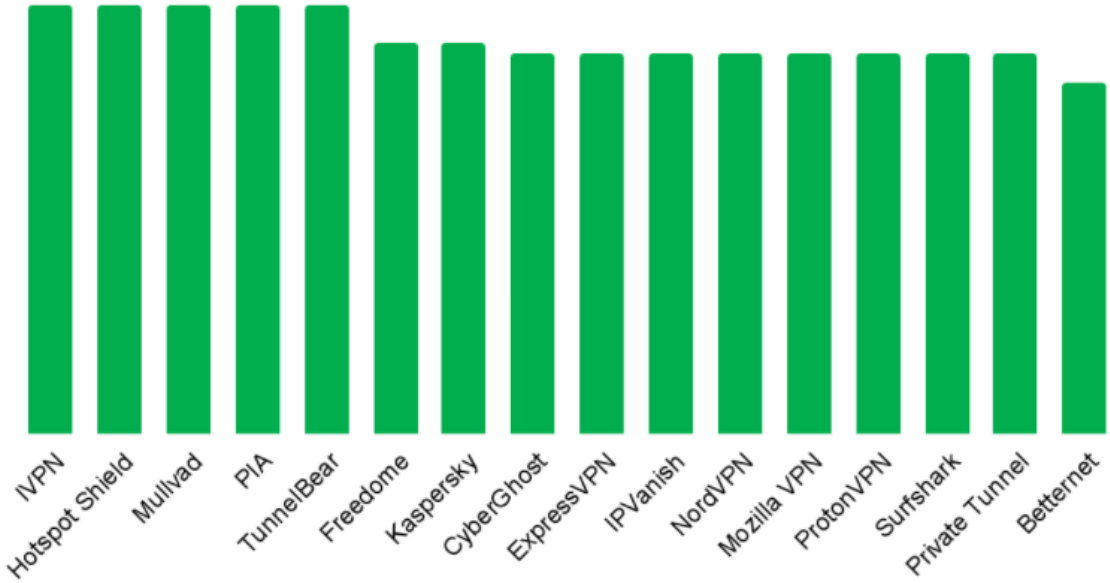
Neither IPVanish nor ProtonVPN met our password complexity requirements because they allowed us to set simple, easy-to-guess (or crack) passwords, such as "aaaaaaaa," "12345678," and "qwertyuiop."

However, the user can decide to make their password more complex than the minimum requirement, and every VPN that required passwords allowed ones that were 21 characters long.

ExpressVPN, F-Secure Freedome VPN, IPVanish, PIA, and Private Tunnel users were not sent a password change notification via email. This could potentially lead to a situation where a user's account could be hijacked without their knowledge.

CyberGhost, ExpressVPN, Mozilla VPN, PIA, Surfshark, and TunnelBear did not meet our brute force mitigation checks. CyberGhost, ExpressVPN, and PIA allowed 30 attempts without triggering a defense. Mozilla VPN, Surfshark, and TunnelBear were found to lock out accounts for periods of time after a number of failed login attempts. This could be abused by malicious actors to deny access to legitimate accounts by simply entering incorrect passwords against the targeted account.

Encryption

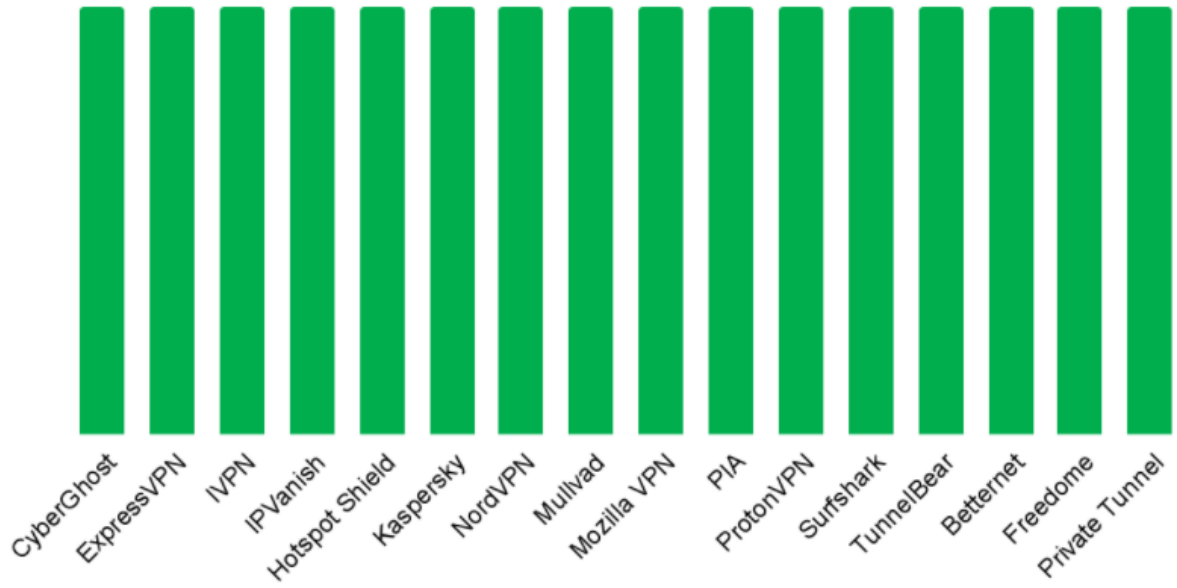


For our encryption testing, we looked for DNS leaks, IPv6 leaks, WebRTC leaks, and whether a TLS version above 1.3 was used. We wanted to see whether VPNs used encrypted communication, without modifying traffic or injecting ads or content, or intercepting TLS connections, or injecting scripts into HTTPS requests. We also checked to see whether there were indications that sensitive data was stored outside of the app container or system cred storage facilities. If sensitive data was stored locally, we looked to see whether it was encrypted with a key from hardware-backed storage requiring authentication. And we ran a scan to see whether endpoints exposed unnecessary open services.

None of the VPNs tested were found to be susceptible to TLS downgrade attacks—HSTS headers were found in all cases.

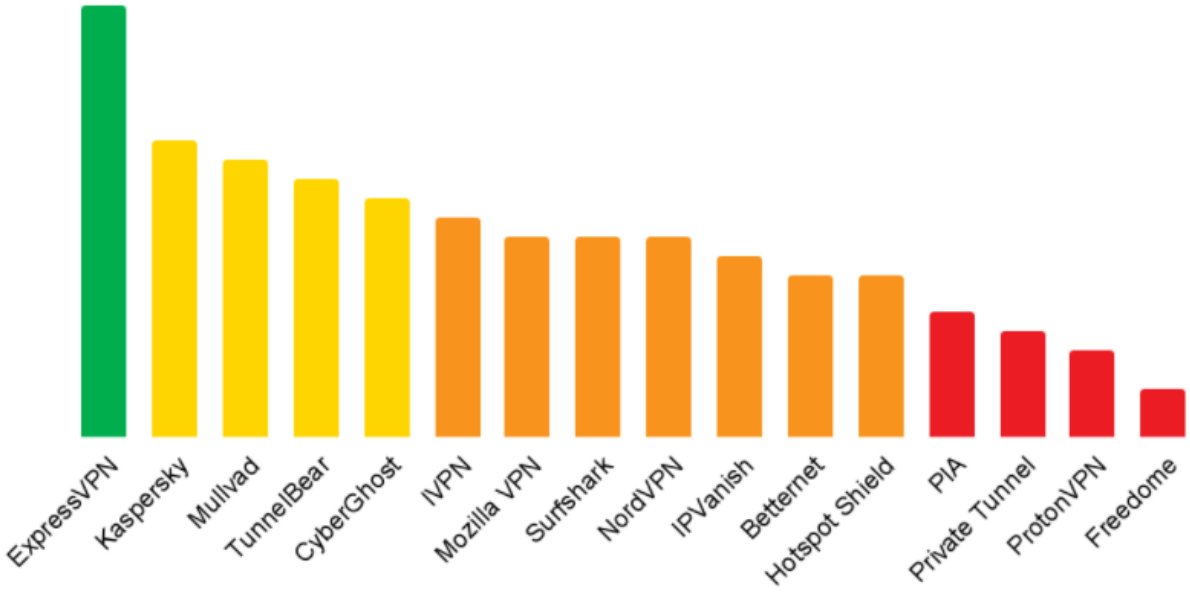
However, there were some areas of concern. Kaspersky failed a DNS leak test, and F-Secure Freedome VPN failed a WebRTC leak test. Betternet was the only VPN that appeared to have an IPv6 leak when using Edge as a browser as found by https://ipv6leak.com (which is run by Private Internet Access, a VPN provider).

Known Exploit Resistance



We looked for open CVEs against the VPN to see whether it was likely to introduce vulnerabilities to the user's device. We found no disclosed vulnerabilities in the VPN versions we tested.

Security Oversight



For our security oversight evaluation, we looked for third-party security audits of the core product that were done consistently and where the results were publicly available. To earn full points in the evaluation, VPN providers needed to have multiple publicly available audits on a regular cadence, without any misses. We did not give credit to companies that didn't have any publicly available security audits, or whose most recent audit was older than 24 months. But companies did receive partial credit for a single, more recent audit, for multiple but inconsistent audits, or for an audit that required additional steps to view (such as requiring emails or allowing only customers to view them). Though we didn't assign points for audit quality, we'd like to see clearbox audits where auditors have access to the server.

IVPN and TunnelBear were the two VPNs to have multiple publicly available audits each year without any misses, and both—along with Mullvad—disclosed information on these external audits in their documentation. ExpressVPN missed its audit in 2020 and hasn't had one yet in 2021, and one audit required additional steps/membership to view. While NordVPN had multiple audits, a user needs to log in to see the report. ProtonVPN had a series of audits done in 2019 but did not appear to have one for 2020. Surfshark had audits in 2018 and 2021. Mullvad missed a year, and Mozilla VPN is a new product, so we were unable to determine whether it will conduct audits regularly. Betternet, CyberGhost, F-Secure Freedome VPN, Hotspot Shield, IPVanish, Kaspersky, PIA, and Private Tunnel didn't have any audits from the past 24 months that we could find.

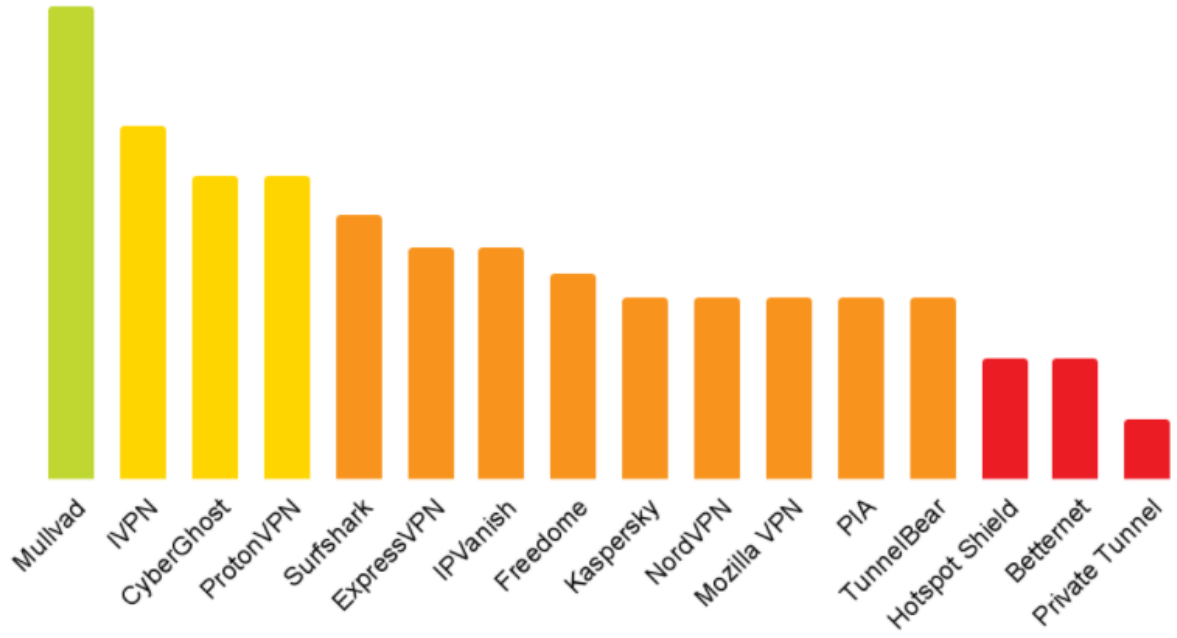
We also conducted a document review to see whether companies with access to user information described systems in place to limit and monitor employee access to that data. F-Secure Freedome VPN, IVPN, Private Tunnel, ProtonVPN, Surfshark, and TunnelBear either provided only vague or indirect mention of these systems, or failed to provide any information on them at all. IPVanish, Kaspersky, and PIA ranked highest in our evaluation by stating that only specific and necessary employees are able to access user information in order to reasonably provide necessary services, with a direct statement about systems in place to directly monitor and limit employee access to personal user information. And Mullvad doesn't collect such information at all.

Next we looked for companies that described, in their terms of service (ToS) or privacy policy, an internal security team to conduct security audits on the company's products and services. ExpressVPN was the only VPN provider that disclosed how it performs these internal security audits and what aspects of security are audited, and that publishes summaries of these reports for users. CyberGhost, Kaspersky, and Surfshark mentioned internal audits without providing much detail. None of the other VPNs mentioned such audits in their ToS or privacy policy.

