Spoke Media.

KELLY: Hey Bob.

BOB: Hey Kelly.

KELLY: So it's that time again. Can you guess?

BOB: I bet we're doing a mini-sode.

KELLY: Yes! We're doing a mini-sode. There the listeners' opportunity to have any and all of their burning tech questions answered.

Okay, so here's today's question.

DAVID: Hello, I'm David from Quebec. So Bob, VPNs. Do they actually protect our privacy and security like they all claim? I understand how they work in a technical sense, but in real world applications, do they do what they say? Thank you very much, and have a good day.

KELLY: Bob, I hear about this so much. Like, every time I talk about technology with people, they seem to bring up VPNs in some way, and I still don't have a clear idea of how they work. Do you?

BOB: I do. And I have a clear notion about whether or not they're worth it, and we'll hear all about it after the break.

[AD BREAK]

Spoke Media.

KELLY: So Bob, VPNs. What are they? How do they work? Give me the skinny.

BOB: Sure. So VPNs, virtual private network. They've been around for a long time, but you're hearing about them more and more now because, for good reason, people care more about their privacy now. The short version about what a VPN is, is it creates a virtual tunnel between your computer and the computer that you're talking to across the Internet. So somewhere along the line, you have the idea that when bits and bytes fly out of your laptop through the air, to your ISP, across some backbone cables, and then eventually to the other server and back again, that people snooping along the way might be able to see that data. A virtual private network creates what's essentially a wrapper around your information so that someone who tried to do that couldn't. So it blocks people from seeing that information. So that's how virtual private networks work, and theoretically, they can protect you. But there's a whole bunch of caveats to this, and I think the short version of the story is for most people it's

probably not worth it. If you are the kind of person who really needs a VPN, you work for a company or a government organization that provides you with one that's specially formulated for your computer, for your company or the computers you need to connect to. So you don't need to learn about VPNs from this podcast. But for the rest of the public, there are different kinds of VPNs. There are free ones, there are paid ones. As a general rule, if you really care about this, pay for it. Free always means that you're just the product. So, I wouldn't trust a free VPN. VPNs can cost 5 or 10 dollars a month, and that might be worth it to you for the added level of security. However, for starters, the real reason that VPNs started to actually get attention was back when, uh, the federal government changed rules on how data can be shared and essentially ruled that ISPs were allowed to share your information to marketing companies. So companies like Comcast for example, can now trade on your data. Now it's supposed to be anonymized, but that freaked a lot of people out. And so they said, I don't trust my ISP, I want a VPN. So that's good. If you get a VPN, Comcast can't see your data. However, you're just routing it all through this other company, and now you're shifting the risk from your ISP to your VPN. Maybe you trust the VPN provider more than you trust your internet service provider, but I'm not exactly sure why you would. Um, you might believe in them. Maybe you have some personal information about why they're more trustworthy. Maybe you've seen them, uh, resist a subpoena from the FBI in a way that you don't think that Comcast might resist a subpoena from the FBI, but ultimately, legitimate corporations that take your money and have a bank account can't resist a subpoena from the FBI. So there's really no guarantee that the VPN isn't ultimately going to cough up your information to the US law enforcement agency or some other international law enforcement agency. So, it's a matter of shifting the risk. There's a bunch of other caveats too. Using a VPN will pretty much always slow you down, because you're routing all your traffic through this third party and the robustness of your network relies on how big their network is. So it's just another opportunity for something to go wrong or to slow you down while you're using the Internet. And if you're streaming, we all know how frustrating it is when streams die. Speaking of streaming, a lot of companies will not allow you to use a VPN. Like Netflix. So one of the things that VPNs do is they disguise your IP address. So Netflix doesn't know where you're coming from, and the way the Netflix video rights work, people who live in the US see different films that people who live in the UK, then live in Europe or whatnot. Netflix has to keep track of that. And as a result, if they see that you're using a VPN, they cut you off. Now there's a bit of an arms race in that game because there are new VPNs popping up all the time, and for a while, they get around Netflix's barrier. Netflix finds out about them and they cut you off. And it's not just Netflix by the way. So, Major League Baseball and the NHL and all these sports networks, they also need to know where you are so they can follow a blackout rules. And VPNs can't be used for any of those either. So VPNs can actually limit the content that you can access.

KELLY: Okay. This is just a funny story. Um, the only experience I've had with VPNs is when I was in high school and AP scores came out. Everyone was so excited to see them, or anxious to see them, and people were like, well, you can use a VPN so you can get your score earlier because it'll mask your IP address so they don't know where you're from.

