		[answers as of Oct. 17, 2018]	[answers as of Oct. 17, 2018]	[answers as of Oct. 17, 2018]	[answers as of Oct. 17, 2018]	[answers as of Oct. 17, 2018]
	CDT's Things to Look For	**ExpressVPN**	**IVPN**	**Mullvad**	**TunnelBear**	**VyprVPN**
Date Responses Reviewed		**Oct. 17, 2018**	**Oct. 17, 2018**	**Oct. 17, 2018**	**Oct. 17, 2018**	**Oct. 17, 2018**
CORPORATE ACCOUNTABILITY & BUSINESS MODEL						
What is the public facing and full legal name of the VPN service and any parent or holding companies? *Do these entities have ownership or economic stakes in in other VPN services, and if so, do they share user information? Where are they incorporated? Is there any other company or partner directly involved in operating the VPN service, and if so, what is its full legal name?*	*For commercial privacy and security tools, reputation matters. VPNs should be clear about not just the individuals in charge of running and securing a VPN, but ultimately, who owns the company. The more information that a VPN can make available here, the better. If the VPN's public brand name is different from its legal name, users should know this.* *This should include both the brand and incorporated names of company, specific individuals who are responsible for operating the company and maintaining security, and whether the VPN is part of a larger company.*	ExpressVPN is operated by Express VPN International Limited, a privately held British Virgin Islands company. ExpressVPN's leadership team and owners are not involved in any other VPN company/brand or any business other than ExpressVPN. While the company, its infrastructure, and its agreements with users all fall under BVI jurisdiction, ExpressVPN's team is physically distributed across more than a dozen cities worldwide. In many cases we contract with local entities or subsidiaries to provide payroll services for staff that ExpressVPN hires. Our core functions like engineering, network operations, marketing, and customer service are performed by full-time, dedicated employees who work solely on ExpressVPN.	The public facing name is IVPN. The legal name of the company is Privatus Limited. Privatus Limited has no parent or holding companies. There are no other companies or partners directly involved in operating the IVPN service.	The public-facing name is Mullvad VPN. The legal name of the company is Amagicom AB which is directly owned by the founders Fredrik Strömberg and Daniel Berntsson. Amagicom AB is incorporated in Sweden. Neither Amagicom AB nor Fredrik Strömberg nor Daniel Berntsson has ownership or economic stakes in other VPN services. No other companies are directly involved in operating Mullvad VPN.	TunnelBear's team and offices are based in Toronto, Canada while the corporation, TunnelBear LLC, is incorporated in Delaware, USA. TunnelBear is wholly owned by McAfee. McAfee is a well known security software company, with both consumer and enterprise products. While McAfee owns TunnelBear, TunnelBear operates independently with no TunnelBear customer information shared with McAfee.	Golden Frog, GmbH is the full legal name of the company that offers VyprVPN. You can have more details about our team and company's ownership on our About Us page. We do not have economic stakes in other VPN providers and thus do not share any user information with any other VPN service. Golden Frog GmbH is incorporated in Switzerland and we store all of our customer data in Switzerland. Switzerland's favorable privacy laws reflect our mission as a company and respect the rights of Internet users. To our knowledge, we are the only VPN provider in the world that 100% owns and operates its server and network infrastructure, including our zero-knowledge DNS service. We do not rely on third party hosting companies for servers or network services and therefore are not vulnerable to their privacy policies or security practices.
Does the company, or other companies involved in the operation or ownership of the service, have any ownership in VPN review websites?	*One of the major issues with VPN reviews across the internet is that are many incentives for VPN providers to "game" the system. VPN providers should not be reviewing themselves.*	No, neither Express VPN International Limited nor any related companies own a VPN review website.	No.	No.	No. TunnelBear offers an affiliate program where we pay commissions to websites who send us customers. We require these affiliates to disclose their financial relationship with TunnelBear. TunnelBear does not own or operate any review or affiliate websites.	No. Our company does not have ownership nor operate any VPN review websites.
