VPNS 101 with Charly Leetham

Episode 3: How to Choose Your VPN Wisely

Welcome to VPNs 101 episode three with me, Charly Leetham. Today we're going to talk about how to choose your VPN wisely. We are going to take the stuff that I spoke about in the last episode and dig down a little further into it.

Paid vs Free VPNs

The first thing we're going to talk about is paid versus free. There are going to be people out there saying, "Oh, this one's free. You should just use it. It's fine. It works for me. Yeah, and it's free. You don't have to pay for it."

I think what I want to say here is that you are either the customer or you are the product. If you pay for something, you are generally the customer. There are no absolutes, so please don't come at me about this one. I'm not talking in absolutes. I'm going to be talking in generalities here. When you're paying for something, you are the customer. When you are taking something for free, you are generally the product.

Why do I say that? Particularly with VPNs, let's just look at VPNs in general. VPNs cost money to run. You have the hardware that they run on, you have the bandwidth that they use (the bandwidth is your stuff coming in). You've got to be able to take the stuff that you've got coming in and the requests that you've got coming in. They've got to terminate it on the hardware and then they've got to send that through and send that out into the internet as well. So the bandwidth that they use is a lot of bandwidth. There's the hardware that it runs on, and then you've got all the applications that run on that hardware to make the VPN service run. You've got the maintenance on it, you've got the security considerations on it. You've got all of the IT security policies, processes, and procedures that go into making sure that that service is secure.

Someone has to pay for that somewhere along the line. It is the rare person that will say, "No, I'm just going to run this absolutely altruistically, and I'm not going to take a cent for it, and I'm not going to get my money back somewhere." Somebody has to be paid for some way.

So if you aren't paying for the service, someone else has to be paying for the service. That is typically done - and I've got my notes here, so if I'm looking to the side, please bear with me - that is typically done because they are selling your data or your personally identifiable information so that you get marketing back at you, people trying to sell you stuff. You end up on all these lists: CEOs in the tech industry, or CEOs in the beauty industry, or you're a hairdresser, so you're starting to get stuff targeted at you

because you're a hairdresser.

They'll sell your data. And it's not just data they can sell. They can also sell your browsing history. They can also sell what you're doing through that VPN. If they aren't reputable, they can be selling that information as well. So just be careful.

They may also inject ads into your stream. So if you can imagine you're sitting there, you're working, then all of a sudden an ad pops up while you're working and you can't get rid of it. It might be coming through the VPN service. They might be injecting it into the data stream while you're using it. That would really annoy me, by the way.

Another thing they might do is they might cap your speed. Like I said, bandwidth costs money. Speed costs money. To reduce their cost, to manage their cost, they might actually say, "Well, we've got this big pipe, but what we're going to do is we're just going to oversubscribe it." And then as more and more people come on, they're going to drop the speed, and it's being dropped and it's being dropped, and eventually it becomes unusable because it's so slow. It's like going back to dial-up modem days, basically.

So that's what you've got to consider when you're looking at paid versus free. Where is the money coming from if you're not paying for it? How are they paying for that service? How are they maintaining that service? How are they ensuring that your security and your privacy is maintained?

Jurisdiction Matters

Jurisdiction is the next thing. Take the little eyes that I have on this map as a grain of salt. Please don't worry about where the reds and the greens are. It is just an indication that there are some surveillance agreements between governments across the world. And this is saying that we need to understand when we're looking at where our VPN provider is actually headquartered or based.

When we're talking about surveillance agreements across the world, we're talking about governments that share intelligence. And yes, I am looking at my notes here. Sharing intelligence, including data on their citizens. Some of these surveillance agreements (and I am no expert, so there is a really huge caveat here - I'm no expert on these agreements) - I know enough to be careful around where we do things and how things are done and to ensure that I actually do follow the laws in the countries that I'm in.

They can legally compel companies to hand over user data. So if they've got an ongoing investigation and they need to get stuff, they have got laws in place in the countries where they can go to companies and say, "Give us that data."

We are seeing a lot of that in the news now. Some companies are saying, "No, that's not what you're entitled to. And if you need to get it, we're going to have to go to court so that you can get access to it," because the companies themselves have got to make sure that they're maintaining their own privacy things and that they're following the privacy laws, and they're not in breach of the privacy laws because

the government comes in and says, "Give us that information."

So they can compel organizations to hand over user data. They can also put gag orders in place to stop those organizations telling you that your data has been handed over.

I'm not saying that they do this. I'm saying that the laws are there. They may possibly allow that to occur. I'm being very careful to caveat this because it's such a huge part of the law. It's such a huge morass of laws that all sort of interact together. And one person will look at it and interpret it one way, and another person will look at it and interpret it the other way. And that's why often it ends up in court trying to work out which part of the law, which interpretation of the law is actually correct. That's what I'm trying to say there.