We looked to see whether protections against unauthorized access were described clearly. ExpressVPN and Mullvad exceeded industry standards in these protections. ExpressVPN surveyed its server infrastructure and open sourced its Lightway protocol, which was also publicly audited. Mullvad's approach to preventing unauthorized access to data is a novel one—the company doesn't keep any unnecessary data at all. CyberGhost, F-Secure Freedome VPN, IVPN, PIA, and ProtonVPN had unclear, imprecise, vague, or missing descriptions of

protections against unauthorized access, or ones that fell below the industry standard. TunnelBear's information was incomplete and was closer but not up to the industry standard.

Security Over Time

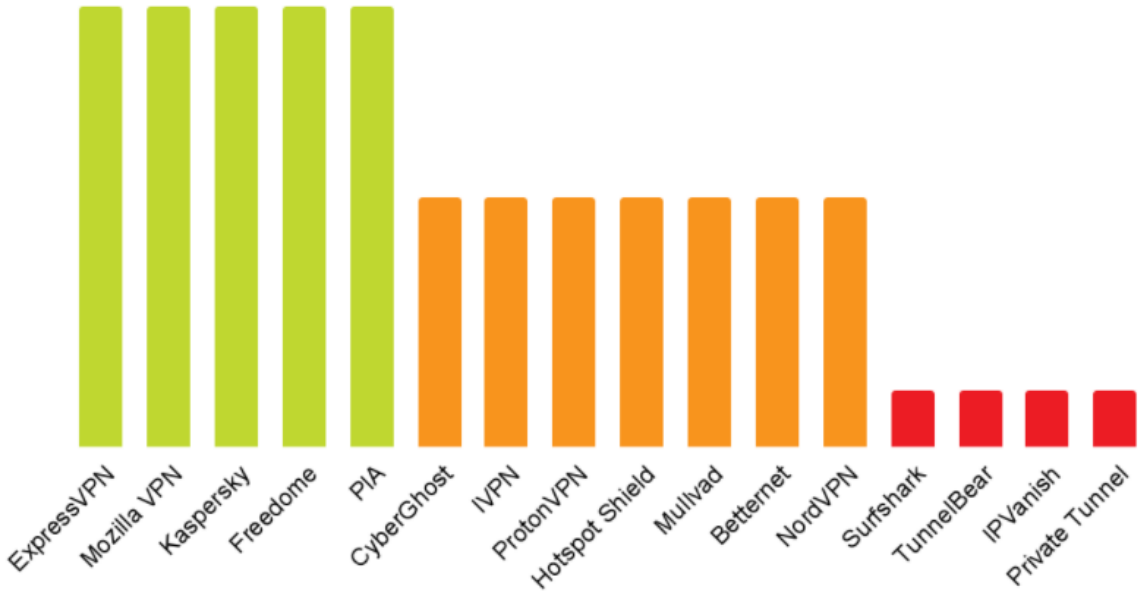


Here we looked for signed (authenticated) updates, the ability to get automatic updates, notifications for updates (if not automatic), and a low number of steps (menus or screens) to update the software. Mullvad had both authenticated and automatic updates. IVPN had automatic updates as well. CyberGhost, IVPN, Mullvad, PIA, and ProtonVPN took the fewest number of steps to update. Ten VPNs did not offer automatic updates at all. CyberGhost, ExpressVPN, F-Secure Freedome VPN, IPVanish, Mozilla VPN, NordVPN, and PIA didn't appear to provide automatic updates on Windows or notifications when an update was available, though it's possible that no updates were made available during the time of the test.

We conducted a document review to see which VPN providers claim a period of product support. NordVPN was the only VPN with a hard deadline of product support or product life, with a support period that was defined both clearly and intentionally. CyberGhost and Kaspersky also claimed they would provide support or firmware updates, but there was no time period defined, though Kaspersky stated it would notify users in case of an update.

We also looked at documents to see whether VPN providers claimed that software can be kept up to date for security issues. CyberGhost, ExpressVPN, and IPVanish did, with some level of detail about how and when this occurs. F-Secure Freedome VPN and Mozilla VPN made some references to updates for security reasons or vulnerabilities, and IVPN stated that it may update devices for patches or bug fixes. The other VPN providers didn't mention software updates for security issues at all.

Vulnerability Disclosure Program



We gave credit to companies that have some kind of coordinated vulnerability disclosure program or bug bounty to accept vulnerability disclosures for researchers. We also looked for a time frame of review of these reports, and whether the companies committed to not pursue legal action against security researchers.

The majority of the 16 VPNs tested—Betternet, CyberGhost, ExpressVPN, F-Secure Freedome VPN, Hotspot Shield, IVPN, Kaspersky, Mozilla VPN, Mullvad, NordVPN, PIA, and ProtonVPN—do have an official vulnerability disclosure program for security researchers to report their findings, or described an unofficial way to report findings, such as a dedicated security email address. Only F-Secure Freedome VPN's bug bounty, through parent company F-Secure, specifies a time frame in which it commits to review the reports.

ExpressVPN, Kaspersky, and Mozilla were the only companies that explicitly stated in their ToS or privacy policy that they will not pursue legal action against security researchers, though PIA has a partial safe harbor on its website, stating: "In addition, if you provide us time to respond to your discovery and do not damage our systems, we will not pursue any criminal charges."

Although vulnerabilities may not be what's being tested at all, we noticed that Betternet's website asks beta testers to sign a nondisclosure agreement.

Recommendations for Industry Improvement in Security

Many of the VPNs we tested had shortcomings in build quality and reliability, security oversight, security over time, and the ways VPNs engage with security researchers and respond to vulnerability reports.

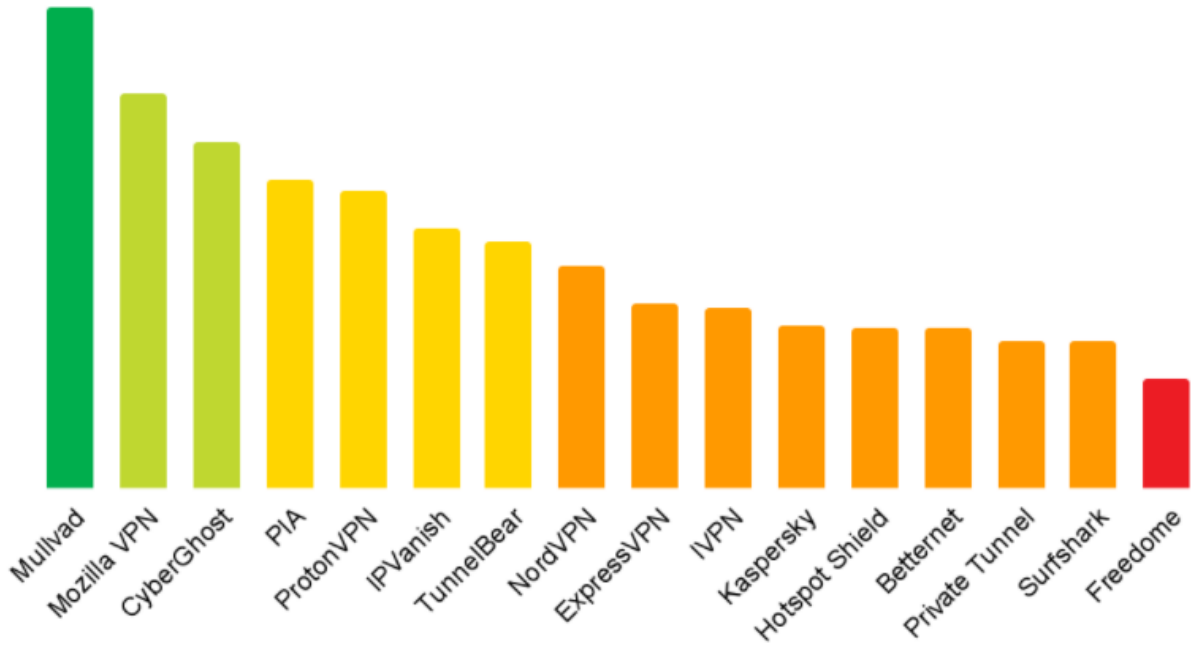
We identified some specific areas that could use improvement industry-wide.

- We looked for WireGuard support and for IPsec/OpenVPN configurations with good primitives (P-256 with AES-256 GCM), if offered. Some VPNs are still **using poor IPsec or OpenVPN configurations,** while another is using **PPTP.**
- Only six of the 16 VPNs had **open source software** and **reproducible builds.**
- Three VPNs left users **vulnerable to brute force attacks, and three left them vulnerable to account lockouts.**
- In many VPNs' terms of service or privacy policy, there was **no evidence of robust internal procedures for audits or for preventing unauthorized access by employees.** And some VPNs that had **third-party security audits** did not make them available to the general public or conducted them inconsistently.
- Given that software updates often have bug fixes and that VPNs are a security product, we'd like to see **signed updates** that are **easy to install,** if not automatic. And we'd like official documentation that VPNs will be **kept up to date for security issues,** with a **clear period of support.**
- Though the majority of VPNs had a vulnerability disclosure program for researchers to report security issues, only one (F-Secure Freedome VPN) had a **time frame to review vulnerability reports,** and only three stated without stipulation that they will not **pursue legal action against security researchers.**

Data Privacy Evaluation

In addition to our data security evaluation, we also looked at VPNs' data privacy. Data privacy is a measure of how the VPN and its service provider collect, share, and use a consumer's personal data, and the user's ability to control the flow of their data. This analysis is based in large part on our evaluation of user interfaces and publicly available materials.

Access and Control: Data Control



To analyze data control, we scoured through privacy policies to determine the level of control consumers can have of the collection or processing of their information by the product manager, or otherwise. We looked at whether consumers could turn off targeted ads, and for an explanation of how they can control the information used for targeted ads. And we looked for privacy policies that claimed consumers could request or obtain a copy of their information, as well as descriptions of information they could obtain and whether it was available in a structured data format. We also looked to see whether the company claimed that consumers could obtain all public and private user information the company holds about them.

We found that every company we analyzed could do better when it comes to allowing consumers to obtain all public-facing and private user information the company holds about them.

IPVanish, Mullvad, PIA, and ProtonVPN had easily accessible and useful data privacy controls. F-Secure Freedome VPN offered no such controls, and TunnelBear had unclear information on controls in its documentation.

We looked for privacy policies that stated that consumers can turn off targeted advertising or otherwise control it. None of the VPNs we tested use targeted ads at all, though Betternet does have a version that shows ads.

Mozilla had similar controls and allows users to opt out of tracking, such as cookies, campaign and referral data, and so forth, but the company indicated in its terms that these were enabled by default, and investigation showed that it's likely to refer to the browser rather than the VPN. However, the VPN's privacy and security settings had "data collection and use" and "allow Mozilla VPN to send technical data to Mozilla" enabled by default, without providing information on what the technical data consists of.

F-Secure Freedome VPN and Private Tunnel did the worst, with only vague or indirect statements that users can opt out of cookies in general, with no direct mention of targeted ads. The company assumes the user is knowledgeable about how and where to control cookies within their browsers.

We looked to see whether the privacy policy claimed that users can request a copy of their information or obtain it through a known service, and this is an area that needs improvement by several VPNs in our test, the majority of which (Betternet, ExpressVPN, F-Secure Freedome VPN, Hotspot Shield, IVPN, Kaspersky, Private Tunnel, and Surfshark) allowed users to obtain a copy of their information only under GDPR or CCPA, or were limited regionally, or required a fee. Mozilla VPN, Mullvad, PIA, and ProtonVPN scored top marks for providing the consumer with easily accessible functions or services to obtain comprehensive user information. CyberGhost, IPVanish, NordVPN, and TunnelBear stated that users could obtain a copy of their information via email, by contacting the company, or by other means.

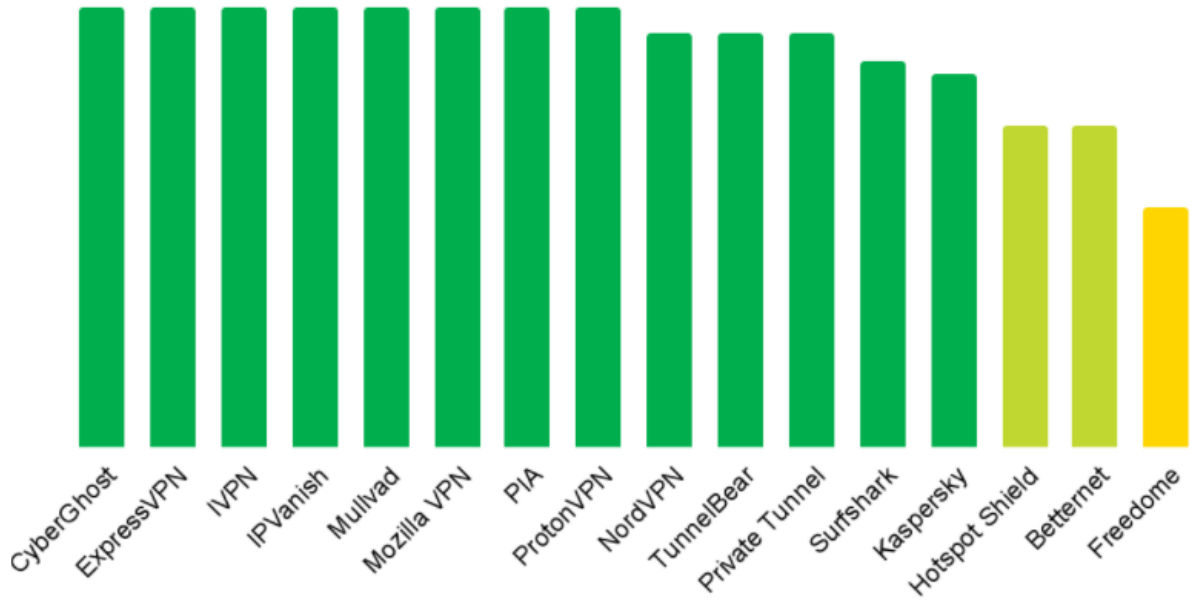
Next we looked to see whether the privacy policy or data portability service had a disclosure of what data consumers could obtain. CyberGhost, Mozilla VPN, Mullvad, PIA, ProtonVPN, and TunnelBear did best, with a data portability service, clearly stating that users are able to obtain all of their personal information, and a clear definition of what constitutes "personal information." The other VPNs did not specifically address a data portability service in their documentation.