Because people in Texas would get it at a different time than people in New York. It was ridiculous. But I think that seems like a similar thing. It's--

BOB: Yeah. So VPNs can be used to mask your IP address, and, and there are the tools that are illegal or semi-legal to mask your IP address for that purpose. As, as a way of evading a filter, you can use them. But again, there's also lists of VPNs that these companies use to check against this. So that's not a good long-term strategy. One of the things that VPNs have going for them is a lot of people work in coworking spaces now. If you work at a coffee shop or if you work at one of those coworking spaces, maybe you don't trust their wifi networks so much, and you want to use a VPN just to protect you from the people sitting around you. And that's not a bad idea. I can see the rationale for that. But, but just to give you an idea of how it works and doesn't work, you know when you go to, and there's that little lock in the address bar, which means there's an HTTPS instead of an HTTP? So, what that indicates is that all of the web browsing traffic between you and the computer you're going to is also encrypted. So that data is also protected. So the VPN is, is sort of a meaningless added layer in some ways for web traffic, but it's going to protect you when you look at email or do any other kind of internet connection. So people are kind of familiar with this notion that, like, is the traffic between my computer and the computer I'm talking to protected or not? So VPNs add this added layer, but they have all these caveats. And so, my opinion is for most people it's not worth it. This is one of the reasons that you haven't seen like a brand name VPN that everybody can name pop up. Uh, good news on that front. Firefox is about to introduce a VPN service that consumers can at least dabble with and try to use. So I think we might see some competitors in that space. But I ultimately, what I suggest is like good internet hygiene, if you're really concerned about security. Like, not reusing passwords or using a password manager, not clicking on emails, being really vigilant about that kind of stuff, is way more important than using a VPN.

KELLY: So this is a little broader than just VPNs, but you brought up something that I maybe embarrassingly don't know a ton about either, is when I'm in a Starbucks or any other coffee shop and I'm using their wifi, I'm not super informed as to why that might be a bad idea ‘cause I don't really know what can happen when I'm using Starbucks’ wifi.

BOB: Yeah. And in fact I've, I've done experiments with hackers where they just sit next to you and they can sniff what you're typing out of the air. So there's no reason that you should presume that data that leaves your computer, flies through the air to the Starbucks router, is safe. It's not safe. Somebody could just sit next to you and sniff those packets out of the air with pretty rudimentary technologies. Now as with all of these situations, I advocate people taking sensible risks and avoiding terrible risks. So you can go to a Starbucks and sit down and kind of look around, and the thing about this kind of piracy, this man in the middle attack they call it, requires someone to be there physically, like, within a few feet, within a few dozen, maybe a hundred feet of your computer to pick your data out of the air. So if you look around and you know the four people near you, odds are low that this is going to happen. It doesn't happen as often as some computer security experts seem to suggest that it happens. But I never do something like online banking or something really critical, some kind of really, really critical

email. And if I had serious company secrets, I would never use public wifi for that kind of thing. But you are taking your digital life in your own hands by randomly connecting to wifi hotspots. So you have to decide how important your information is at that point. Like, I'm not going to tell you not to use public wifi, because the truth is not that many people get injured by it. But it does happen, and it's not really that difficult to happen. And if you ever wanted to do an episode on hijacking someone's wifi, I know just the people to ask.

KELLY: [laughs] Maybe I'll take you up on that. Um, okay. So, for re-answering David's question, what's the TL;DR on VPNs, Bob?

BOB: If you are really curious and don't mind spending $10 a month to see what a VPN is like and how it works for you, then be my guest. There is not a VPN I can recommend right now. And I think for the vast majority of internet users, their focus is better spent on doing other things to keep their internet hygiene safe, like better passwords and better security habits. So for most people, I don't think they should spend money on VPNs.

KELLY: Yeah, that makes total sense. Thanks Bob for answering and thanks to David in Quebec for asking.

If you have any questions about your digital life, write to us or send us a voice memo at sobob@spokemedia.io or tag us on Twitter @SoBobPod. Who knows, you may be featured on our next mini-sode.

So Bob is a Spoke Media production.

It's hosted by Alia Tavakolian and Bob Sullivan.

It's produced by me, Kelly Kolff, with help from Reyes Mendoza and Tre' Jones.

This episode was mixed by Alexander Mark.

Our head a post-production is Will Short.

The songs you heard in this episode come from FirstCom.

And our executive producer is Keith Reynolds.

Thanks for listening.