The Five, Nine, and Fourteen Eyes Alliances

But let's look at the alliances that exist. There are three alliances that I am aware of:

The Five Eyes Alliance - This is the core group, and that is United States, United Kingdom, Australia, Canada, and New Zealand. They all share data.

That's been expanded out into **The Nine Eyes Alliance**, which is those base five plus Denmark, France, Netherlands, and Norway.

And then there is **The Fourteen Eyes Alliance**, which includes the base nine plus Germany, Italy, Spain, Sweden, and Belgium.

If your VPN is based in any of these countries, if they're headquartered in any of these countries, they will be subject to the laws of that country. They will be subject to what data they are legally required to hand over on request of the government, on request of the authorities (not just the government, on request of the authorities).

So just be aware of that when you are looking at that.

Privacy-Respecting Jurisdictions

There are some countries that aren't included in these alliances. They have declined to become part of these Eyes alliances. They are better at respecting privacy. We call them privacy-respecting jurisdictions. We are looking at countries like Panama, Switzerland, Romania, and the British Virgin Islands.

Now these are probably the four countries that, if you're looking for a VPN provider, see if they're headquartered there. See if their main base is in one of those four countries. You probably - you are more likely to have something that won't be able to hand over your data. They can say, "No, this is outside of

our legislation. You can't get access to that data."

So just consider that when you're looking at where to take a VPN.

Now what do those four countries do? It's not just that they don't hand over data. They're not required to log data. Some of these countries that I was talking about, they require everyone to log the data. It doesn't matter what you do. It's got to be logged and it's got to be kept for three or five years or something.

They don't cooperate with the global surveillance treaties. They have stronger privacy protection laws in general.

So don't just check the features of your VPN. Check the country where it's registered. Check where a company is actually registered.

So that's your jurisdiction. That's the thing. That's probably the first thing you should be looking at before you even start looking at features. Is it in a country that respects privacy and keeps our data private?

Must-Have Features

Now let's talk about the features. These are the must-haves.

No Logs

What do we mean by no logs? I spoke about that in the last episode. No logs means no records of the websites you visited, the IP address you're using, the downloads, the timestamps, any of those sorts of things. They do not log what you're doing once you've logged into the system. There is no logging about where you're going, what you're looking at, any of that sort of information.

There is probably a record of when you have logged in, and that's probably the only thing. Now, I don't mind that there is a record of when I've logged in because I can see if my account's been compromised, basically. So make sure there's no other logging feature.

The thing to remember here is don't just take their word that they don't log. We have certainly seen within the industry providers saying, "No, we don't log," and then we found the logs. They're logging and they're selling that data. There are disreputable companies out there all the way through.

So just bear that in mind. You shouldn't just take their word for it. You need to go and look at independent reviews. You need to also see if they've got independent audits from reputable companies, from reputable auditors to say, "Yes, we have audited their processes. Yes, we can guarantee (big rubber stamp) that

there are no logs being kept."

Most of the providers that I will be suggesting have gone through a lot of that auditing process.

Kill Switch

A kill switch is not that you can just turn it off really quickly and go on your merry way. A kill switch actually protects you if the connection between your PC, your device, and your VPN provider drops.

So occasionally, you know, things happen on the internet and you lose communication with a site. It might be a glitch. It might take a couple of minutes to recover. It might take an hour or so to recover. Maybe something breaks and it stops you being able to get into your VPN. Maybe it's down for maintenance (very rare). Maybe they start maintenance and you can't get on, or you're using it and they take it down for maintenance and your connection stops.

Rather than the connection just stopping and the software going, "Oh, well, we can't get a connection to the VPN, so we're just going to funnel all of your traffic out into the internet without going through the VPN. So we're going to expose your IP address. We're going to expose your data to the big bad world," the kill switch goes, "There is no connection to the VPN. I'm shutting your internet down. I'm turning it off until you tell me what to do."

That's going to protect you from exposure of your real IP address, any DNS leaks, and of course it's going to protect your sensitive data. You're not going to be communicating with a public Wi-Fi system, for example, and have your data out there in the digital space where people can look at it and try and hack into it.

The benefit with the kill switch, of course, is that if you decide that you want to take the risk - "Yeah, I can't get onto my VPN at the moment, I'm just going to drop the VPN and just go out there" - you get to make that decision. It doesn't make the decision for you. It protects you.

Split Tunneling

Split tunneling is cool. I have had trouble with this in the past with some providers. Some providers do it really well. With split tunneling, you can choose which apps use the VPN and which don't.

What do we mean by that? Well, it means that I might be sitting here with my VPN up. I might be tunneling to a US server for whatever reason. Maybe I'm working with a US company and I've got to use the VPN to get into their system. They require me to have a US IP address. And then I decide that I need to go do my banking. I need to go to Australia and get to an Australian site and do my banking. It says, "No, you're not in Australia. We're not going to let you in." I'm a person in Australia, but it looks like I'm in

the US because I've got a US IP address, and it says, "No, we're not going to let you in."

