CHOOSING A VPN

That One Privacy Guy's – Guide to Choosing the Best VPN (for you)

*Disclaimer: The below guide is my opinion, which I will try to provide as many examples for and as much evidence as possible to support. I reference my VPN Comparison Chart throughout much of this post, not so much for shameless self promotion, but because I believe it to be a solid resource to determine if a VPN meets your criteria and to assist you in deciding which is best for you. Much of this guide is relevant and therefore repeated in the other guides I have on That One Privacy Site. If you just want an ELI5, read the **bolded** segments throughout the guide for the highlights. If you want to go down the rabbit hole on this topic, read on, and buckle up – this is going to be long.*

TABLE OF CONTENTS

I. INTRODUCTION:

The following is intended to be a detailed guide to answer the question, "How do I choose the best VPN (for me)?" The reason this is a hard thing to help people with, is that their needs and level of technical knowledge vary greatly – there is no one perfect VPN, they all have at least some flaws and some will just flat out be better for different people.

I very well might have forgotten to add a section I intended to, said something that needs clarification, or was just sleepy when I wrote parts of this guide, so I intend to update and expand it as needed.

I'm assuming that if you're reading this far, you have at least SOME knowledge as to the basics of what a VPN is, so I won't cover that here. This will be heavily emphasizing the need of a VPN for privacy, but I will echo and expand on other use cases as well towards the end.

II. A WORD ABOUT TRUST

No matter what reason you want a VPN, you want to know that the service you choose is trustworthy and is not compromising your data. Even if you're only concerned with geo-unblocking or other non-privacy uses, keep reading. I'll get more into this in the

"Privacy" section, but it's important for everyone to be exposed to it at least a little.

A preface regarding privacy and trust, from a Reddit thread I made a while back. This applies to every company, but I would suggest especially so for VPNs.

> *We live in a society where privacy is undervalued and under assault daily. Some people eventually notice this and discover that they do value their own. They set out on a pilgrimage of sorts to educate themselves and learn about tools to help them protect it (as I did when I started my project). Because we depend on each other for direction and others to write software and run services to help keep us secure – TRUST AND TRANSPARENCY – are paramount.*
>
> *However, transparency comes before trust.*

III. A WORD ABOUT VPN AFFILIATES

You may have started your search for a VPN by looking for "VPN Reviews" in your search engine of choice. if you had, you would have gotten page upon page of what seem to be harmless review sites, top 10 or blog style reviews of different VPN services. You may even be coming here for confirmation of what you were told on those sites. The sites making these recommendations are, in *almost every* case, paid by the services they review and recommend. They are beginning their business relationship with you, with what essentially amounts to **a lie**. The technical term for this kind of marketing is "native advertising" and it's abuse is a huge problem in the VPN industry.

I purposefully made a point to capture this kind of data on my VPN Comparison Chart. There you can find information on services that have affiliate programs, the specific policies they have for them and whether or not the affiliates act ethically, essentially what the services tolerate from those representing them, when it comes to persuading YOU to buy into the information they put out.

Note that not all affiliates *have* to be bad actors and simply *having* an affiliate program is not necessarily grounds for mistrust of a VPN, but rather when those services allow their resellers to generate referrals by hook or by crook. If you see a service appear over and over again on the kinds of sites mentioned above, there is a good chance they are making money from, and are perfectly okay with these kinds of deceptive practices as a part of their business model. They often will claim that it's just the affiliate doing this, and that they can't control what others do. This is false. Affiliates, like anyone entering into a business relationship with someone, agree to certain terms put forth by the service hiring them. If a company doesn't **expect** and **enforce** certain standards from their affiliates (not spamming, not breaking copyright, disclosing who they are, etc), they are approving these methods, and are not worthy of your trust. If they are willing to lie to you before you even buy into their service, the stage is set for them to be dishonest with you when you interact with them on a normal basis as a customer.

IV. IF YOU'RE CONCERNED WITH PRIVACY

- **a. More on Trust**

As a lawyer represents your legal interests, a VPN service (among others) represents your privacy interests. If a lawyer does something to violate your trust or is not honest about some aspect of their representation that could affect you, you would discard them and you'd be right to do so. Likewise with a VPN service. There are many out there that are not worth your time or money. Unlike a lawyer, a VPN can be put together and promoted by anyone with access to a computer, the key difference being that you would never even see their face.