Users seeking to access their personal data might want to obtain this information in a structured data format, and unless they are PIA users, they might be out of luck. Of the companies that provide data to all users without regional restrictions, PIA was the only one that stated users could obtain it in a structured or machine-readable format.

Consumers might also want to make sure they can obtain *all* public and private user data the company holds about them. CyberGhost and Mullvad not only allow them to do so but also list the individual pieces of information encompassed by this. IPVanish, Mozilla VPN, and TunnelBear also stated in their documentation that they allow users to access this data, but without clear and detailed descriptions of what's included.

Only IVPN, Mozilla VPN, and Mullvad got full credit for claiming in their documentation that they do not gather information from third parties.

Data Use and Sharing: Data Sharing



In this section, we wanted to know whether the company claims to share information with third parties only if it's reasonably necessary to deliver the service, and whether the company discloses what information it shares, what types of third parties it shares it with, ideally by name, and whether it shares user information with government or legal authorities. We also looked at whether third-party domains contacted by the product or service are named in the privacy policy.

We checked whether VPN companies claim to share information with third parties only as is reasonably necessary to deliver the service to consumers. Eleven VPNs met our standard by claiming not to sell, rent, or share personal data, and providing a statement that they'll only share personal data necessary to provide the services explained in the privacy policy. Some claimed to do so for any data, not just personal data. But some VPNs fell short. F-Secure Freedome VPN's documentation included a statement alluding to only sharing what is necessary, but it was website specific. Betternet's and Hotspot Shield's documentation mentioned that they may share information outside of their privacy policy with consent. Kaspersky and NordVPN stated that third parties are contractually obligated to use shared personal information only to support the requirements of their service or device.

Ten VPNs either claimed to not share data with third parties other than previously identified necessary services or clearly disclosed the information they share and with whom, with a definition of what it considers personal information and a precise definition of what is included, as well as details on whom it is shared with and why. F-Secure Freedome VPN did the worst here; it did not provide sufficient reference to what is shared with whom. Surfshark also did poorly, because it defined what information is shared but did not delineate and define what is

considered personal information. Betternet, Hotspot Shield, NordVPN, and Private Tunnel did define what they consider personal information and what is shared but were vague about with whom the information is shared.

All but three VPNs clearly disclosed the types of third parties they share user information with. F-Secure Freedome VPN did the worst; it made it reasonably apparent that it may share information with third parties that are vaguely defined. And Betternet and Hotspot Shield provided only a partial list of the types of third parties that they share user information with.

We looked to see whether the company clearly disclosed the name of third parties with which it shares user information. Eleven VPNs provided a comprehensive list or mention of third-party names and claimed they don't share personal information with third parties not included in the list. F-Secure Freedome VPN scored worst here, without any kind of mention at all. Betternet, Hotspot Shield, and TunnelBear got partial credit for listing multiple different types of third parties but did not claim to be limited to that list.

With the exception of Kaspersky, each VPN clearly disclosed in its privacy policy or terms of service whether it shares information with government or legal authorities.

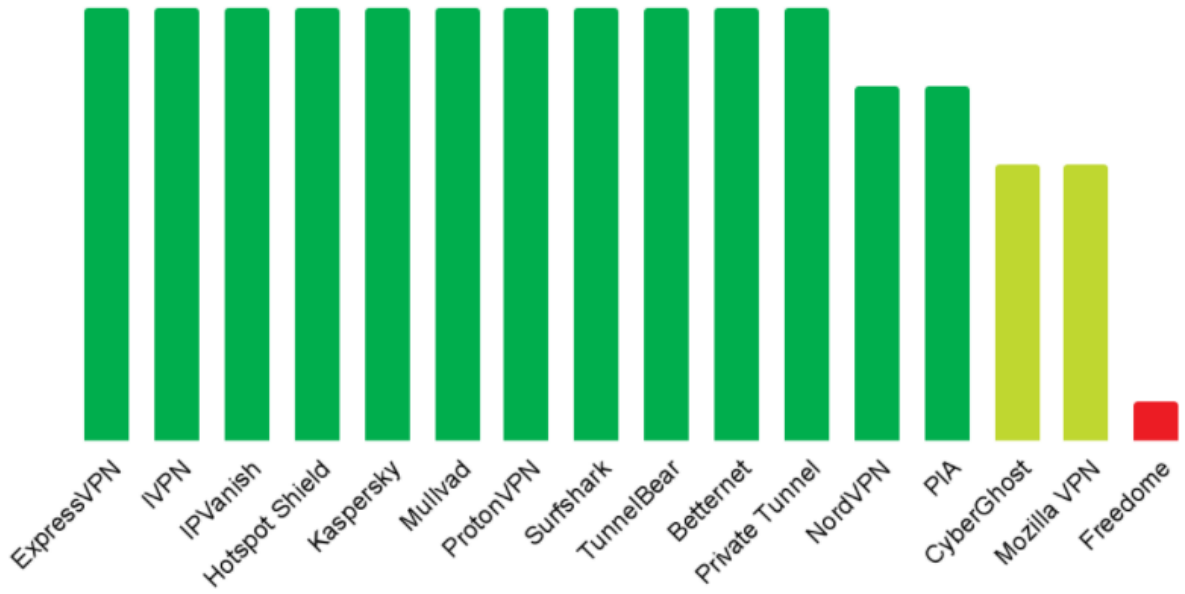
We checked to see whether third-party domains contacted by the product or service were named in the privacy policy, and endpoint analysis perfectly matched with what was stated in documentation for all the VPNs we tested.

All VPNs except CyberGhost and F-Secure Freedome VPN explicitly disclosed every way in which they use consumer data in a detailed and comprehensive way, including information directly concerning the use of the information gathered, and making it reasonably apparent that the consumer is at no point excessively yielding their privacy through the company's use of the data. F-Secure Freedome VPN provided only vague or generalized information on how consumer information is used, not claiming in strong enough terms that it limits data use. CyberGhost did a little better by including information directly concerning the use of information gathered.

Overall, F-Secure Freedome VPN scored poorly in the data control section and would benefit by committing not to sell, rent, or share personal data unless it's to complete necessary services explained in the privacy policy, such as payment. Mozilla VPN could also improve its rankings by listing all of the ways in which it might use consumer data or by limiting these ways to the ones listed.

IVPN did well with its statements that no third parties have any access to user data, and that all first- and third-party tools are hosted on its own servers—and by giving options and clearly outlining the information required when using outside parties, such as payment processors. For example, IVPN uses the open source web analytics platform Matomo, hosted on its own server infrastructure, to analyze information about website visitors.

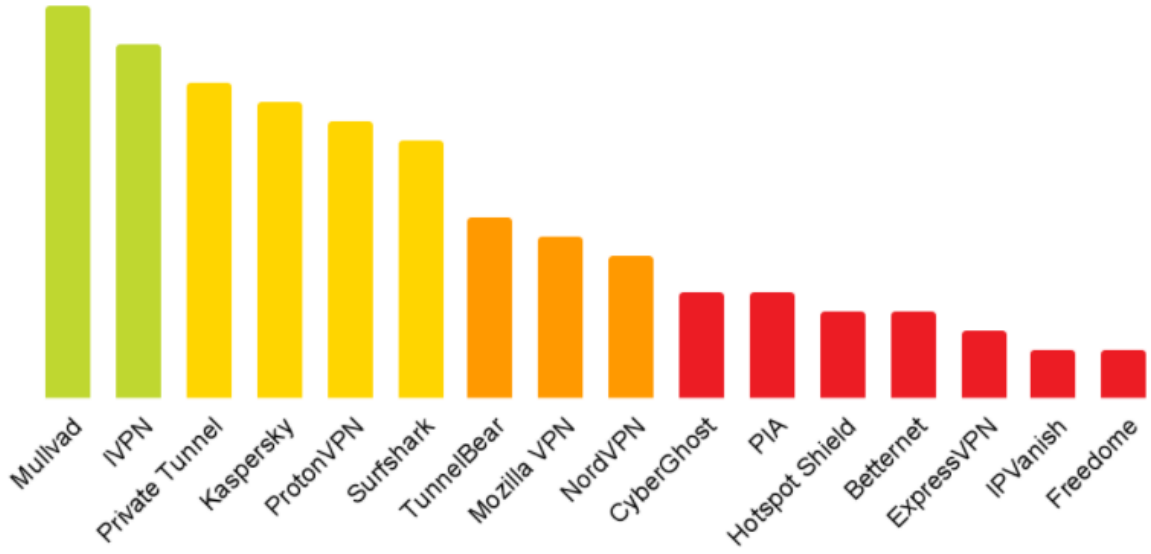
Data Use and Sharing: Data Use



We looked at whether companies put limits on the use of data that's consistent with the purpose for which it was collected. F-Secure Freedome VPN did the worst here, making only a vague statement that it will limit what's necessary. Mozilla claimed it will use data as stated in the privacy policy but also stated that it may use consumer information outside of it with consent. Cases for consent were not outlined, but it's clear that the company may use data that it does not need to provide or maintain the service. CyberGhost, NordVPN, and PIA got partial credit for claiming they'll use data only as stated in documentation, and if use can be done with consent, they outlined the consent mechanisms. All of the other VPNs we looked at scored top marks for making a direct, clear, and precise statement claiming that the company itself puts limits on data use in order to provide and maintain the service.

F-Secure Freedome VPN failed to explicitly list each way it uses consumer data, providing only generalized information on how it is used. And though CyberGhost provided a detailed list of how information is used, it wasn't reasonably apparent that the consumer was not excessively yielding their privacy through the company's use of their data.

Data Retention and Deletion



We looked at whether the companies claimed, on their own, to either delete outdated and unnecessary personal information or render it to be reasonably deidentified.

In last place were CyberGhost, F-Secure Freedome VPN, IPVanish, NordVPN, PIA, and Surfshark, all of which claimed not to delete outdated or unnecessary user information or were vague as to what they do after they no longer need to retain personal data either internally or contractually. Faring only a tiny bit better were Betternet, ExpressVPN, and Hotspot Shield, which made vague reference to not retaining outdated or unnecessary information if they are legally obligated to do so. IVPN, Mozilla VPN, and Private Tunnel got partial points for saying information will no longer be retained or will be deleted, destroyed, or anonymized/deidentified. Only Kaspersky, Mullvad, ProtonVPN, and TunnelBear stated that outdated or unnecessary information will be deleted or destroyed.

We looked for specific retention periods for different types of information, reasonably scoped to get rid of outdated and unnecessary personal information. Kaspersky, Mullvad, Private Tunnel, and Surfshark earned top marks for having reasonable hard deadlines for destroying or deleting data. IVPN provided reasonable retention periods, but only for a few pieces of information. All of the other VPNs didn't do as well, either not mentioning retention periods at all or saying retention periods will be dictated by law or as long as the company is obligated to keep information for internal or legal reasons.

We looked in the privacy policy for controls allowing users to delete data that was not necessary, and how easy those controls were to find and use. IVPN, NordVPN, and Private Tunnel made it easiest. CyberGhost, Mozilla VPN, PIA, and Surfshark asked users to contact the company. Mullvad did the same, but it does not keep any real personal data. IPVanish also asked users to call or email, though it was unclear whether this applies only to those under CCPA or to all users.

ProtonVPN and TunnelBear scored a little lower for providing proprietary controls with vague, unclear descriptions—or for reserving the right to alter or remove the controls.

Betternet, ExpressVPN, F-Secure Freedome VPN, Hotspot Shield, IPVanish, and Kaspersky did the worst, either only providing controls under GDPR and CCPA or reserving the right to refuse a removal request if deemed impractical or unnecessary—with the reasons for rejection undefined. (Although this wasn't factored into our rankings, we noticed that Betternet's website has a dead link to a page that users are directed to when clicking on "do not sell my personal information.")

When a consumer's service is terminated or it no longer operates, only IVPN and ProtonVPN claim to delete user information immediately and permanently, within a reasonably short (under 30 days) time frame after an account is canceled or deleted, unless there is a valid and reasonable need to maintain data, such as an active legal proceeding. The VPNs were transparent about the fact that backups containing user data could retain personal information.

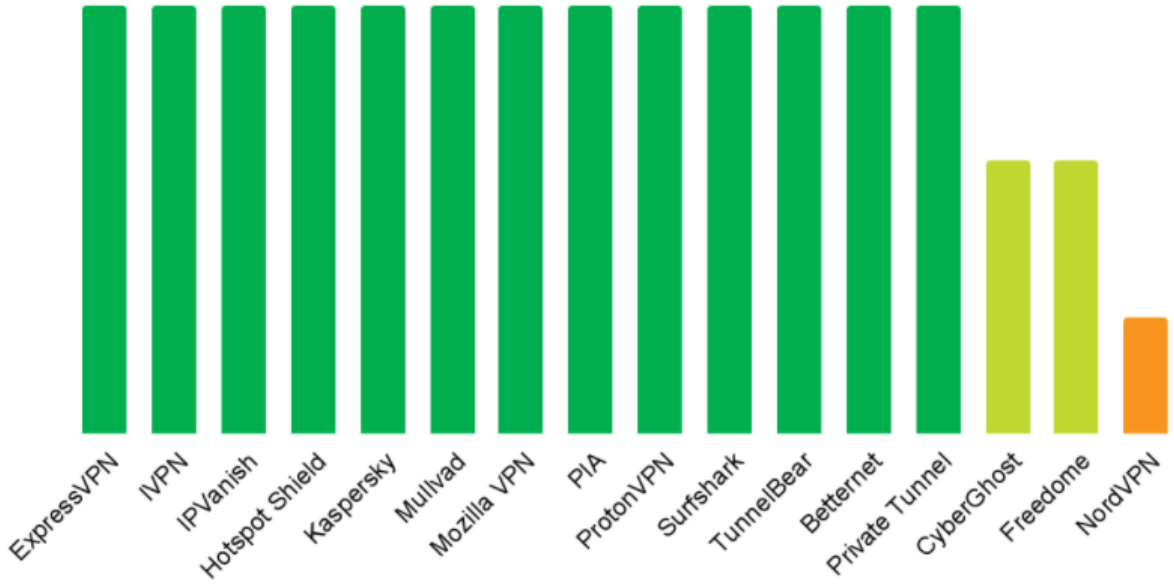
Betternet, Hotspot Shield, and Private Tunnel did a smidgen better here, with unclear descriptions about what happens to user data or descriptions that don't point to its deletion.