So I can set up split tunneling to say, "Right, when I access this site, don't use the VPN. Just use my network directly so that it looks like I'm in Australia."

If you want to use things like Netflix and stuff, which has VPN detection on it, and it says, "No, you can't connect to us because you're using a VPN and that's against our rules," you can actually set it up so that when you get to Netflix or you use your Netflix app on your phone, it doesn't use the VPN.

So split tunneling is really, really good so that you can have as much protection as you possibly can and still be productive without having to turn on and off your VPN all the time.

Multi-Device Support

Being able to use your VPN across multiple devices simultaneously is the fourth thing to consider. It is no use getting a VPN that you can only use on your PC, or you can only use on your phone, or your tablet, or even just your TV.

It's really important that you are able to use your VPN across all of your devices. You need to be protected. It's pointless, you know - if you're protected on your PC but you're not on your phone, you're opening yourself up to all sorts of things.

So make sure you can use the service that you've got across multiple devices simultaneously, not just one at a time. Not "You can only use it on your computer, and if you're not using it on a computer, you can use it on your phone." I've got my phone and my computer sitting here. I want to be able to have them both running because I use them for different things. I have my phone sitting here doing something at the moment - it's running my notes - and I want to have that protected by my VPN whilst my PC is protected by my VPN.

So we've got to make sure that you've got the multi-device support.

Support and Usability

The final thing to consider is your support and your usability. Make sure that you've got apps that run on your phone. Make sure that it's easy to install on your PC or your Apple device, or your Apple desktop.

There are some providers that also allow you to run it on your TV, on your Apple TV, or on your Android TV, your smart TVs. You can actually put the client on there and protect your TV as well, so your TV can be using the VPN as well.

Make sure that the apps are simple to use, that there's something available for every device, that you

don't have to do a whole song and dance to do it. You know, stand on your left foot, put your hand in the air, stick your tongue out, those sorts of things to get your apps running.

24/7 support is probably also something you should be looking for. A lot of these companies are headquartered not in Australia. Well, all of these companies are headquartered not in Australia. And our daytime is typically not their daytime. So we want to make sure that you've got support available 24/7. And in this day and age, I'd say you'd want live chat.

I have thoughts on whether you want an AI chat or not. You really probably need to have - I feel that being able to have a live chat with a real human in the long run is the goal of all of this. Yes, AI, but if you're still having trouble, you need to be able to speak to someone to get them to help you.

And finally - I say finally, whatever - make sure there are guides available. Make sure that you can go to their website, you can download a PDF if need be, have it sitting on your device, and if you're trying to set things up, you can actually look at it and go, "Yeah, that makes sense."

So support is the other one that isn't on this slide.

Free Trials and Refunds

Free trials and refunds are the other thing to consider when you're looking at getting a VPN. So these look good on paper. The question is, will they actually do the job and will they do the job for you in a sufficient and adequate fashion?

You can do all of the paper audits. The proof is in the pudding. You need to be able to make sure that this works. Free trials and/or money-back guarantees - refund, money-back guarantee - are probably things that you want to consider.

Can I download this? Give it a try, even if it's just for seven days. Can I test this out? Can I test all the functionality or 90% or 80% of the functionality of this offering and see if it meets my needs?

If you can't get a free trial - let me just finish that thought - do I need to put my credit card details in to be able to get that free trial? Or can I get the free trial, and if it expires, that's on me, and I can then go back and put in my credit card and purchase it?

That's my preference, by the way. I don't like giving my credit card out to get these things. I prefer to do my testing and then make a decision as to whether I want to give out my credit card details. Totally up to you. That's the sorts of things I look for.

If I can't do that, what's the money-back guarantee on this? What is the refund policy on this? If it really doesn't meet my needs once I've got onto the internet and I've run it for a couple of days or a couple of

weeks, what are my options? If it really doesn't meet my needs, can I get my money back on it? There are lots of things you should be considering there.

Summary

So in summary, today we've spoken about paid versus free. I think I have beaten the drum on that sufficiently now, so hopefully it makes sense to you.

Considering the jurisdiction that your VPN provider is headquartered in is really important for your privacy concerns and making sure that your privacy concerns are met.

What features you need to consider when you're looking at a VPN - what I consider the must-haves - and what support is available. And finally, what your trial options are, whether there's free trials and refunds.

Next Episode

Moving on to the next episode, I'm actually going to be talking about some of the ones that are out there and things that they do and don't do, and trying to give you some ideas of where you might want to go look for a VPN to use.

Connect With Me

If you guys want to know a little bit more about me, if you want to get in touch with me, if you've got questions that you want to ask, you can connect with me in any of these locations. You can follow me there. I would really appreciate the likes and follows - it really does help.

You can also join my community at AskCharlyLeetham.locals.com and have conversations there. If you scan that QR code, it will take you to a page on my website which has all of this information that you can just click on.

https://askcharlyleetham.com/connect-with-me