If you are looking for a VPN for privacy purposes, you already believe you cannot trust certain parties. Those parties might be companies whose websites you visit or maybe even an oppressive government whose mass surveillance is encroaching on your rights. You are being put in a position where you must rely on someone other than yourself for protection and the last thing you need is one more party that you can't trust.

This decision is an important one, and not just any VPN service is worthy of that trust. You're trusting them to know what they're doing – to be able to operate a competent service that will protect your privacy. You are trusting them to be responsive to new technical and geopolitical threats to their operation. You're trusting them to be honest with you in the way they do business so that when you are shopping and comparing, you are getting accurate information.

- **b. More on Affiliates**

In the main section at the beginning of this guide, I talked about affiliate practices, so I will only briefly mention it here. **If you choose a company with an affiliate program, choose one that expects and enforces good behavior from their reselling partners.** You can usually read their affiliate terms on their site. If they are not publicly visible, they should respond with this information when asked. If not, or if they play games with you, look elsewhere. More information on affiliate policies and behavior can be found on my VPN Comparison Chart.

- **c. Jurisdiction**

In the last few years, certain revelations have been made manifest regarding the mass surveillance programs of various countries around the globe. These countries are known as the five, nine, and fourteen eyes. These countries not only spy on their own citizens where they can get away with it, but they spy on each others, and swap notes to bypass governmental restrictions on power. If a service, or the people who run a service is based in one of these countries, it's not unreasonable to expect that they may be susceptible to unlawful searches and compromises made in the name of national security. That said, if your threat model includes protection from such actions, choosing a company incorporated outside of these jurisdictions probably would not be adequate to protect you – as such actors have vast resources, and if singled out, you would need to worry about more than your VPN (by relying on other tools such as Tor, Tails, paying very close attention to your opsec, etc). **Where the servers you're connecting to and the people who operate / have control of them are located are more important than where a company is incorporated, to protect yourself from government overreach**

Other countries are not part of the spy collaboration mentioned above, but still have issues with government limitations on internet freedom and free speech. **Avoid countries with limited internet freedom**. The degree of internet freedom a country has can also be found under "jurisdiction" on my sheet.

- **d. Logging**

When you connect to a VPN service, you are essentially just adding one more stop along your route to the open internet. The VPN is a "man in the middle" who you are trusting with the traffic and connection data that is being generated in the background as you use the internet. Some VPN companies choose to log this data. There are many reasons for doing so, some more legitimate than others. Some services record this to protect themselves legally in the case they are approached by authorities. Some companies keep minimal connection logs to aid them in maintaining servers. Some will even sell your data to third parties as part of their business model. If your concern is privacy, you most likely do not want your browsing habits and connection data being recorded. **Choose a service that specifically states that they do not keep logs, AND which types they do not keep. Make sure they do not keep ANY kind of activity or connection log** Many services claim to not keep logs, but are vague, and upon closer inspection actually do keep certain types, so be wary of such promises until you've confirmed it for yourself in their respective terms and privacy policies.

- **e. Payments and Communication**

Assuming privacy is your priority, when you go to pay for your VPN service, there are many methods available, but only a few worth consideration. **Services that offer the ability to pay by Crypto Currency, cash, or misc gift cards are the best way to ensure that you are kept as anonymous as possible**. if these services require more personal information than an email address, look the other direction – this is information they're recording about you that may be used at best to sell to third parties, at worst to later identify you.

Some services offer a PGP key for additional privacy. This is a nice thing to have if you want to be able to communicate with them using encryption.

- **f. Protocols**

There are many different kinds of VPN protocols that allow you to establish a tunnel with your service provider – some more secure than others. Certain protocols are documented to have been compromised. Others are free and open source, and as such are freely available for security experts to audit and improve. The free availability of the source code helps to ensure that vulnerabilities are patched quickly and that individuals so inclined can see exactly how their software is working. **Choose a VPN that supports OpenVPN and use it to connect to your VPN server. Avoid using other protocols, specifically PPTP** as its not suited for privacy.