What is the service's business model (i.e., how does the VPN make money)? *For example, is the sole source of the service's revenue from consumer subscriptions?*	*A VPN should be upfront about how it makes money and any incentives that aren't aligned with user's privacy and security interests. If all or more of the VPN's revenue comes from customer subscriptions, that suggests a VPN's users are its actual customers rather than its product. We would note that as VPNs provide "white label" services, such as offering their technology to other companies, and diversify their businesses by offering other security tools or technologies, this should also be disclosed.*	ExpressVPN's sole source of revenue is from consumer VPN subscriptions. We never sell user information or utilize the information that customers provide to us for any purpose other than operating the VPN service.	All revenue comes from VPN customer subscriptions.	All revenue comes from VPN customer subscriptions.	The paid version of TunnelBear solely and exclusively generates revenue from subscriptions. The free version of TunnelBear serves as a marketing tool to permit individuals to try TunnelBear; TunnelBear does not profit from free users by selling bandwidth, usage habits, or use them as a botnet. TunnelBear has plans to offer an SDK which would allow select partners to resell a white labeled VPN service.	We do not sell user data to generate revenue. Our sole source of revenue comes from VyprVPN consumer and business subscriptions.
PRIVACY: Logging/Data Collection Practices and Responding to Law Enforcement						
Does the service store any data or metadata generated during a VPN session (from connection to disconnection) after the session is terminated? *If so what data?*	*A responsible VPN is very up front about what it means by logging and what data it retains over time, even if it is aggregated or anonymous. This should be at the top of any privacy policy or terms of service. It should be separately disclosed and easily discoverable via the VPN's website or app.*	ExpressVPN's apps and servers are engineered to categorically eliminate sensitive information. We do collect limited metadata to aid technical troubleshooting and service improvements, which are: operating systems and app versions successfully activated; dates (not times) when connected to the VPN service; choice of VPN server location (no IP addresses are ever stored); total amount (in MB) of data transferred per day. None of the above data enable ExpressVPN or anyone else to match an individual to specific network activity or behavior. Optionally, users may also opt to share anonymized analytics data such as speed test data, connection failures, and crash reports. These diagnostic reports do not tie back to individual users because we've engineered our apps to never know which user sends which data. For details, please see our Privacy Policy.	No.	No. For details, see our privacy policy (https://www.mullvad.net/en/guides/no-logging-data-policy/).	No. TunnelBear is proud to not store any data surrounding the times and IP addresses when people use TunnelBear. We do collect the aggregate amount of data you use in a given month. This data usage is not session specific, aggregated over the month and deleted once a new month starts. At TunnelBear, we spend a lot of time thinking about how to reduce the data that we're collecting and share the process with our customers. Since 2014, our privacy policy has documented every piece of data that we collect both through our service and more recently, on our website. Having a comprehensive policy has meant that every decision we make has to consider the privacy impact. Whether it's designing features like our map to not store your IP address, setting up marketing tools to respect privacy or even creating our own privacy focused social media buttons, we try to consider privacy in every decision we make. Most recently, in preparation for the GDPR, TunnelBear launched a tool which allows customers to see exactly what information we store.	Each time a user connects to VyprVPN, we retain the following data for 30 days: • The user's source IP address • The VyprVPN IP address used by the user • Connection start and stop time • Total number of bytes used. Nothing more.
Does your company store (or share with others) any user browsing and/or network activity data, including DNS lookups and records of domain names and websites visited?	*This question further addresses the need for VPNs to be clear about how they treat data that could conceivably fit into the definition of "usage" or "activity" logs. VPNs should not maintain this information.*	No, ExpressVPN never logs any user browsing or network activity data, and we go to great lengths to ensure such information never even hits a disk on any server. We run our own private, zero-knowledge DNS on every VPN server. And of course, as we do not possess any such activity data, we do not (and cannot) share it.	No.	No. For details, see our privacy policy (https://www.mullvad.net/en/guides/no-logging-data-policy/).	No. We do not collect connection times, IP addresses, DNS requests, browsing data, or anything else that could be directly linked with an account. TunnelBear has an easy to read privacy policy that outlines what data we collect and how we use it. In it, we explain that we log no customer activity.	We do not store or share any browsing, network activity data, or DNS lookups. We own and operate our own server and network infrastructure , including our zero-knowledge DNS service, so we can ensure that user data is not shared with any third party. This is part of our commitment to providing the highest level of user privacy.