Kaspersky, Mullvad, and Surfshark received partial credit for addressing what happens to personal user information when an account is closed or deleted, stating that it is not immediately deleted or is retained for some period of time.

The other eight VPNs (CyberGhost, ExpressVPN, F-Secure Freedome VPN, IPVanish, Mozilla VPN, NordVPN, PIA, and TunnelBear) stated or made it reasonably apparent that data would be retained after an account is terminated, failed to clarify the difference between disabling and deleting the account, or didn't provide information regarding the handling of personal information after an account is deleted.

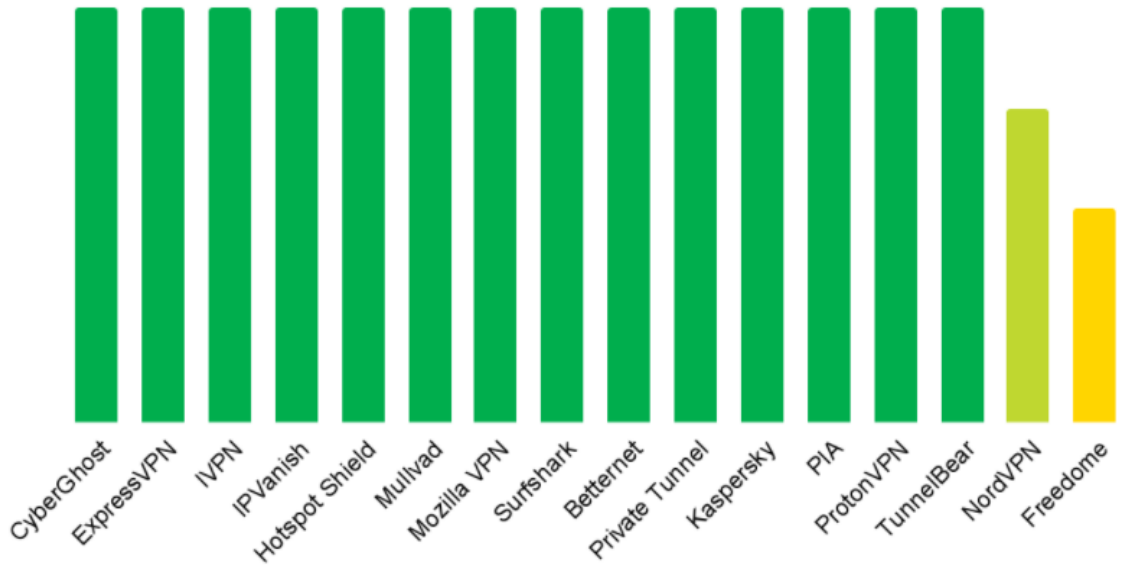
We checked to see whether companies consider user information to be assets transferred in a case where the company is acquired, merges with another company, or declares bankruptcy. Every VPN failed except for Mullvad, which doesn't have data to hand over to a company—including cookie data, because all data auto-deletes as soon as the browser closes, with the exception of Stripe cookies (if used). The other companies stated or implied that user data is an asset that will be transferred or didn't distinguish between bankruptcies, mergers, or acquisitions.

Overreach/Collecting Too Much Data: Data Benefits



We looked to see whether each company clearly discloses its purpose for collecting each type of user information. NordVPN did the worst here, storing executables (presumably indefinitely) without making it reasonably apparent that the collection justifications benefit the user. Reasons for why data were collected were vague. CyberGhost and F-Secure Freedome VPN did a little better than NordVPN: The two VPNs described justifications for collection of data, which seem to benefit the user. All of the other VPNs we tested got full points because the justifications did not include unnecessary or extraneous usages of collected data.

Overreach/Collecting Too Much Data: Data Collection

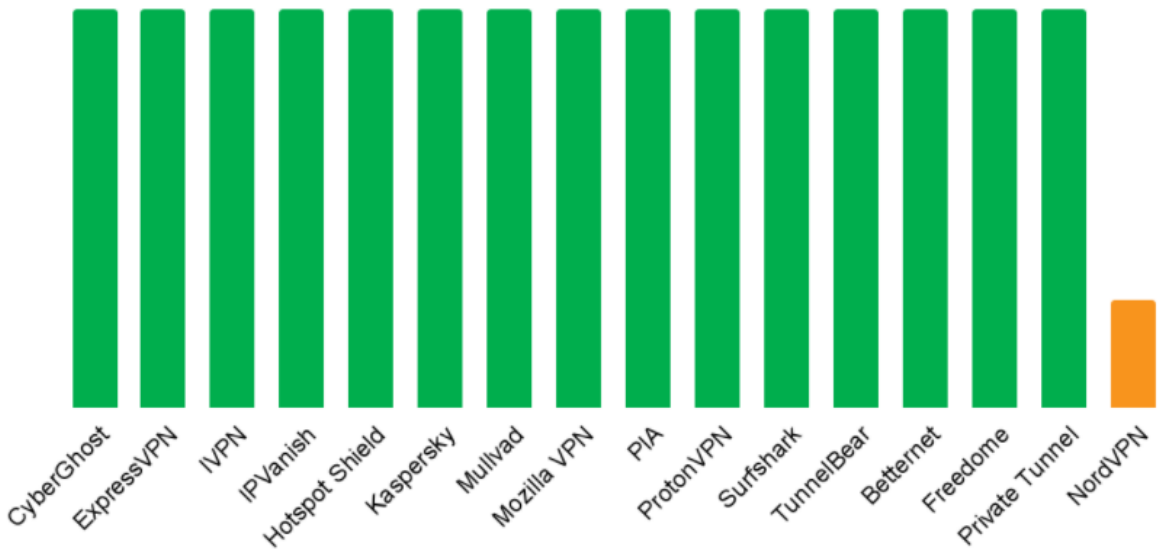


We looked to see whether the company clearly disclosed the type of user information collected. This is one area where F-Secure Freedome VPN fell short, and NordVPN got only partial credit. F-Secure Freedome VPN provided only a few references to the types of user information collected. NordVPN provided details on the types of information collected, but it was not reasonably apparent that it did not collect unnecessary or excessive types of information that might infringe on the rights of the users.

We looked at whether the company clearly disclosed how information was collected. F-Secure Freedome VPN was the only VPN to score poorly here, providing only a few references. Every other VPN provided a detailed reference on how it collects this information, and it was reasonably apparent that the methods weren't overly invasive and do not infringe on the rights of users.

We looked to see whether the company provided detail on the information collected about its users from third parties, which all companies did. Though NordVPN, like the other VPNs, clearly stated that user information was collected from third parties and stated the type of information collected, it did not make it reasonably apparent that the information collected from third parties was not excessive or unnecessary.

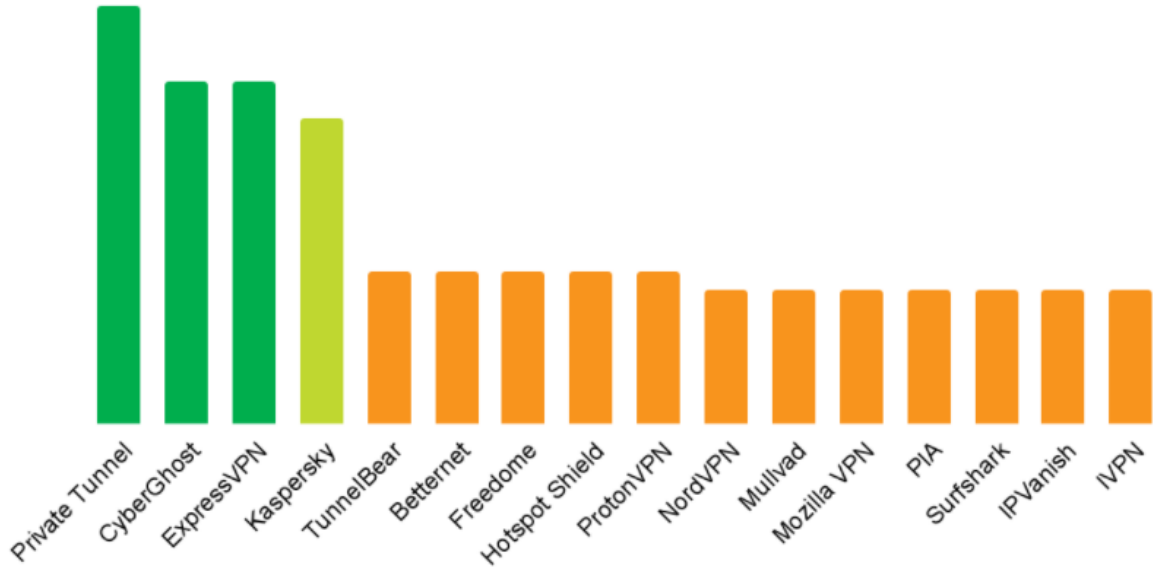
Overreach/Collecting Too Much Data: Minimal Data Collection



Every company except NordVPN claimed to limit data collection and provided a complete list of data elements that align with the functions or features the service delivers, or claimed to only collect information needed to provide the user with the services they're opted into. NordVPN provided a list of the various grounds on which it collects and processes data, stating that it is able to collect and process this data only if it falls within the listed use cases. NordVPN provided no specific declaration of collecting only what is needed.

We also looked at whether the product worked when permissions not relevant to the functionality (such as anonymous usage data) were declined, which was true for all VPNs (though some didn't offer permissions). They all either worked when permissions not relevant to the functionality were declined or didn't ask for such permissions.

Overreach/Collecting Too Much Data: Privacy by Default



We checked to see whether default settings were the most private.

Private Tunnel was the only VPN where we know with certainty that the default settings were the most secure. Others made automatic selections—and it wasn't clear what they were—disabled their kill switch, or required users to choose between different protocols. CyberGhost and ExpressVPN defaulted to an unknown-to-the-user protocol, and IPVanish had a disabled kill switch and no autorun or ability to launch at startup. Hotspot Shield made an automatic connection and its kill switch was disabled, Kaspersky VPN didn't list its protocols, and NordVPN's kill switch and autoconnect were disabled. Mullvad had an automatic selection between OpenVPN and WireGuard, Surfshark's kill switch was disabled, Betternet's kill switch was off by default, and F-Secure Freedome VPN had no autorun and its kill switch was disabled. Betternet stood out for having an unclear autoselect ("our unique protocol, fastest in the industry, and bank-level secure") or allowing users to choose IKEv2 (IPsec).

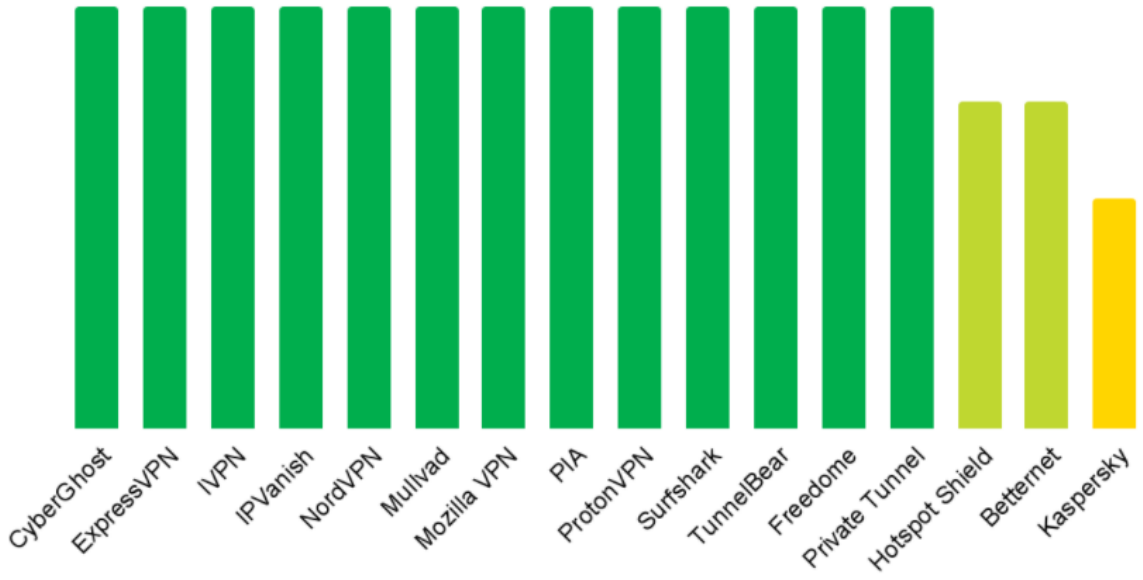
We looked to see whether controls for targeted ads exist and were off by default. Each VPN either had targeted ads off by default or didn't have them at all.