- **g. DNS and IPv6 Leaks**

Throughout the course of using the internet, your computer sends and receives a lot of data that isn't visible to you, the user. When you type in a web address, a request is sent to a server that is usually operated by your ISP. When you connect to the internet using a VPN, this responsibility is now on them. If they don't take certain actions, this request containing info for the site your want to visit is being sent to THEIR ISP instead. This may not be as bad as it going through yours, but as I mentioned logging above – if the company in question even keeps certain logs, there is a chance that the sites you try to visit can be correlated with the timestamps of when such a request is sent. As an alternative, some use public DNS servers, such as google's, which is not ideal for privacy. **Choose a VPN service that maintains their own first party DNS server that won't leak – then TEST IT TO MAKE SURE**.

When using the internet, you connect to IP addresses. Traditionally, IPv4 is used to accomplish this (you may have seen numbers in the past like 8.8.8.8 or 216.58.217.206, etc). There is another standard that will some day be more prevalent, called IPv6, but that is being used now during the time it transitions into normal configurations (vastly more IPv6 numbers exist than IPv4). When you connect and use the internet (unless you have specifically taken steps to disable it), you are sending and receiving IPv6 data. Again, normally, this data is sent and resolved through your ISP and their DNS servers, but unless properly configured, this information might not be securely passing through the VPN tunnel and could be leaking to the open internet. Given such routed global IPv6 addresses, it's easy for remote sites to identify user ISPs. And with requisite authority, account information could be obtained from those ISPs. **Choose a VPN service that either blocks or provides new VPN-specific IPv6 address and provides an IPv6 DNS server that's reachable only through the VPN tunnel – then TEST IT TO MAKE SURE**.

- **h. Encryption and other Features**

Around 1440 AD, the Printing Press was invented. It created a method for the common person to quickly disperse information, technologically reinforcing the natural right to freely speak and share information. More recently the internet allows billions to freely and openly share ideas and advance humanity. This reaffirmed the common person's rights in such a way that was difficult for governments or organizations to stifle. Similarly, until the invention of firearms, only those physically capable could defend themselves from those that wished to encroach on their rights, thus this technological advancement reinforced the individual's right to self defense. This brings us to Computerized Encryption. As with the other technological advancements mentioned above, Encryption provides a simple-to-use method that the average user can take advantage of to reinforce their right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.

Choose a VPN service that has strong data and handshake encryption. Make sure the protocol you choose has the level of advertised encryption available to it, as services typically provide more than one protocol with varying levels of encryption strength. The VPN Comparison Chart can help you determine what is considered strong by the color coding on these fields. Be sure that even if the service has the type of encryption you want available BY DEFAULT – some services will technically offer strong encryption, but it has to be manually configured (not user friendly).

Optionally, depending on your use case and threat model, **you may be interested in making sure Authenticated SMTP (to send email) and P2P (to file share, download, use Bitcoin, etc) are not blocked on your VPN's servers**

- **i. Websites and your Privacy**

When you start to search for services and are browsing on their websites, there are some additional items you may want to consider. Speaking of trust and privacy – some companies will use tracking cookies to determine how to best serve you ads, which other sites you've been to, and some will even phone home with specific personal information. Best case, this is an abuse of power by companies stretching the limits of their ideas on how to gather this info, worst case, it can be used to intentionally violate your privacy and tie your device back to the site and activity performed on it. **Choose a company that respects your privacy enough to use few if any persistent or external tracking cookies**. If they are already violating your privacy the moment you visit their site, you have no assurance that they will take your privacy seriously after hiring them to represent your interests. Available for years, https allows websites to entirely encrypt all data sent and received with the user, effectively blocking out those that might try spying on such web traffic. **Choose a service that encrypts their website with an SSL Certificate**. Additionally, CloudFlare, Incapsula, and similar services have recently become popular with websites for their DDoS protection and dynamic bandwidth scaling. However, these services act as an additional man in the middle between your VPN's website and you. In the wrong hands, the information they collect and have access to about your VPN's website, and your interaction with it, could be compromised. **Avoid VPNs that use CloudFlare, Incapsula, and other such services**.

V. IF YOU'RE CONCERNED WITH SECURITY

Many of the points made above are relevant to security as well as privacy, and I will point some out below.

