# GUIDE

## Privacy Matters

Greetings all.
Today I intend to append a new series to my mini-collection of posts. This series will consist of informative guides for the purpose of depicting certain aspects of the White Hat profession that I believe are of profound importance. Furthermore, I will keep this series simple for everyone to follow, regardless of your tech level. So without further ado, let's get right into it.

In today's guide I will be talking about privacy, the fundamental right of every human, and the controversy around it. I will also be fully divulging the ways in which you could implement security measures in order to strengthen your privacy. Privacy, privacy, privacy. Let us begin.

**Prelude**

It is evident that, despite the increasing concerns over one's reclusion and freedom of expression, there are entities which seek to restrain people for attempting to fight for those very rights. That, of course, points to the fact that subsequently not everyone is in control of their liberties. Most certainly the internet is a setting, one of its kind, that allows higher forces to more easily impose restrictive laws to obstruct people's entitlements. Today I aim to help everyone with this scenario by advising measures to prevent the disclosure of personal information and to let private data stay private.

(Enough of my verbal diarrhea •_•)

## VPN

A VPN is a Virtual Private Network which, when used, routes your entire internet traffic through the provider's server(s) in an encrypted form before reaching its final destination. Sounds safe, doesn't it? Not so fast. When it comes to VPN, it is painstakingly obvious that trusting a company with absolutely all of your data is foolish. Here I outline some points to think about before choosing a provider.

1 Privacy Policy

As lengthy as it seems, you should always read the T&C and PP pages before making a deal. If they mention anything there that may seem off-putting or not to your appeal, disregard the choice. This is for your own protection, since that is what you're here for in the first place.

2 Warrant Canary

It can also be referred to as a Transparency document. This may be a page, or a notice on the website, stating that there have not been any official requests for user data, and that none have been turned over. If the page goes blank, missing, or something indicates that it isn't functioning, it means user data has been requested and most probably handed over to the authorities. This system is used to avoid the company getting in trouble but, at the same time, letting users know that something is up.

3 Own Servers

A big question at hand is whether the VPN provider runs their own servers, their own DNS and their own infrastructure. If they don't then they are owned by a parent company who, if required, will have access to all logs and user data it needs in case there is an issue or an investigation. If they do, that is good news because they are independent and whatever they claim on their website is more likely to be true since they are not affected by any entities (apart from the government of the country they reside in).

4 Location

This is probably one of the most important points to outline. Wherever a VPN provider is situated, make sure it does not have any physical ties to any members of the Five Eyes, that being the US, UK, Australia, Canada and New Zealand. By having ties to any of these countries, the VPN company

straight away loses its powers to protect you. This is a golden rule that needs no explanation.

5 Price

Alright, I think this one is pretty clear. If a VPN is free, don't take it. Remember that for a free service, if you are the customer then you are the product. This is because by offering you a 'free' service the VPN company still needs to make some money. The only way they can do that is by implementing ads and by selling whatever data they can squeeze out of you. They will do this through forms, surveys, and data usage they collect through their VPN app. Thus, you have lost all of your privacy when that's all you came for in the first place. So don't take up free VPNs. If you want extra anonymity, see if the provider allows payment using Bitcoin because that's your golden ticket.

## Proxy

A proxy is a server that acts as an intermediary for any protocol-specific requests from one machine to another. There really isn't much up for discussion here. We all know proxies are not the safest, not the most reliable and definitely not the fastest means of connectivity... but they save you when you most need saving. They can make traffic seem totally anonymous and are a quick and easy alternative for when VPNs don't work. But don't rely on them saving you from the NSA or GCHQ (Britain's equivalent). Whoever is running those proxies are fully aware what you're doing with the service. Even if you're using an SSL-protected proxy, they can still perform a live inspection on the traffic. The one thing you could try is pick proxies from countries where they will not, by any means, give up user data simply because they don't care about threats. Such countries include Russia, China, Romania, and several others that you can dig up on the internet.

## Public Hotspots

This isn't something covered in many places, but I believe it is imperative that it needs to be mentioned. When you're out and about, and you're at a

coffee shop or something, you will most likely use the free Wi-Fi that is usually available these days. If you ever decide you need protection, you already have one complimentary layer set up for you, just by being in a café. However, this will only work if one of the other measures are implemented (e.g. VPN) and that will strengthen your protection.

Using a public hotspot means that, since you are not at your home network, you will not be seen as a domestic target by attackers. So that means that, if someone decides to monitor your connection, all they will see is a random stranger at Starbucks (an example) and they will not know their target, thus you have just been dismissed. Great news, now how about authorities?