We checked whether the privacy/security features were equivalent even with a free version or with auto-renewal turned off. Only Kaspersky VPN didn't meet our standard: It allows only paid users to access its kill switch. Seven VPNs did not offer a free version.

We looked to see whether user interface settings optimal for privacy were set by default, which was the case for Kaspersky and Private Tunnel. CyberGhost had an anonymous usage data submission setting option at setup. It was on by default but obvious to the user. ExpressVPN allowed users to choose during setup whether or not to share crash reports, speed tests, and other diagnostics. For IVPN, launch at login and autoconnect were disabled. The other VPNs mentioned also had the same kill switch and autoconnect issues mentioned previously.

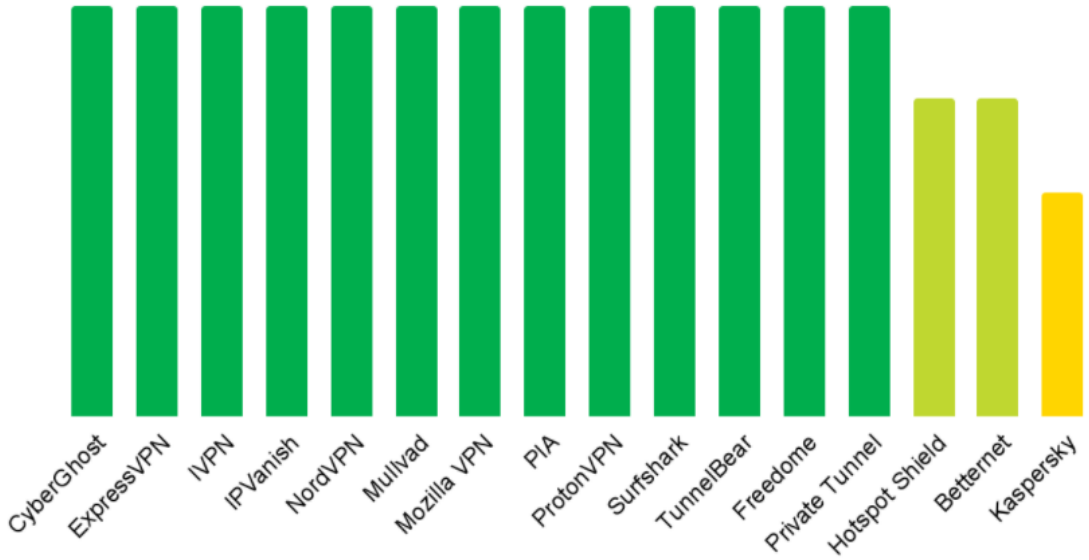
It's possible that some VPNs do not have the most secure settings (such as kill switches) on by default because it would hurt usability. **Users may want to check the settings of the VPNs to ensure that the privacy settings they expect are enabled before using the service.**

Governance: Privacy Policies and Terms of Service



Each VPN clearly disclosed which terms of service applied to the product in question. Both the terms of service and privacy policy documents were easy to find for each VPN product except for Kaspersky, which had a privacy policy and terms of service that were both difficult to find.

Governance: Privacy Policy and Terms of Service Update Notification



Only Betternet, Hotspot Shield, IPVanish, IVPN, and PIA committed to notify users about terms of service changes both with email and with a notice on their sites. CyberGhost, ExpressVPN, Mozilla VPN, NordVPN, and ProtonVPN offered one or the other, with Mozilla VPN saying it will do so before the changes go into effect. The other VPNs will update their ToS page but may not provide any notification that they have done so.

Consumer Reports updates the date of the privacy policy and user agreement when we make changes to either document, and will display a notification, notify users by email, or communicate the change by other means if we deem the change to be material.

As for privacy policy changes, only Betternet, Hotspot Shield, and IVPN stated that they will notify users about terms of service changes both with email and with a notice on the site. CyberGhost, Mozilla VPN, NordVPN, PIA, and ProtonVPN offered one or the other, with PIA saying it will do so before the changes go into effect.

Betternet and Hotspot Shield maintain a public archive or change log of both their privacy policy and terms of service. IPVanish maintains one just for ToS changes.

In some cases, a VPN provider may not require an email address. If this is the case, there may be a need for users to manually check for software updates or privacy policy updates.

Recommendations for Industry Improvement in Privacy

We identified some specific areas that could use improvement industry-wide.

- We found that every VPN company we evaluated could do better when it comes to committing to **allow users to obtain the public-facing and private user information that the company holds,** including users not covered under CCPA or GDPR.
- Many of the VPNs we tested could improve by **providing specific retention periods for any data they do collect.**
- VPNs would better serve their users by **explaining in detail how user data is handled in case of a merger, bankruptcy, or acquisition.**
- The industry could improve by **giving specific retention periods** for destroying or getting rid of outdated or unnecessary personal information. Almost every VPN, including Mozilla VPN and Mullvad, failed to state in their documentation that they will delete user information immediately and permanently in a reasonable time (in this case, 30 days) if service is terminated or inoperable.
- We'd like to see VPNs **clearly outline in their documentation which information outside parties require,** provide options, and **host first- and third-party tools on their own servers**—something only IVPN has done.

Other Issues

A number of technical issues arose in the course of testing VPNs, some of which weren't originally included in our testing process. There were also several areas of concern that would be difficult to fairly quantify across VPNs but which we thought were worth addressing.

Local Logging

Consumers should be aware that while many VPN providers indicate that they do not keep logs, this usually cannot be verified, and in many cases logs were found on the local Windows system that included usernames, emails, IP addresses, and other potentially sensitive information.

Some VPNs left logs that might contain sensitive information on their Windows machine in a variety of places, such as C:/ProgramData and %AppData%, that can persist even after the program is uninstalled.

For example, in IPVanish, the username and all IP logs (with time stamps) are saved locally. This shows what IP the user came from, what IP the user connected through, and when the connection happened, as well as a username.

IPVanish: Locally Logged Username and IP

```
17:04:35 [Verbose] (VpnSDK) LocationChanged="(IPv4) 47.[redacted](United States,[redacted])"
17:04:35 [Verbose] (VpnSDK) AuthenticationStatu Authenticated
17:07:46 [Verbose] (VpnSDK) VpnConnectionStat nnecting
17:07:47 [Information] (VpnSDK::RAS) Connectin "nyc-a97", Protocol=IKEv2
17:07:49 [Verbose] (VpnSDK) VpnConnectionStatu nnected
17:07:49 [Verbose] (VpnSDK::Filtering) Applying DNS leak prevention. VPNAdapter="IPVanish"
17:07:49 [Verbose] (VpnSDK::Filtering) Applying IPv6 lea revention. VPNAdapter="IPVanish"
17:07:49 [Verbose] (VpnSDK::Filtering) Lowering interfa tric for faster DNS resolution.
17:07:49 [Verbose] (VpnSDK) LocationChanging
17:07:50 [Verbose] (VpnSDK) LocationChanged="(IPv4) 173.195.15.125 (United States, New York)"
```

A ProtonVPN username was found in a local log, as well as a multitude of other encrypted strings with labels indicating an abundance of tracking points, such as latitude and longitude, ISP, IP, country, etc. Because this data was encrypted, we couldn't determine what exactly was logged in each category. However, the username was found in the local log in plaintext.

ProtonVPN: Locally Logged Username and Other Data

```
<setting name="Username" serializeAs="String">
    <value>
    AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAfzFbwohcWk
    2mYbHvIF19zFuduvNHICoGnN1Y5Pz0T1YCyhxdWBDK
    6q/0eND4SbmGuiBiBCd3EerM3qEdRBuKhY</value>
</setting>
<setting name="Ip" serializeAs="String">
    <value>
    AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAfzFbwohcWk
    VDyCUkrTUH4GkfGzhc2Ya/RjlXXwmXqhQXed16Dvfv
    kpwBZUhn91ZKU=</value>
</setting>
<setting name="Latitude" serializeAs="String">
    <value>
    AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAfzFbwohcWk
    qDCXgChVQFnk26yzSQuLrI0EmBAx5/71Idz7VFmjoI
    1kdiALOXi5958=</value>
</setting>
<setting name="Longitude" serializeAs="String"
    <value>
    AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAfzFbwohcWk
    XPGz7h4/eBnfIDZqSWRzTQkolCGZouZHBOTY8upsOz
    rlrtESRON2bf0=</value>
</setting>
<setting name="Isp" serializeAs="String">
    <value>
    AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAfzFbwohcWk
    Mki/NefdIxV9t9iSa0olzqf3wor0JM6rElFdECNhKq
    9tZyxYVgtGGJ0=</value>
</setting>
<setting name="Country" serializeAs="String">
```

```
</setting>
<setting name="UserVpnUsername" serializeAs="String">
    <value>
    [{"User":[redacted]IL","Value":"AQAAANCMnd8BFdERjHoAwE/Cl
    E+8oALolh/[redacted]AAAAIAACAAAADPV39lx4Ei2hbmQxOf2v83rgyk
    Zlslb88OfPkkjd/zwktakBhi6glIaTiJg3OwhVOQev6vaoYTLvyxVUUiOPhdNk
</setting>
<setting name="UserVpnPassword" serializeAs="String">
    <value>
    [{"User":'[redacted]AIL","Value":"AQAAANCMnd8BFdERjHoAwE/Cl
    fi8TmyqmWtXcRqugAAAAAOgAAAAAIAACAAAACAlGIcAvkz7YoZBT6ixva98NFR
    WFAAAAA66DROvAqLLoltEAyHVVGEPm7pySXVFDllgPoNCKwllayYSEajBpkZf5
```

With Surfshark, the email address used and other data, such as an authentication token and recent connection location, were stored locally.

Surfshark: Locally Logged Email Address and Other Data

When testing Mozilla VPN, we found a private key that we believe was consistent with a vulnerability Mozilla found and has since fixed.

Although there was no personal data included, TunnelBear's local trace log showed app navigation along with a time stamp for each click.

TunnelBear: Locally Logged Data

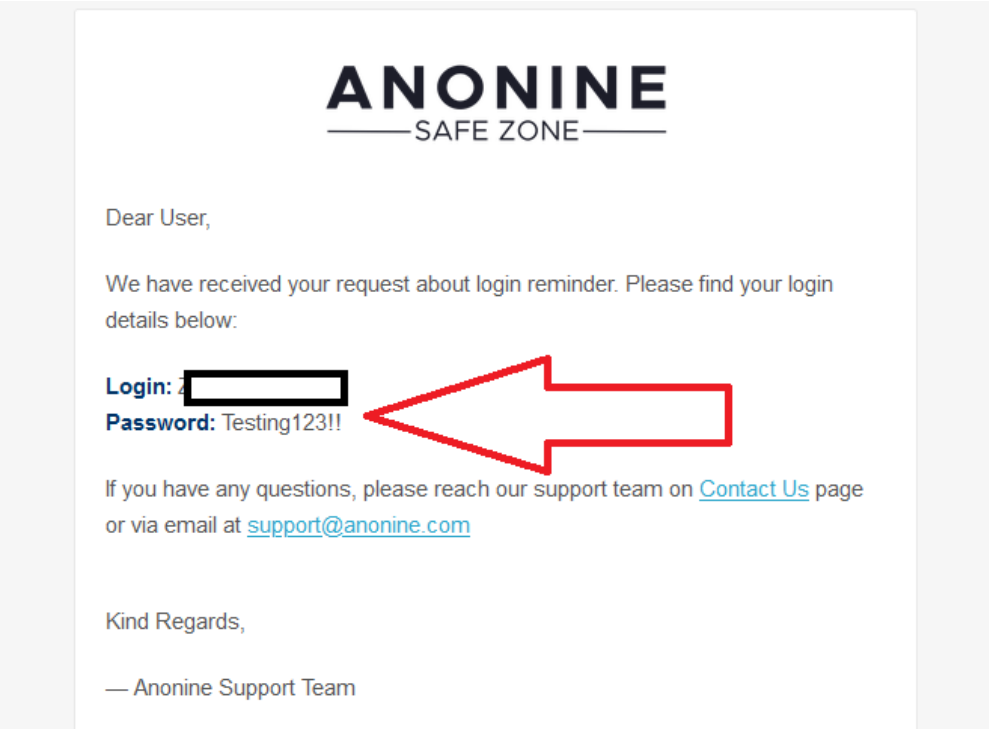
```
15:55:07,420 [1] INFO  - Navigate: SETTINGS
15:55:07,472 [1] INFO  - Navigate: SETTINGS
15:55:07,502 [1] INFO  - Home unloaded
15:55:27,141 [1] INFO  - Navigate: HOME
15:55:27,154 [1] INFO  - Navigate: HOME
15:55:27,164 [1] INFO  - Home loaded
15:55:27,164 [1] INFO  - ApplyTheme: Black
15:55:41,138 [1] INFO  - Set IsOn: True
15:55:41,140 [1] INFO  - OnIsOnChanged
15:55:41,147 [1] INFO  - Connecting Fastest...
15:55:41,148 [1] INFO  - OnVpnStatusChanged
15:55:41,148 [1] INFO  - Current Connection Id eff3cb66-705b-47cf-9
15:55:41,149 [1] INFO  - Test VigilantWithUntrustedNetwork
15:55:41,157 [1] INFO  - MapService Connecting check transactionId
15:55:41,157 [1] INFO  - MapService Connecting...
```

Additionally, though not part of the 16 VPNs tested against the Digital Standard, the following behaviors were noted on other VPNs:

- Anonine was able to provide a user password in clear text via email, indicating that it was both stored and transmitted in an unencrypted format. In response, the company said, "In some cases that is the only way to let user access their account, also we notice that client should change this password."