Jurisdiction, specifically Enemies of the Internet are important to be aware of, to ensure an environment where laws are enforced and physical security that we take for granted in some parts of the world are applicable to the servers we communicate with. This also helps indicate that our service and the servers we connect to are located in places that respect internet freedom. This information can be found on the Comparison Chart and confirmed on Reporters Without Borders' Website.

IPv6 should be specifically tunnelled or blocked outright the same as with the privacy scenario above.

First party DNS servers, as mentioned above, are ideal for preventing leaks of your data.

Both data and handshake encryption should be strong and available for the protocol you choose (which again, should not be PPTP). Other protocols are probably secure enough for daily use. Note that no protocol is bulletproof and exploits probably exist and are discoverable for each and every one of them. Such exploits are even more discoverable by governments with vast amounts of resources.

VI. IF YOU'RE CONCERNED WITH UN-GEOBLOCKING

If your only concern is escaping geoblocks, your needs are far less numerous. Being able to connect to an exit node in the country of your choice is really the only requirement. This doesn't mean necessarily however that you want to neglect the proper security measures discussed above, only that for things like Netflix, Hulu, certain TV online channels and sporting events, they are less important **if un-geoblocking is ALL you're trying to do, almost anything will work, HOWEVER – if Privacy and Security are of any concern whatsoever, heed the advice above and know that un-geoblocking will virtually always come naturally when shopping for those needs** (as long as required server availability is a feature of your chosen VPN)

VII. IF YOU'RE CONCERNED WITH BYPASSING RESTRICTIVE NETWORKS

Some parts of the world are resisting the ever-growing ability for their citizens to freely share information and as such have implemented roadblocks in their networking infrastructure to cripple such communication. For example, the "Great Firewall of China" has several layers of VPN detection and blocking built into it. Other networks belonging to large corporations or maybe even your Internet Service Provider may restrict you from using certain ports, limiting what you can use the internet for. However, there are ways to get around these restrictions by using the right VPN.

Features such as multihop, TCP port 443, Obfsproxy, SOCKS, SSL tunnels, SSH tunnels, and some other proprietary solutions (which may be built specifically by a given VPN company) can be useful in avoiding these restrictions. As for which are most effective, it's a matter of which restriction is being inflicted upon the user. Speak with your VPN service's support team to determine which might be effective in your case. The VPN Comparison Chart shows which services support which of these protocols and features in their configuration. Using TCP port 443 is usually a relatively common and user-friendly measure to bypass a restrictive/oppressive network.

VIII. CLEARING UP MISCONCEPTIONS

Kill switches – Many VPN services offer in their client a feature called a "Kill switch". The idea with a Kill Switch is that when the VPN loses its connection, it completely prevents the device from using internet, thus preventing accidental leaks of local connection data. Kill Switches are implemented very differently and will never be secure due to their design. The only 100% effective and secure configuration to accomplish prevention of leaks is a properly configured firewall. There are two main types of kill switches, those that shut down preconfigured apps in response to detecting the VPN connection has dropped and those that disable the network connection (or delete routes etc) if they detect a disconnection. In both of these cases the Kill Switch component is having to react to an event and very often leads to leaks – just a single packet is all it takes to compromise your privacy. The only way to be absolutely certain that packets cannot leak is for there to be an independent component (the Firewall) that blocks all packets unless destined for the VPN interface.

Warrant Canaries – Some VPN services maintain a document called a "Warrant Canary". This is a document put out and updated by them certifying that they have not been contacted by government agencies or coerced to compromise their user's data. In theory, if such an event occurred forcing them to compromise their principles, they would stop updating the canary, which in turn would indicate to users that their data is no longer private. Note that not all companies use effective warrant canaries. There is some debate as to the effectiveness of a warrant canary between experts to begin with – as force can be used by governments to coerce companies into maintaining them, thus nullifying their effectiveness. They are *usually* nothing more than marketing theater. If a company WAS operating a good canary, it would be almost impossible to tell. A warrant canary is almost a better feature to care about once you've found a trustworthy, capable service, rather than looking for a company that has one when shopping around.

I hope that this guide has been useful. Feel free to ask me if you have any questions – as usual you can contact me on using the contact info on the "contact" page of the site.

Written by That One Privacy Guy
If you like the project and find my work useful, please consider donating – your generous contributions help pay for the hosting, tools, and time I need to do my research and keep the data fresh.