This doesn't really change the situation with the authorities, as their power extends in all directions. An FBI official could literally just walk into Starbucks and ask for all the Wi-Fi logs and he (or she) would be handed them instantly. So your only protection from the government remains a VPN or a proxy, which will deter anyone from looking in the place of origin of the traffic. But is that all there is?

## TOR and I2P

These two words you may have heard of. The first one is much more known, but I think the second one is worth including. Sure, they aren't your fastest means of 'proxying' but they are by far your safest bet. What I find miraculous is that people are still getting caught doing terrible things when using these services. I'm not saying this to discourage you from using them, I'm telling you this because it's something to be aware of.

The problem when people get caught over TOR is poor self discipline. If you wish to do something online, and you don't want anybody to know of it, TOR is not enough. You also need to stop bragging you did it, stop bragging under your name! Drawing attention to yourself, using your real name and frivolous acts like these will most certainly cast doom onto you.
Why did I mention TOR though? Oh yes, right, use the TOR browser (connected to the network, of course) and that will send your traffic through 3 relays before reaching your target. What I like the most is that

those 3 relays are different for each website you visit. Now that's some auto-proxychains-power safety right there if you ask me.

A similar story goes for I2P, except it doesn't relay your traffic through 3 mediums, but it does encrypt your traffic end to end and it does have base32 addresses (if you use the network) that are incredibly difficult to decrypt, so much as realistically impossible. Either way, these are your alternative methods of achieving total privacy if you seek it.

## Email

This may not seem very important but it is. Email is fundamentally flawed, and judging by how we use it and how much we rely on it, it poses a huge risk to our privacy. So what is the solution here. Well, there's one solution and that is to use a privacy oriented service. No silly, not Gmail or Yahoo but something like Startmail, Tutanota, Riseup, or ProtonMail (yes, I know all about the hack). However to use them you'll need to spare a bit of money, it's not free you know (except Riseup, that is absolutely free of charge).

So there you have it, a way to save the day.

## Operating System

If you're looking for a private way to browse, a private way to open files, and a private way to do pretty much everything, you need a privacy-oriented OS that will do half of the work for you. You have a few choices here, the more obvious ones notably being Tails, Whonix, and then there's JonDonym.

Tails OS isn't very difficult to get used to. All you need is a USB stick with 2 GB of space and you are set. What's great is that all of your internet traffic is already redirected through TOR and you are able to set up I2P in just the same way.

Whonix works best as a Virtual Machine so I suggest you keep it as such. It isolates programs into workstations so that if you get a virus that tries to mess with you, it will stay in the workstation it arrived, and it will never move.

There is very little to say about JonDonym because it is little known, but I can say that it is a great Tails OS alternative as it functions in a similar fashion. I think it is a great (and a greatly underrated) alternative for Tails and I've enjoyed testing it and using it for privacy purposes. So yes, it is a recommendation, along with the other two.

## Behaviour

There are plenty of discussions out there on this topic, but I feel like I have to mention it as it goes well along with everything I've already talked about.

Firstly, I cannot stress enough how important it is that you never talk about yourself if you're seeking privacy and/or anonymity. Practise self discipline, make sure you understand that whatever you type on the internet stays there. So think twice before doing anything that may reveal who you are.

Secondly, it is your responsibility to deal with arising threats. If you feel you are being tracked, followed, monitored, whatever, then immediately stop what you are doing. Take a break for 10-15 minutes, meanwhile cleaning all cookies and cache, then return, maybe even on a new browser. Be thoughtful, improvise, make wise decisions that you think will get you to safety.

Remember one thing on the internet: safety first. This is the motto and it doesn't change. Your safety is more important that whatever it is you are doing. So if you feel threatened, cut loose immediately and stay loose until the appropriate time. You shouldn't hesitate to protect yourself, even for a mere second. In a future tutorial I will demonstrate how to set up a ‘trip wire' that securely erases your entire hard drive in case you are physically approached. I'm sure this will prove useful with this privacy Guide.

**Links and Downloads**

- TOR
- I2P
- A great read
- StartMail
- Tutanota
- Riseup
- ProtonMail
- Tails
- Whonix
- JonDonym

## Conclusion

I think I've covered most of what needed covering on this topic. There you have it, ways to keep your privacy intact and your mind open. I hope you've learned from this and that you will use this knowledge wisely. If you feel I've missed something, ask in the comments for me to add it and I will try my best.

This series of Guides will be branching out in all sorts of directions so bear with me, as this is just the beginning. I hope you all enjoyed this one, have a great day, and I have a tutorial coming up pretty soon so stay tuned. As always, leave any suggestions for future guides in the comments.

Have a great day, peace.
TRT