- Encrypt.me was found to log the user's email address locally in clear text.
- Windscribe's local logs had both the local and remote IPs saved, with an obfuscated octet.

Anonine: Password Emailed in Clear Text



ANONINE
SAFE ZONE

Dear User,

We have received your request about login reminder. Please find your login details below:

Login: [redacted]
Password: Testing123!!

If you have any questions, please reach our support team on Contact Us page or via email at support@anonine.com

Kind Regards,

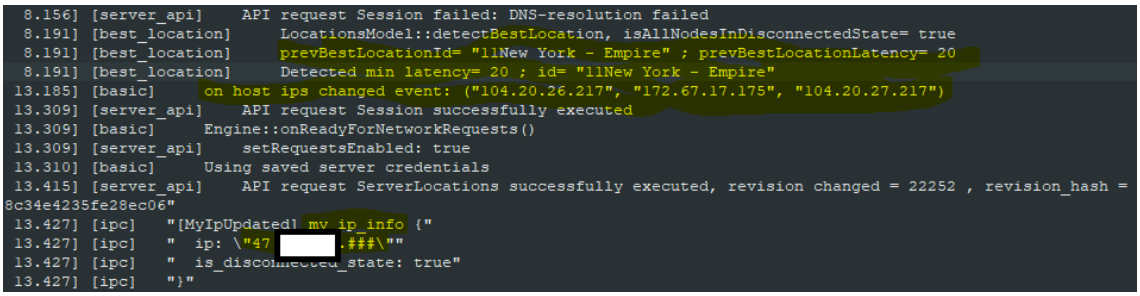
— Anonine Support Team

Encrypt.me: Locally Logged Email and Account ID

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <userSettings>
        <CloakUI.Properties.Settings>
            <setting name="LastEmail" serializeAs="String">
                <value>[redacted]mail@gmail.com</value>
            </setting>
            <setting name="UseSparkleBetaURL" serializeAs="String">
                <value>False</value>
            </setting>
```

