Don't use VPN services.

No, seriously, don't. You're probably reading this because you've asked what VPN service to use, and this is the answer.

Note: The content in this post does not apply to using VPN for their intended purpose; that is, as a virtual private (internal) network. It only applies to using it as a glorified proxy, which is what every third-party "VPN provider" does.

(A Russian translation of this article can be found here, contributed by Timur Demin.)

Why not?

Because a VPN in this sense is just a glorified proxy. The VPN provider can see all your traffic, and do with it what they want - including logging.

But my provider doesn't log!

There is no way for you to verify that, and of course this is what a malicious VPN provider would claim as well. In short: the only safe assumption is that *every* VPN provider logs.

And remember that it is in a VPN provider's best interest to log their users - it lets them deflect blame to the customer, if they ever were to get into legal trouble. The $10/month that you're paying for your VPN service doesn't even pay for the lawyer's *coffee*, so expect them to hand you over.

But a provider would lose business if they did that!

I'll believe that when HideMyAss goes out of business. They gave up their users years ago, and this was widely publicized. The reality is that most of their customers will either not care or not even be aware of it.

But I pay anonymously, using Bitcoin/PaysafeCard/Cash/drugs!

Doesn't matter. You're still connecting to their service from your own IP, and they can log that.

But I want more security!

VPNs don't provide security. They are just a glorified proxy.

But I want more privacy!

VPNs don't provide privacy, with a few exceptions (detailed below). They are just a proxy. If somebody wants to tap your connection, they can still do so - they just have to do so at a different point (ie. when your traffic leaves the VPN server).

But I want more encryption!

Use SSL/TLS and HTTPS (for centralized services), or end-to-end encryption (for social or P2P applications). VPNs can't magically encrypt your traffic - it's simply not technically possible. If the endpoint expects plaintext, there is *nothing* you can do about that.

When using a VPN, the *only* encrypted part of the connection is from you to the VPN provider. From the VPN provider onwards, it is the same as it would have been without a VPN. And remember, **the VPN provider can see and mess with all your traffic.**

But I want to confuse trackers by sharing an IP address!

Your IP address is a largely irrelevant metric in modern tracking systems. Marketers have gotten wise to these kind of tactics, and combined with increased adoption of CGNAT and an ever-increasing amount of devices per household, it just isn't a reliable data point anymore.

Marketers will almost always use some kind of other metric to identify and distinguish you. That can be anything from a useragent to a fingerprinting profile. A VPN cannot prevent this.

So when should I use a VPN?

There are roughly two usecases where you might want to use a VPN:

1. You are on a known-hostile network (eg. a public airport WiFi access point, or an ISP that is known to use MITM), and you want to work around that.
2. You want to hide your IP from a very specific set of non-government-sanctioned adversaries - for example, circumventing a ban in a chatroom or preventing anti-piracy scareletters.

In the second case, you'd probably just want a regular proxy *specifically* for that traffic - sending *all* of your traffic over a VPN provider (like is the default with almost every VPN client) will still result in the provider being able to snoop on and mess with your traffic.

However, in practice, **just don't use a VPN provider at all, even for these cases.**

So, then... what?

If you absolutely need a VPN, and you understand what its limitations are, purchase a VPS and set up your own. I will not recommend any specific providers (diversity is good!), but there are plenty of cheap ones to be found on LowEndBox.

But how is that any better than a VPN service?

A VPN provider *specifically seeks out* those who are looking for privacy, and who may thus have interesting traffic. Statistically speaking, it is more likely that a VPN provider will be malicious or a honeypot, than that an arbitrary generic VPS provider will be.

So why do VPN services exist? Surely they must serve some purpose?

Because it's easy money. You just set up OpenVPN on a few servers, and essentially start reselling bandwidth with a markup. You can make every promise in the world, because nobody can verify them. You don't even have to know what you're doing, because again, nobody can verify what you say. It is 100% snake-oil.

So yes, VPN services do serve a purpose - it's just one that benefits the provider, not you.