Privacy For Real: An Interview with Paul Rosenberg

by Jim Davidson

Paul Rosenberg is someone I've known for much of the past 25 years. He was one of the people involved in the Laissez Faire City project and with that group he met my friend and mentor Michael van Notten. Paul is author of many books, including electrical systems and fibre optic systems installations guides for construction contractors as well as the crypto-anarchy movement's favourite novel A Lodging of Wayfaring Men *and other excellent novels. Paul is the founder and chief executive of Cryptohippie.com and writes regularly for* The Freeman's Perspective. *In this interview, I ask Paul some important questions about virtual privacy networks.*

Paul, what mistakes do people make when buying a VPN… a virtual private network?

In this case “making a mistake” depends on what you’re trying to do. If you just want to keep your boss happy (“Yes, I have a VPN”) or keep the jerk in the back of the Starbucks from reading your traffic, a lot of the cheap VPNs might be fine.

But then again, the cheap VPN might not be fine, because there are plenty of scammers in the market, and they’ll be very happy to sell your data out from under you… and the fact that you paid to protect it means that it can be sold for a high price. I have no idea how often that’s actually done, but I’d bet it happens a lot. And I don’t know how to separate the good from the bad without testing them. What they say on their web sites ain’t necessarily so.

If your goal is actual privacy, on the other hand, the mistakes are fairly clear. The first, perhaps, is to get the cheapest thing you can find, imagining that nothing can possibly go wrong. Beyond that, there are a number of technical things that are necessary for real privacy.

The first is multiple hops. A one-hop proxy – the typical cheap VPN – was kind of cool back in the 1990s, but surveillance, both corporate and governmental, is far more sophisticated now, and cross-linking databases sees right through single hops. A minimum of two hops is necessary, and those hops need to be in different jurisdictions, so that they can’t be correlated by a single operation.

The right way to do it, of course, is for the VPN to sense the jurisdiction of their customer, then reroute them to a second jurisdiction, then send their data out of their network in a third. *That* makes for strong privacy.

What else?

Something that almost no one pays attention to, but which is crucial, is anonymous authentication… or, to say it properly, out-of-band authentication. If you log in with the usual username-and-password, the system knows who you are, and that’s a problem for everyone. The solution is to authenticate, not to log in. The system should verify your connection without identifying you. But, that’s hard to do, and you can’t get it cheap.

What about DNS leaks? I’ve heard that mentioned.

Yeah, that’s an issue too. Any good VPN has to run their own DNS. But more than even that, they need to run their own private key infrastructure. Snowden revealed, basically, that the certificate agencies were compromised. So, if your VPN doesn’t have it’s own key infrastructure, the odds are very high that your privacy is merely an illusion.

After that come techie things like crowding at exits, padding traffic and lag obfuscation. But I won’t go through all of that, cool as it is.

Anything else?

I should add one more critical point, and that’s having no single point of failure. There should be no single office, or person, who can blow through your privacy. For example, all the sales and customer service for the VPN should be run by one company. Another company – in a different jurisdiction and operated by different individuals – should run the network. The network operator should rarely deal with a customer, and the sales people should have noting to do with network operations. It’s safer for the operators and far better for the customer.

Don't people have to trust VPN operators a heck of a lot? It seems like a popular VPN could simply steal a lot of valuable information.

Definitely. Using a bad or scam VPN is worse than using nothing at all. Sadly, however, a lot of people see “free” or “cheap” and all further inquiry evaporates. But you’re right, you are trusting the VPN operator a great deal.

It’s possible to build a VPN that requires zero trust, but that’s even harder to do, and there just isn’t market support for it. We’ve tried.

If Cryptohippie somehow disappeared, what would you do to secure your privacy?

My first choice would be to find a service as much like Cryptohippie as possible. It would include anonymous email, a method for authenticating without providing user information, a multi-jurisdiction, multi-hop approach to networking and end-to-end encryption. In short, they’d have to hold privacy as a first consideration, placing everything else beneath it.

Does such a company exist?

Not so far as I know. You’d have to be a privacy activist to run that kind of company. That is, you’d need a core group of people who were willing to suffer in the pursuit of privacy, not just people trying to make money on a web service.

When Cryptohippie started, there was nothing like it. It had to be created from scratch, and it took seriously dedicated privacy activists to do it. If it closed I’d have to look for the next generation of such people… and go back to old-fashioned op-sec practices in the mean time.

As you can see there are many potential difficulties you face in keeping your communications private and your data secure. If you need additional tech support or guidance, please let me know.

=====

Jim Davidson is an author, entrepreneur, actor, and director. He is the cfo of [KanehCN3.com] and the vision director of [HoustonSpaceSociety.net] You can find him on [Twitter.com/planetaryjim] as well as [Pocket.app] and [Flote.app] also as planetaryjim. He appreciates any support you can provide as times are very difficult. See the Paypal link on this page. Or email your humble author to offer other choices. Visit [IglooLuau.com] for more information. Those seeking a multi-jurisdiction multi-hop VPN for communications privacy please visit https://secure.cryptohippie.com/houstonspacesociety.php For those seeking colloidal silver try [ppmSilver.com/Jim] Ask Jim about CryptoWealth.