```
2021-05-24 10:38:10.345 -04:00 [Debug] [PropertyProvider<CloakAccount<>>] UpdateProperties - updating "CloakService.CloakAccount" from
"CloakAPIDataTypes.Account"
2021-05-24 10:38:10.417 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "Email" = "[redacted]@gmail.com"
2021-05-24 10:38:10.499 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "AccountID" = "usr_v6fiktrjps5te6cb"
2021-05-24 10:38:10.598 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "IsVerified" = True
2021-05-24 10:38:10.687 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "EmailOptIn" = False
2021-05-24 10:38:10.804 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "Content" = "CloakService.CloakAccount+ContentHolder"
2021-05-24 10:38:10.911 -04:00 [Debug] [PropertyProviders.PropertyGroup] Property changed: "IsRegistered" = True
2021-05-24 10:38:10.911 -04:00 [Information] [CloakService.CloakIPCService] Raising event Registered in all connected clients
2021-05-24 10:38:10.911 -04:00 [Debug] [CloakService.CloakIPCService] Raising event Registered in client with ID "uuid:da8065e7-c568-4a0f-8a0a-
fb3d8e40743a;id=1"
2021-05-24 10:38:10.913 -04:00 [Debug] [CloakService.CloakDeviceProvider] Releasing SyncLock
2021-05-24 10:38:10.969 -04:00 [Information] [CloakService.CloakIPCService] Get Support Ticket request from Client with ID "uuid:da8065e7-c568-4a0f-8a0a-
fb3d8e40743a;id=1"
```

Windscribe: Locally Logged IPs



Combined, these local logs raise the obvious question: If VPNs are not transmitting (using) that information, why was it collected on the local device at all?

Dark Patterns

In the past, NordVPN was called to task in a subreddit called r/assholedesign for disabling features when users turned off auto-renewal and for a "70% off" ad with fake timer that reset if users didn't subscribe.

Though we didn't come across either issue, we did come across other dark patterns, where four VPNs made it difficult to stop auto-renewal or cancel.

Our testing team found that ExpressVPN had an unusual user interface to cancel a subscription, requiring a consumer to click a button to turn off automatic renewal a total of three times.

NordVPN required multiple clicks to unsubscribe, followed by accessing an email confirmation (which expired in 15 minutes) to complete the cancellation process.

PureVPN had no menu method to unsubscribe and required consumers to either use the third-party payment processor or create a support ticket to do so.

Similarly, Surfshark made it hard to cancel the subscription: A tester on our team needed to send an email to do so.

Human Rights and Corporate Social Responsibility

Because VPNs handle a tremendous amount of user data, many sell themselves on trust. It's difficult for consumers to know how carefully the data is protected. For that reason, some users might find that accusations of wrongdoing by a VPN, its executives, or its parent company affects whether they want to give the company their business. Companies with long histories often draw media and social media attention to their executives or the behavior of their parent

company. VPNs and their owners, in turn, are often quick to deny misbehavior or to say that it doesn't impact their users.

Our testing didn't consider a company's reputation or any past scandals, but such details do frequently arise in discussions among security researchers as well as consumers.

Recently, ExpressVPN's CIO, Daniel Gericke, was one of three men who received a $1.6 million fine by the U.S. Department of Justice for hacking and spying on U.S. citizens (including journalists and activists) on behalf of the United Arab Emirates (UAE) as part of Project Raven. Reuters reported that some of the human rights activists Project Raven spied on were later tortured by UAE security forces. The company affirmed its support of Gericke in a blog post and did not state that it would terminate him. Gericke did not make any public statement himself.

ExpressVPN is owned by Kape Technologies, which was previously named Crossrider. And Crossrider was a plugin development platform that allowed users to distribute ad injection software, which some considered malware. (Kape did not respond to a request for comment.) Kape also previously operated software called Reimage, which is said to enhance computer performance but has been reported to signal false positives on its security tests in order to sell its premium service. Teddy Sagi, the owner of Kape Technologies, was listed in the Panama Papers as a sole shareholder of at least 16 offshore companies—primarily real estate—established through Mossack Fonseca, according to Haaretz. In 1996, 16 years before he acquired Kape Technologies, Sagi was sentenced to nine months in prison for bribery and fraud, according to the Financial Times.

PIA is also owned by Kape Technologies. Before its acquisition, the company hired Mark Karpeles, who was the former CEO of Mt. Gox Bitcoin platform. According to CNN Business, Karpeles was found guilty of illegally altering Mt. Gox's electronic records to falsely inflate the company's holdings by $33.5 million and was sentenced to 2½ years in prison, with a four-year suspension, which means he won't have to serve time unless he commits a criminal act during that time. Karpeles was acquitted "on the more serious allegations of embezzlement and aggravated breach of trust," according to CNN. He maintained his innocence throughout the trial and hasn't made any recent statements to the media.

PIA founder Andrew Lee owns Freenode Limited, where there were mass resignations of staffers after a dispute over changes he imposed, according to Vice and Ars Technica.

Kaspersky Lab has faced allegations of engaging with the Russian FSB, which it has denied. In fact, the U.S. Department of Homeland Security banned Kaspersky products from U.S. government departments in 2017, and its ads were subsequently banned on Twitter, according to Reuters. There have also been news reports about allegations that hackers working for the Russian government stole confidential data from an NSA contractor's home using Kaspersky antivirus software, and the Wall Street Journal reported on allegations that the Russian government uses Kaspersky antivirus software to "secretly scan computers around the world for classified U.S. government documents and top-secret information, modifying the program to turn it into an espionage tool." Kaspersky denies these allegations as well. (It was found in 2015

that the antivirus software was not using security best practices.) CEO Eugene Kaspersky has worked for the Russian military, which was mandatory, and was educated in a KGB-sponsored technical college, though the company denies direct ties or engagement with the Russian government. Kaspersky Lab has committed to increased accountability, migrated some of its core infrastructure from Russia to Switzerland, and has solicited independent reviews and analysis of its source code.

Logging

VPNs often promise to not keep logs, leading privacy enthusiasts and criminals alike to falsely assume that their data is private. This idea is often dispelled in court documents, like when IPVanish handed over logs that weren't supposed to exist. This happened when IPVanish was owned by Highwinds Network Group. Its next owner, StackPath, told TorrentFreak that the VPN under its management did not keep logs. IPVanish is now owned by Ziff Davis, previously called J2 Global. According to the site ProPrivacy, the IPVanish site itself claimed not to keep logs both before and after the incident.

ExpressVPN, on the other hand, told investigators it did not have any logs or customer data on a server in Turkey, which was raided by Turkish authorities, according to Hurriyet Daily News. According to the site, authorities said the server was used to hide details regarding an assassination of a Russian ambassador. ExpressVPN released a statement about the incident.

Separately, PIA was unable to provide logs in both a 2016 investigation (paywall) into a fake bomb threat and a 2018 hacking case, according to various media reports and legal documents.

Inaccurate Presentation of Products and Technology

VPNs can offer some protection on untrustworthy WiFi networks, help circumvent some censorship blocks, keep your browsing habits away from ISPs, and limit some types of tracking—such as your IP address from websites you visit and the domains you connect to from your ISP. But masking an IP address is not the same as granting anonymity.

Not only can VPN providers see your real IP address but companies can also use many other methods to track users, such as device fingerprinting, browser fingerprinting, web cookies, tracking pixels, and more. Websites often request data that can pinpoint people's geographic location, such as WiFi networks, device location based on GPS, cell tower identification (CDMA or GSM cell IDs), and more. Various companies collect wide-ranging data, beyond IP addresses, and sell that information to data brokers. Many of the risks that consumers use VPNs to try to protect against are already largely mitigated through the use of HTTPS. And many risks, such as social engineering, are not mitigated by using a VPN.

However, a number of VPNs do not refrain from making sweeping claims, or using potentially misleading or overly broad language to describe their tool and what it can do.

Sweeping or Overly Broad Anonymity and Privacy Claims

Betternet's website claims "**privacy from online snoops**," despite the fact that there are various other methods used to spy on consumers online. A spokesperson for Betternet's parent company, Aura, did not respond to repeated requests for comment.

CyberGhost offered "**unrivaled internet anonymity**" along with promises to "**keep all prying eyes at bay**" and to help users "**stay untraceable and anonymous online**" and "**safe from hackers and snoopers**." "Turn yourself **digitally invisible**," the copy reads, while promising to "protect your digital identity from your ISP, government authorities, and snoopers," and it says that the tool "prevents ISPs, advertisers, or governments from monitoring, recording, and analyzing your surfing behaviors." It also says users can "**start browsing without worrying about cybercriminals, mass surveillance, and online behavior tracking**." And the service promises "**absolute privacy on all devices**," a bold claim considering digital fingerprinting and nation state resources, especially for a service that's proprietary and from its website does not appear to be regularly audited.

In response to a request for comment, a spokesperson pointed to the latest version of the VPN's ad-blocking capabilities, security suite (including PrivacyGuard, which has features dedicated to helping Microsoft Edge and Mozilla Firefox users limit privacy-invading settings in their browsers, as well as Security Updater and Antivirus, which has new features and the ability to schedule scans, a Prevention Engine to protect users from malicious activity, and a Privacy Assistant to help users assess their privacy levels, with suggestions on how to maximize it. The company also gives users access to a private browser, which it says provides an anonymous browsing experience, a secure photo vault with a PIN and biometric login, an ID guard to

monitor and alert users of data breaches, as well as a password manager. The company also pointed to the resources and guides available on its Privacy Hub.

ExpressVPN says on its FAQ page that its tool "**allows you to stay private, stay secure, and access the online content you want—no matter where you are,**" allows you to "stream and download anything securely, **anonymously**, and with no limits," mentions protecting online banking credentials and social media passwords through VPN encryption, and says that its service is "high speed, secure, **anonymous**."

In response to a request for comment, a spokesperson said the company explains that "a VPN is just one of several layers of protection when it comes to online security and privacy" in a blog post and that the company has "aimed to be consistent and clear in noting that a VPN does not make people fully anonymous online," for example, on this page, as well as in guides on improving mobile security, staying safe while using a browser, how to use the Tor Browser, and so forth. It also stated that consumers can use ExpressVPN with a pseudonym and a throwaway email account. "As with any product or industry, not every nuance can be communicated in every message, especially when there are constraints such as character limits. When we see, for example, leading password manager brands say on their homepages that 'More than 100,000 businesses trust [us to] protect their data' or that users can 'Stop worrying about data breaches,' we understand these not to be claims that a password management is a cure-all for all data risks. When a home security product advertises 'Whole Home Protection,' we understand that it is not the only safety measure that we need to take, and we also understand that there are categories of risk that it is not accounting for (e.g. it won't save my home from earthquake damage)," the spokesperson said.

F-Secure Freedome VPN's copy reads, "**Keep your browsing private and protect yourself from hackers and online tracking**," "explore the internet and **stay safe from harmful and dangerous web pages** to ensure your security and privacy," and "**stop advertisers from tracking you and making money at the expense of your privacy**."

In response to a request for comment, a spokesperson said in an email, "Complete online security and privacy consists of layers. Typically a single point solution does not provide complete protection against all online threats. VPN is one of the tools helping consumers stay safe online and reduce the risk of security and privacy incidents. Due to varying security and privacy needs F-Secure offers a portfolio of products from point solutions for specific needs liked FREEDOME to complete 'cover-it-all' security suites like F-Secure TOTAL. F-Secure is a European security provider operating under strict EU privacy legislation. Where F-Secure FREEDOME differentiates from many other VPN products out there is the fact that it comes with Browsing Protection capabilities. Known malware, phishing and tracking sites are filtered on the gateway level (currently IP addresses and http supported, support for https in development). F-Secure FREEDOME Android comes with antivirus (same as in Mobile Security)."

Hotspot Shield's web copy promises "**anonymous surfing**" and "private web browsing," and to keep user data safe online from "hackers, snoopers, and identity thieves" and secure from "hackers, cyber criminals, and data thieves," and to shield user identity from "hackers and cyber

predators." It also says that "hackers and cybercriminals can steal your personal information—such as credit cards, bank account numbers, passwords, and other personal data—and use it to commit fraud." The site promises that the VPN will "let you conduct your online activities (visit the websites you want, make online transactions, download files) **anonymously, without being tracked and spied upon**." It also says that "Hotspot Shield encrypts your connection and doesn't log any data that could be tied to you," and that it will "never track, log, or store any of your personally identifiable information, including your IP address." But free versions of the app allow personalized identifiers (such as ad identifiers and cookies) and log internet or other network and device activity, as well as geolocation information. Hotspot Shield's parent company, Aura, did not respond to repeated requests for comment.

IPVanish's web copy was often nuanced, but it did have some sweeping statements, claiming to "**shield your internet traffic from third-party spying**," "keep your online presence and information private," "safeguard any connection to handle personal data with **uncrackable security**," "prevent snooping and spying while on public Wi-Fi," and "prevent your personal data (mobile banking, emails, social media, etc.) from being stolen by hackers." A graphic also promised sweeping protection: "**no hackers, no firewalls, no government**," it reads. IPVanish did not respond to a request for comment.

Kaspersky's site reads, "When you're connected to the Internet through a VPN connection, this private Internet access **ensures that you're not exposed to phishing, malware, viruses and other cyber threats**." It says, "Your privacy is also guaranteed, as no one will be able to detect your online behavior." It also promises privacy ("**prevent business and governments from spying on you**") and security ("ensure that your data is not intercepted by cybercriminals") and that it "hides your identity and online activity from businesses and governments recording your behavior." It also says that "whether you do shopping, banking, video calls or emails, **hackers can never intercept and steal your data**."

Kaspersky says it uses "military-grade 256 bit encryption" that "**prevents criminals from stealing the data which you send and receive**." It says that "data encryption also ensures that your online banking and payment details **can never be intercepted**," and that, with the VPN, "you can browse, stream, communicate, and shop safely & away from prying eyes." The company says its VPN will protect you from big companies that harvest and sell your personal data, as well as cybercriminals that intercept name, address, and credit card details each year.

"The marketing statements made on a product page for a VPN refers to the features and functionality of only the use of a VPN for its intended purpose. A VPN is a private internet access and a user visiting a product page of any security company should understand that the features listed are only that of the product in question," a spokesperson said, adding that all marketing materials are accurate for the functionality of the VPN. "VPN technology is effective for several scenarios. For instance, it let users change their IP, including geolocation. Moreover, it protects against surveillance at the 'last mile': all traffic is encrypted, including DNS requests, SNI, which could tell the provider or an attacker who has connected to the network which sites the user is visiting. At the same time, after leaving the VPN server, the traffic is no longer

additionally encrypted, it is almost impossible from the outside to attribute it to a specific user." The spokesperson also stated that various reports indicate "the VPN market is growing and considered as one of key layers of user protections. For a wide range of different threats, users need to use comprehensive security solutions," and Kaspersky VPN Secure Connection doesn't protect from scenarios not relating to IP addresses (such as malware, cookies, or scammers taking control of ISP providers). The spokesperson said that a VPN can disable your internet if a connection drops, and it "creates an encrypted tunnel so no one can read your online data." "Moreover, Kaspersky VPN Secure Connection can help when the payment page can be designed without considering the protection of payment information (or) There may be a last-mile man in the middle attack by forcing the user to install the provider's certificate into the system with a root certificate (practiced in some countries)."

With a few exceptions, **NordVPN** makes sweeping claims, such as, "**all your data stays safe** behind a wall of next-generation encryption" and "**your data will never be compromised** with NordVPN. Work, browse, or use social media platforms safely." NordVPN promises "secure and private access to the internet." A video on NordVPN's site said that a VPN hides not just your IP address but also your "virtual location," and that "thanks to its encryption, **third parties cannot spy on your online activity**." The video recommends a VPN for journalists working under an autocratic regime, because otherwise their freedom or even life might be in jeopardy. And the site says that because a VPN encrypts your connection to the internet, "no one can eavesdrop on the websites you visit or data you share," and that it hides your IP and location, "so snoopers can't track you down." It says that a VPN can help hide your "browsing history, messages, and other private data" from the "**government agencies, marketers, internet service providers**" who "would all love to track and collect" that data. And it advises, "Use it at home, at work, and on the go to enjoy **non-stop protection**."

"We stand with our claims and we put a lot of work to check them and to make them accurate," a NordVPN spokesperson said. "In such statements and slogans we have to explain complicated things in a few words, but almost always those are followed by a deeper explanation in the following paragraph or a landing page. We believe that on our website we provide thorough information on how VPNs work and what value they bring. Additionally, I would like to stress that some of our features surpass the usual benefits of a VPN."

In 2019, a regulatory ruling by the Advertising Standards Authority in the United Kingdom found one of NordVPN's ads to be "misleading in the absence of adequate substantiation." A NordVPN spokesperson said, "In 2019 we tried to create a short, simple, and fun ad, but too much creativity sometimes brings errors. That ad was found to be misleading by the ASA. ...The main problem with the ad was that the creative showcase of the problem could be interpreted in different ways," the spokesperson said.

PIA's website says, "Keep your data encrypted and secure. **Don't let anyone get their hands on your data** like emails, pictures, banking details, or anything else best kept private." It says that hiding internet traffic data from ISPs or network administrators via the product "**prevents your browsing data from being stored, collected, and sold by third parties**." The site says that by hiding your IP address and changing your virtual location, "**you can avoid being**

tracked by advertisers." The site previously said that you can "**anonymously connect to the internet through a PIA VPN server, then nobody can track your activity**," but this statement was removed, a spokesperson confirmed.

A spokesperson for PIA said, "We at PIA also believe in truthful, honest advertising, and we don't like the marketing 'tricks' that many VPNs use to sell their products—that's why we've taken a different approach and don't try to scare people into purchasing our product. VPNs are a very useful tool in the internet user's toolkit, and we're happy to honestly portray how PIA's VPN can help users enjoy more digital privacy and online freedom." They agreed that the vast majority of websites and apps are already encrypted, and said, "You're 100% correct in that the vast majority of websites and apps are already encrypted, and hence, a VPN's extra encryption is more of a safety net than something absolutely necessary. But that doesn't change the fact that it *is* a safety net. A VPN *does* keep your data encrypted and secure, as it makes 'man-in-the-middle' attacks significantly more difficult to occur, encrypts traffic going to 'http' sites, and provides an extra layer of protection in the event a zero-day attack is able to overcome/imitate a TLS certificate or otherwise breach an encrypted data transfer. The latter does indeed happen, and the menace of zero-day attacks is that no one knows until after the breach has happened that anything was wrong. A VPN provides an additional level of encryption that makes many, myself included, feel safer when accessing the internet from insecure locations." The spokesperson also said that although they don't believe the language is misleading, some of it would be changed to be more specific. "All of the website's top pages have been updated to reflect this honest approach to VPN marketing, and the entirety of the website (only low-trafficked pages remain) will reflect this as soon as is possible."

"I think PIA is one of the few honest VPNs who's trying to 'tell it like it is' and doesn't need to mislead or be overly aggressive in its advertising," the spokesperson said. Additionally, they said the company is producing an in-depth informational video and blog post "explaining precisely what a VPN is and what it isn't, where we examine all the use cases for a VPN and dispell some common marketing tropes."

Though not as egregious as some examples, **Private Tunnel** makes some sweeping claims. It says that you can "**protect yourself against malware and DDoS attacks**" and "be secure, be protected, be private, wherever and whenever you surf the net," and that you can stop hackers: "If your computer is already infected with malware, Private Tunnel will block communication to the hacker's server." Though that's not necessarily technically wrong, some malware can damage your device even when you're offline.