Do you have a clear process for responding to legitimate requests for data from law enforcement and courts?	*A VPN's physical location and the national law it operates under can afford users different privacy protections and does dictate how a VPN might respond to a government request for data. CDT recommends that VPNs, at minimum, provide transparency reports about how often they receive court orders and other government requests and have a clear process in place for responding to any requests for data.*	Our first principle is that we never store any data that could match an individual to specific network activity or behavior. Thus, our process is to inform law enforcement that we do not possess logs of connections or user behavior that could associate a specific end user with an infringing IP address, timestamp, or destination. Not storing any sensitive information also protects user privacy and security in the event of law enforcement gaining physical access to servers. This was proven in a high-profile case in Turkey in which law enforcement seized a VPN server leased by ExpressVPN but could not find any server logs that would enable investigators to link activity to a user or even determine which users, or whether a specific user, were connected at a given time. ExpressVPN is based in the British Virgin Islands, a jurisdiction with strong privacy legislation and no data retention requirements. Legally our company is only bound to respect subpoenas and court orders when they originate from the British Virgin Islands government or are made in conjunction with BVI authorities. The British Virgin Islands only upholds foreign governments' requests for information when the crime under investigation would be punishable by at least a one-year prison sentence under BVI law (dual criminality provision).	Yes, please see 'Law Enforcement Legal Process Guidelines' - https://www.ivpn.net/legal-process-guidelines and Transparency report – https://www.ivpn.net/transparency-report	Yes, see our article "How we handle government requests for user data" (https://mullvad.net/en/guides/how-we-handle-government-requests-user-data/).	Over the past 7 years, more than 25 million people have connected to TunnelBear. By design, we don't know much about who these people are or how they've used our service. We've done this on purpose, as we see it as crucial to operating a VPN service. When TunnelBear receives a request from governmental authorities, law enforcement agencies or in connection with a legal proceeding, the request is reviewed by our legal counsel to ensure that the request is valid and to determine the appropriate nature and scope of our response. At TunnelBear, we believe that the best way to protect our customer's privacy is simply to not store data that puts your privacy at risk. If we're required to respond to a request, you can see the exact data that we might be required to provide by downloading a copy of your data from TunnelBear's privacy center.	Yes. All legal requests are directed to Golden Frog GmbH's legal team. Golden Frog GmbH is a Swiss corportation and because all customer data is stored in Switzerland, we are legally prevented from directly answering any foreign (non-Swiss) legal requests. We will only respond to a valid legal order from the relevant Swiss law enforcement agency acting on its own or at the request of a foreign law enforcement agency using the proper Mutual Legal Assistance Treaty with its legal jurisdiction.
SECURITY PROTOCOLS & PROTECTIONS						

	CDT's Things to Look For	ExpressVPN	IVPN	Mullvad	TunnelBear	VyprVPN
Date Responses Reviewed		Oct. 17, 2018	Oct. 17, 2018	Oct. 17, 2018	Oct. 17, 2018	Oct. 17, 2018
What do you do to protect against unauthorized access to customer data flows over the VPN?	*It is very difficult for an individual to assess the security practices of a VPN. While perfect privacy and security does not exist, VPN users can expect trustworthy VPNs to use up-to-date protocols and software/hardware hardening.* *Several practices CDT thinks are important to look out for include practices and policies around software updating ("patching"), vulnerability handing (which includes "bug bounties" as well as process for addressing flaws), and any discussion of technical, administrative, and even physical security.*	ExpressVPN takes the following approach to ensuring the security of our systems and customers: • Make systems very difficult to compromise. • Minimize the potential damage if a system were to be compromised. • Minimize the amount of time that a system can remain compromised. • Validate these points with regular penetration tests, both internal and external. Specifically for our VPN servers, here are some examples of measures we employ: Being difficult to compromise: 1. Fast patching, made possible through automatic provisioning and deployment. 2. Hardened OS and applications 3. Training of employees 4. Requiring multi-factor authentication, including YubiKey physical touches for commits and SSH access 5. Hardening workstations, i.e. protecting devices used by employees by eliminating risks and threats 6. Using bastion boxes for SSH access, which channel information between the internet and the internal network through a high-security intermediary 7. Strong security settings for the VPN: i. Secrets generated on the server itself ii. Weak authentication protocols are disabled iii. Strong encryption and hashes iv. Perfect forward security to ensure that compromised or stolen encryption keys do not affect the security of past or future communications (learn more here: https://www.expressvpn.com/blog/perfect-forward-secrecy/) v. Clients strongly authenticate servers: clients expect both a signature from our CA, as well as a specific common-name for a given server; we can revoke server certificates in less than an hour (learn more here: https://www.expressvpn.com/blog/secure-expressvpn-server-connections/) 8. Code audits i. Requiring code reviews for all changes ii. Github scanning for known vulnerabilities in dependencies iii. External scanning