A spokesperson said that Private Tunnel shouldn't be included in the same category as consumer VPNs, because it's primarily focused on providing next-gen technology to SMBs and enterprises. "Legacy VPNs are limited in their capabilities for consumers. This is why for the past 4 years we've worked to develop next-generation OpenVPN, specifically tailored for businesses. Cyber Shield is a feature of our new product OpenVPN Cloud and it offers some powerful security tools. While we do own Private Tunnel, we are beginning to sunset it and directing private tunnel users to Cyber Shield because it comes with 3 free concurrent connections and is more robust than a legacy VPN. We've spent the past several months

informing our customers and encouraging them to make the switch. Although not our target audience, for the security conscious consumer, it's a very good option. Regarding your questions, in the spirit of transparency, the marketing copy for Private Tunnel was developed 6 years ago and we have been in the process of updating it. Back then, it was reasonable to cite the IP address obfuscation offered by consumer VPN as a privacy strategy. As a company, we thrive in the complex requirements of the Business VPN space that include remote access, site-to-site, IoT security, network virtualization, and IDS/IPS. We are primarily focused on protecting against threats at the networking layer."

Private Tunnel CTO & co-founder James Yonan, who is also the original author of the OpenVPN open source protocol, wrote, "VPNs are about security, not privacy. The sophistication of app and browser tracking has evolved to a point that mostly undermines the privacy benefits of a VPN, and this is a factor in driving our product roadmap to sunset Private Tunnel and move toward next-generation OpenVPN, which is 100% focused on security. Next-Gen OpenVPN is at the epicenter of innovation in our space. We think there are many VPNs in the space today that have taken our core technology and gone heavily on branding and marketing, where security is an afterthought. We have a culture that puts security, innovation, R&D, and transparency first; our marketing reflects that."

ProtonVPN's website states, "Our **anonymous** VPN service **enables Internet without surveillance**." It does qualify this a bit on a different page, pointing out that large companies can track users across multiple sites using cookies or canvas fingerprinting.

"It's absolutely true that some VPN providers don't in fact provide what they promise. We, however, stand fully behind the quality (including security) of ProtonVPN," a spokesperson said, pointing out that the company is open source and subjects itself to audits. "We adhere to a strict no-logs VPN policy, though it's also worth noting that under Swiss law we *can't* be obligated to save connection logs. User security is therefore ensured by a combination of technology, transparency and regulatory environment."

The spokesperson said that while they "can't account for every hypothetical technique that governments may create one day," ProtonVPN "1) is designed and 2) operates in a way to protect folks from surveillance." They pointed to their no-logs policy and encryption, stating that "ProtonVPN puts a huge block between your ISP and you—and ISPs are where governments usually go to surveil citizens." The company also pointed to several strategies it has in place to prevent government spying, including its "Secure Core" that allows users in high-risk countries to route their VPN through the safest countries. "We also intentionally work with vetted third parties to position ourselves outside of risky governments' legal jurisdictions (and unlike many VPN services we are not subject to data sharing agreements like Five Eyes and 14 Eyes). These are strong measures, but if a government successfully finds its way around them, we will shut down operations and leave the country. If we can't live up to our standards, we won't tout things we can't provide."

As far as anonymity, the spokesperson said, "ProtonVPN certainly offers it as long as you're not using the most idealistic version of the term. For instance, using VPN will conceal your real IP

address from websites, ISP, etc. But using VPN won't somehow let you use the internet without *any* IP address (you'll have the address of whatever server you're connected to). Likewise there's a big difference between using VPN once and using it consistently (our settings allow you to have VPN on by default).

"I'd compare it to the concept of having freedom. Does having freedom literally mean you can absolutely do whatever you want, whenever you want, wherever you want? No, and no one actually uses that as their definition of freedom. The same is true with anonymity. There is nothing that can 100% guarantee that online activity won't come with identifiers. But if we're using a serious and practical definition of anonymity, yes, VPN will allow you to conceal things like IP address, browsing history, etc from entities that would otherwise watch you."

ProtonVPN further pointed to its NetShield feature, which does DNS filtering against a database of domains to block malware and allows users to block ads and trackers, and to its full disk encryption infrastructure, its Secure Core, and its no-logs policy.

But the company admits that there are limits to what a VPN can do, and that it can't protect you from malware from email attachments, a device being hacked by software downloaded from a USB, or companies using canvas fingerprinting.

"The best way to summarize it is that VPN is *a* tool for particular issues. Against ISPs, VPNs work very well on their own to prevent surveillance. Against websites, you will want to bring in more tools. A lot also depends on the user's own decisions. VPNs give you *practical* anonymity, but they can't stop you from voluntarily revealing your identity. If you appear on TV with voice distortion and a mask on, those items don't prevent you from still saying your name or announcing your hobbies."

Additionally, VPNs do not prevent users from giving companies their name and search history. "This again is why we recommend pairing VPN with privacy-friendly browsers and doing things like clearing cookies + history regularly. But another factor is policy. The success of a data request depends on the laws in any given country, including what they let the government obtain + obligate the company to do."

Surfshark's website says you can "**prevent tracking**" by enabling the VPN "to **prevent companies, hackers, or bots tracking you online**." It also says it will "protect your privacy"—"Get Surfshark VPN to **protect your online activities** on all the devices you have." And it says "browse privately: encrypt your internet activity so no one can track or steal your data." The description of the VPN on the media page says, "Protect your online identity, **stay private at all times** and access geo-restricted content."

A Surfshark spokesperson said, "Surfshark has always stood true to its advertising statement, so all of the claims you mentioned are substantiated. A VPN technology developed by Surfshark can prevent IP tracking as it changes the user's IP address. This protects the user from tracking based on the geographical location provided by its IP address—a method most often used for tracking by 3rd parties. Although not a universal one, it is a measure of privacy protection. It's

true—there are many ways for companies to track people online, and Surfshark does not protect from all of them. However, Surfshark provides considerable protection from tracking by changing a user's IP address and encrypting its online activities from unsolicited third-party interference. However, if a user logs into some service by providing personal details (for instance, Facebook) and accepts all the website's cookies, Surfshark can do nothing."

Military-Grade Encryption

We looked at the main pages for all of the VPNs that we analyzed. Betternet, CyberGhost, Hotspot Shield, and Kaspersky all used the hyperbolic term "military-grade encryption." (There is no specific VPN standard for "the military," and this term is often a red flag for security professionals.) PIA, too, used the term in the metadata of a page a spokesperson indicated it was in the process of removing.

A spokesperson for Kaspersky says its website states "military-grade 256 bit encryption," which refers to AES-256 encryption. "This standard was established in order to be in compliance with the Federal Information Processing Standards (FIPS) that govern the handling of sensitive data. In 2001, Advanced Encryption Standard (AES) was announced as the new standard for information security by the National Institute of Standards and Technology (NIST), a unit of the US Commerce Department. In an attempt to bring encryption to the masses, security companies started to look for a term that describes the highest-level security with less jargon. As AES is used by the US government to secure classified information and by the NSA to protect national security data, the term 'military-grade' seemed suitable."

ProtonVPN is run by the same company that runs ProtonMail, which was recently called to task for logging the IP address of a French climate activist in response to an order by Swiss authorities. This may not affect its VPN service, which ProtonMail says is treated differently under Swiss law. And ProtonMail's privacy policy and terms of service clearly stated that they can be forced to collect information on accounts belonging to users under Swiss criminal investigation. However, many users felt that web copy (which has since been modified) stating that tracking was off by default was potentially misleading. Users may also have been unaware that there are international legal agreements such as MLATs and the CLOUD Act that allow companies to file legal requests in other countries.

Most Accurate Presentation of VPNs, Their Uses, and Their Underlying Technology

VPNs have a history of potentially misleading ad copy, which appears to be a norm in the industry, but some companies buck the trend by both refraining from overly broad claims and educating users about the limitations of VPNs.

- **IVPN**'s web copy was incredibly accurate and nuanced, using honesty as a differentiator with language such as, "**we don't promise anonymity or 'military grade encryption**'" and pointing out that a fixed encryption standard for militaries doesn't exist, and that

implementations vary across different segments of armed forces. And its descriptions accurately depict what it can and cannot do, such as “What you do online can be tracked by organizations you may not know or trust and become part of a permanent record. **A VPN can’t solve this on its own**, but can prevent your ISP from being able to share or sell your data.” IVPN even has an **ethical guidelines page** on its website, with information on its marketing practices and commitments.

- Mozilla VPN does a great job of educating users about both the benefits and limitations of VPNs, by pointing out that using a VPN “**won’t, however, prevent you from things like clicking on suspicious links, downloading malware, or being victimized by email fraud**. You still need to practice good habits to stay safe online.” “While a VPN provides a secure connection to the internet, it **doesn’t protect you from all bad actors out there**. Any time you’re online, with or without a VPN, you should **be wary of suspicious links, misinformation campaigns, phishing scams and other threats**. Staying safe online is an everyday mindset.” With the exception of a line that says “your online activities stay anonymous because we never log, track, or share your network,” Mozilla VPN provides accurate, nuanced benefits with adequate qualifications, for example, “**browse more anonymously**” rather than anonymously, followed by “Users care immensely about being anonymous when they choose to. A VPN is a key component as it encrypts all your traffic and protects your IP address and location.” It also says “**Communicate more securely**” rather than “communicate securely,” followed by, “Using a VPN can give an added layer of protection, ensuring every conversation you have is encrypted over the network.” Mozilla even posted its easy-to-read Data Privacy Principles.
- Mullvad does an excellent job of describing a VPN as “**a good first step**” toward protecting privacy and pointing out that it’s “**not the ultimate solution**,” and the site also provides information on what to do beyond using a VPN to increase personal security.
- TunnelBear’s web copy stops short of promising people online anonymity and instead uses statements with qualifications such as “your browsing is private, so **you can’t be easily tracked online**.”

Ownership

It’s worth noting that many of these VPNs are owned by the same companies, as previously mentioned. Aura (or Pango, in the U.S.) owns Betternet and Hotspot Shield. Ziff Davis owns IPVanish. (This was formerly J2 Global, which acquired Ziff Davis in 2012 and changed its name to Ziff Davis in 2021.) Kape owns CyberGhost and PIA, and recently acquired ExpressVPN.

Some of these companies have questionable histories.

TunnelBear was acquired by McAfee in 2018—and McAfee has had its own share of controversies prior to the acquisition. Without admitting wrongdoing, the company paid a $50 million penalty in 2006 when the Securities and Exchange Commission filed securities fraud charges saying the company overstated its net revenue, a type of accounting fraud that inflates revenue to investors. And in 2012, the company’s antivirus product turned off its AV protection

and in some cases prevented connection to the internet—and, according to community posts, the company was slow to address the problem.

In the past, ExpressVPN, NordVPN, and Surfshark were not public about their ownership, though they have since released names.

Transparency Reports

When companies disclose their practices for sharing user data with the government and other third parties, along with the number of requests they have received and how they have responded, they can help users understand their policies as well as threats to users' privacy and free expression. CyberGhost, IVPN, Kaspersky, Mozilla VPN, PIA, ProtonVPN, and TunnelBear were the only VPNs that had transparency reports we could easily find.

CyberGhost's report breaks down complaints by type and year. In 2020, it received 117,219 DMCA complaints, 10,707 malicious activity flags, and 50 police requests. Oddly, the company stated that it responds to malicious activity by blocking the attacked IP, making further exploits impossible. That means that users may have difficulty reaching any website that another user has tried to attack.

IVPN's transparency report states that it did not receive any valid legal requests in 2020, and it received a single request in 2021 but did not provide information.

Kaspersky has a transparency report but doesn't distinguish between its VPN and the rest of the company.

Mozilla, too, has a transparency report that doesn't distinguish between its VPN and the rest of the organization.

It's unclear from PIA's website what time period this applies to, but a chart updated in March 2021 listed that it had received two court orders, 12 subpoenas, and three warrants, and was unable to produce logs for any of them.

ProtonVPN says it updates its transparency report whenever there is a notable new legal request but only includes requests coming through official channels, such as court orders, directly from government entities, or from company legal/security departments. The transparency report says the company could not comply with a January 2019 data request from a foreign country that was approved by Swiss courts because it does not have any customer IP information.

TunnelBear's most recent transparency report states that the company received 22 requests for data in 2020, confirmed that one person had an account, and did not share any usage data.

Complaints

In 2017, Hotspot Shield had an FTC complaint filed against it by the Center for Democracy & Technology (CDT). The complaint alleges undisclosed and unclear data sharing and traffic redirection. CDT claimed that Hotspot Shield intercepted and redirected web traffic to partner sites, including those belonging to ad companies, and that it monitors information about user browsing habits and transmits cell carrier data over an unencrypted connection. Hotspot Shield is owned by the same company that owns Betternet. It was formerly called AnchorFree and rebranded to Pango, and was later acquired by Aura. This complaint was filed when the VPN was owned by AnchorFree—and AnchorFree's CEO told ZDNet that he disagreed with the complaint. We are not aware of any Federal Trade Commission investigation having been opened into this matter. The FTC declined to comment on whether it investigated.

VPN-Owned VPN Review Sites

Many publications that review VPNs use affiliate links, which doesn't necessarily mean that these programs affect the reviews. However, there are some instances where companies that own VPNs also run the lists and do not fully disclose that they do so.

For example, Kape (which owns CyberGhost, ExpressVPN, PIA, and ZenMate) owns Webselenese, a marketing firm that runs the VPN review sites SafetyDetectives and vpnMentor.

And Ziff Davis, formerly J2 Global, which owns IPVanish, StrongVPN, and Encrypt.me (which is becoming StrongVPN, according to its landing page), also owns PCMag, IGN, Mashable, ExtremeTech, RetailMeNot, and more. However, it does not appear to be promoting its brands heavily on the sites it owns in the way that Kape does.

Response to Breaches

It's not possible to know with certainty whether VPNs handle or have handled security breaches or other incidents in a transparent way, but we can look at how some VPNs responded. (For example, Windscribe was quick to disclose publicly that it had two unencrypted servers seized in the Ukraine as part of an investigation but that the servers contained no user data.)

NordVPN received flak for failing to immediately disclose a security breach to customers and the public until after a security researcher tweeted about it, 17 months after it took place. In that breach, attackers gained access to one of its servers through a remote management system and stole encryption keys that could be used to mount decryption attacks on some users. NordVPN reportedly stated that it had planned to reveal the breach after internal audits were completed. It also terminated its rental contract with the data center involved in the incident.

Hotspot Shield responded slowly to a vulnerability resulting in the VPN leaking the location of the user's country and the user's WiFi network name, according to ZDNet. It responded by saying that individual users would not have been identified.

Not all responses are negative, however.

After rumors of a backdoor in its antivirus software in 2001, F-Secure Freedome VPN owner F-Secure responded by clearly and publicly stating that it would not leave backdoors in its products, regardless of the source, and would additionally be adding detection to programs that may be used to benefit organized crime or for terrorist activity.

And Mozilla Foundation publishes security advisories for all of its products, including Mozilla VPN.

VPNalyzer Issues

As separate independent research, VPNalyzer tested a total of 80 VPN providers—that also included the 51 VPNs tested for this report—and found several previously unreported issues such as traffic leaks during tunnel failure, and in some cases DNS and other traffic leaking even with the VPN's kill switch feature turned on. It found that a majority of VPN providers and servers do not support IPv6. VPNalyzer identifies that adoption of good security and privacy practices such as doing DNSSEC and RPKI validation, and implementing a DNS proxy, is not uniform across VPN providers. Finally, it also found that malicious and deceptive behaviors by VPN providers such as traffic interception and manipulation are not widespread but are not nonexistent. In total, the VPNalyzer team filed more than 29 responsible disclosures, 19 of which were for VPNs also studied in this report, and is awaiting responses regarding its findings.

Additional Recommendations

Recommendations for Industry Improvement

- VPNs should **distance themselves from employees and partners that engage in human rights abuses.**
- VPNs should **provide accurate information about logging practices and how they would respond to government requests for data**—information that should be both in the terms of service and somewhere more accessible. VPNs should also share regularly updated **transparency reports.**
- VPNs should **present their products and technology accurately,** and not make sweeping or overly broad promises about anonymity, untraceability, or "military-grade" encryption. They should also disclose when they, themselves, are the owners of VPN ratings sites in which they are prominently rated.
- VPNs should **let their users know about any security breaches** as soon as they're able to do so.
- It should be **easy for users to cancel their accounts.**

Best Practices

Our top VPN picks for privacy and security all had open-source code on the client side and reproducible builds, accurately depicted their products and services, and had either a coordinated vulnerability disclosure program or a dedicated contact for reporting vulnerabilities.

IVPN had consistent, ongoing, public third-party audits annually without any misses, which included server-side audits. It also states in writing that it immediately and permanently deletes account information (unless there's a valid and reasonable need to maintain it) within a reasonably short time frame (under 30 days) after service is terminated or inoperable. And it explicitly states that no third parties have any access to user data, and that all first- and third-party tools are hosted on its own servers, gives options, and clearly outlines the information required when using outside parties, such as payment processors.

Mozilla VPN publishes security advisories, explicitly states it won't pursue legal action against security researchers, and has 10 principles it abides by on its website.

Mullvad does not collect data, has authenticated and automatic updates, and explicitly states that outdated or unnecessary information will be deleted or destroyed, with reasonable hard deadlines for destroying or deleting that data.

Recommendations for Top VPNs

Although Mullvad, IVPN, and Mozilla VPN—in that order—rose to the top, there are still improvements that can be made. We'd like to see all three:

- Disclose **how they perform internal security audits** and **what aspects of security are audited**, and **publish summaries of these reports** for users.
- Provide **details on how and when the software is updated** for security issues.
- Describe **technical measures in place to limit unauthorized access** to data.
- Provide a **hard deadline of product support/life,** with a clearly and intentionally defined support period.
- Set a **time frame to review vulnerability disclosures** and bug reports.

We'd like to see IVPN **authenticate its updates with a signature**. And we'd like to see it describe in more detail the **systems in place to monitor employee access to user data**. Additionally, IVPN has information only on how to **obtain access to the data the company holds** under GDPR, and could make this available for all users, regardless of jurisdiction. We'd also like to see IVPN explicitly state in its ToS or privacy policy that it will not pursue legal action against security researchers.

We'd like to see Mozilla VPN **authenticate its updates with a signature**. We'd also like to see it improve its lockout policy to meet our **brute force mitigation** checks. Mozilla could **autoupdate its VPN** as well. We're interested in clear and detailed descriptions of what's included in the public and private data it holds that users can obtain, or provide sufficient detail on the types and pieces of personal or aggregate information it collects from third parties.

Mozilla also did not describe the ways it will use consumer information provided with consent outside of its privacy policy. Lastly, we'd like to see Mozilla **separate its transparency report by product** so that it's clear which requests for data were specific to VPN users.

Mullvad collects incredibly little user information, but we'd still like to see an **annual transparency report** disclosing how many user requests for data the company receives and how many it complies with.

We'd also like to see both IVPN and Mullvad explicitly state in their ToS or privacy policy that they will **not pursue legal action** against security researchers.

Recommendations for Users

Of the 16 VPNs we analyzed, Mullvad, PIA, IVPN, and Mozilla VPN (which runs on Mullvad's servers)—in that order—were among the highest ranked in both privacy and security. However, PIA has never had a public third-party security audit. Additionally, in our opinion, only IVPN, Mozilla VPN, and Mullvad—along with one other VPN (TunnelBear)—accurately represent their services and technology without any broad, sweeping, or potentially misleading statements.