for known vulnerabilities iv. Static analysis tools running with every commit as part of our Continuous Integration process. v. Audits by external security penetration testers 9. Physical security of the team and infrastructure. Minimizing the potential damage stemming from a compromised server: 1. Encrypted filesystem 2. Services running with least privilege possible 3. Authentication credentials are strongly hashed Limiting the length of time that a system can remained compromised: 1. Notice hacks early: Intrusion detection, including integrity checks at boot 2. Read-only disk image running in RAM only, doesn't use disk, which means neither data nor access by hackers can persist 3. Frequent rebuilds of the OS to ensure servers are regularly patched and preventing attackers from having persistence (learn more here: https://www.expressvpn.com/blog/how-expressvpn-keeps-its-web-servers-patched-and-secure/) 4. Frequent reboots: since we boot into a read-only image with integrity checks, a reboot will clear most attempts at persistence In general, security is ingrained in our culture. ExpressVPN's reputation and long-term business success depend on protecting our customers. We believe we are both properly incentivized as well as capable of doing this well. We maintain a library of content detailing various other measures for other parts of our service such as our website, API servers, and customer support team. For more information, please visit our Trust Center: https://www.expressvpn.com/trust	If an adversary gains physical access to a server it is prudent to assume that they will gain access to the unencrypted data stored on the server. As VPN servers are not under the direct physical control of IVPN they have been designed with the expectation that they will be compromised. To protect the privacy of IVPN customers the following controls are implemented: • No logs relating to the customer connection or network activity generated by an IVPN user are created or stored. This includes not creating any temporary or in-memory logs. • No storage of information relating to an IVPN user's account i.e. authentication credentials are not stored locally. • 24/7 monitoring of all servers to alert IVPN of any suspicious activity or if a server is taken offline. If a server is offline and there no evidence from the data center that it is a hardware fault then procedures are followed to revoke the certificates on the server to prevent a potential MITM attack. Administrative controls: • Implementation of an Information Security Management System (ISMS) based on ISO 27001. • Background screening of all employees. • Mandatory information security training. • Vetting of data centers where servers are hosted. • Patch management policy to ensure consistent and rapid resolution of vulnerabilities. • VPN servers do not store any logs relating to the customer connection or network activity generated by the customer. VPN gateways do not store any information relating to a user's account e.g. authentication credentials. Technical controls: • Enforcement of 2FA for system access. • Access control using a private VPN with RSA 4096 certificates for authentication. • Mandatory Access Controls (SELinux). • Firewalled IPMI. • Full disk encryption (LUKS) requiring password entry at boot. • Configuration management software to enforce consistent configuration and security controls based on CIS Benchmarks. • 24/7 systems monitoring and alerting of suspicious system activity using host-based integrity protection. Customer connections: • Customer VPN connections are secured using OpenVPN with RSA-4096 / AES-256-GCM keys. • Full mesh multi-hop network – IVPN customers can choose to connect to any location in the IVPN infrastructure and have their VPN traffic exit in any other location. To enable this functionality, secure VPN tunnels are established between every server in the IVPN network. This makes it significantly more difficult for an adversary to gain access to a server as the servers would be in multiple jurisdictions. In addition, should the exit server be compromised the adversary would not be able to trace an IVPN customer's connection other than to the entry VPN server.	Secure systems are required for privacy, and since Mullvad's beginning, security has always been deeply ingrained in our culture. • In our app we offer such security features as a kill switch, DNS leak protection, and IPv6 support, all of which we were either first or among the first. • We only utilize the two best VPN protocols, OpenVPN and WireGuard (we were an early adopter of the former and we pioneered the latter). • Because reliability is paramount, our app is built in Rust, a programming language made for building secure programs. • We use code signing for app and server code. • All of our sysadmins use the Qubes operating system, as does most of our team. • We also protect our laptops against tampering.	Protecting our customers data and preventing unauthorized access is our highest priority. We employ an extensive list of processes, techniques and services. Our infrastructure and client apps have undergone extensive hardening, testing and the VPN industry's only independent public security audit. TunnelBear hardens every server with full disk encryption, malware and intrusion scans and intrusion protection techniques. Security patches are up to date. Hardware 2FA is extensively applied throughout our organization. SDLC methodology is followed with all development and is architecturally reviewed, peer-reviewed, tested and independently audited on an annual basis - the results are available for the public to see.	Our approach is unique in the VPN industry; we fully own, engineer, and manage our VPN servers and network. Therefore, we are the only company that handles VyprVPN users data and we can guarantee higher levels of protection and security from end-to-end. Unlike competitors, we don't use any 3rd-party companies to host our servers and we have 24/7 monitoring for unauthorized changes or physical access to all servers and networks.
What other controls does the service use to protect user data?		We work to empower customers to protect their privacy and security in every aspect of what we do. In addition to those we've mentioned in previous answers, some other ways we do this include: • Open-source leak testing tools, aimed at enabling reviewers and other third parties to independently verify leakproofing claims, providing insight into what our engineers work on to protect users, and raising the bar for the entire VPN industry. • Acceptance of Bitcoin as payment for those seeking to increase their anonymity. • Comprehensive and transparent Privacy Policy explaining how we treat sensitive data, what we store and never store, and why. • Transparency and disclosure to users when things go wrong and we accidentally ship bugs in our software, through blog posts and other communications. • Bug bounty program for any potential security vulnerabilities and privacy leaks. • Extensive guides to general privacy and security matters on our website, including primers on tech safety for survivors of domestic violence, securing your mobile device, protecting your financial privacy, and more. • Contributions to the VPN community, including helping to fund the Open Source Technology Improvement Fund's (OSTIF's) independent security audit of OpenVPN. • Public advocacy for digital rights, including sponsoring and working with organizations such as OpenMedia (who we recently joined up with to develop a Message-Your-MEP tool) and the EFF.	• IVPN accepts anonymous payments using cash since 2010. Customers are also able to pay anonymously using Bitcoin if they are able to source Bitcoins anonymously. • All VPN servers are built using Open Source software e.g. CentOS, OpenVPN, StrongSWAN etc. • Vulnerability disclosure process at https://www.ivpn.net/vulnerability-reporting • Warrant canary - https://www.ivpn.net/resources/canary.txt • IVPN is a transparent organisation with information about staff published on https://www.ivpn.net/aboutus and Linkedin. • In-depth privacy guides for IVPN customers - https://www.ivpn.net/privacy-guides	We offer a number of features to protect our users' privacy, including these industry firsts: • We accept payment with cash in the mail and Bitcoin. • In our account sign-up process, we ask for no personal information whatsoever, not even an email address. • Our VPN app is open source (find an independent audit report of it on our website). We are also contributors to the privacy and security communities at large. When we discovered that OpenVPN was vulnerable to Heartbleed and later Shellshock, our warning to the community benefited many other VPN services who took action based on our advice. In addition, we are the only VPN service to currently offer VPN tunnels with experimental post-quantum security.	TunnelBear is proud to be the first and only VPN provider in the world that has released a public, full infrastructure security audit from a verified third party. We have hosted bug bounties, accept honey and Bitcoin as alternative payment options for privacy conscious customers, and continue to have annual full audits of our system, apps and code.	Any site-to-site transfers of customer metadata is via encrypted channels only. We store no credit card or other immediately abusable payment information for any of our customers. (We utilize well known, industry standard, payment processors to protect this information.) We utilize multiple protocols for encryption which include a NAT firewall for all connections. Additionally, we have a Kill Switch feature which automatically blocks your internet connection whenever VyprVPN is disconnected. Additionally and perhaps most importantly, we are constantly investing in our talent to ensure that they are experts in their fields and prepared for any potential challenge. We truly work to guarantee our customers are getting the best, most secure service available.

CENTER FOR DEMOCRACY & TECHNOLOGY