Podcast Transcript

EPISODE #73

VPNs: Privacy Myth vs. Reality

Published December 22, 2025 • Runtime: 22:31

https://myweirdprompts.com/episode/vpns-privacy-myth-reality/

EPISODE SYNOPSIS

Dive into the often-misunderstood world of Virtual Private Networks (VPNs) with Corn and Herman. They dissect the industry's grand claims, questioning whether VPNs truly deliver on their promises of privacy and security. From the illusion of trust to "quantum resistance" and the controversial debate around backdoors for law enforcement, this episode unpacks the technical realities and marketing hype surrounding VPNs. Discover why redirecting your data flow might be trading one set of problems for another, and gain a clearer perspective on what real digital privacy entails.

DANIEL'S PROMPT

Daniel

I was a freelance writer for VPN reviews and I've reached the conclusion that there's something illogical about the privacy argument. We're essentially moving our trust from the government to a VPN company that often lacks transparency. I personally use VPNs to encrypt my traffic on shared connections, like in hotels, rather than to hide from the government. Lately, I've noticed commercial VPNs claiming to be "quantum resistant," which brings up the challenge quantum computing poses to current encryption standards like AES-256. I actually have an objection to unbreakable encryption because I believe law enforcement should have mechanisms to disrupt criminal activity. I also doubt that truly unbreakable encryption exists against government capabilities. What are your thoughts on my arguments against VPNs, and do you think it's possible for anyone to buy unbreakable encryption for the cost of a monthly subscription?

TRANSCRIPT

Corn

Hello and welcome to My Weird Prompts! I am Corn, your resident curious sloth, and I am joined as always by the one and only Herman Poppleberry. Today we are diving into a topic that has been sitting in our inbox from our producer, Daniel Rosehill. It is all about the murky, often contradictory world of Virtual Private Networks, or VPNs, and the massive claims they make about privacy and security.

Herman

It is a pleasure to be here, Corn. And frankly, it is about time we addressed this. The VPN industry has become a multi-billion dollar behemoth built largely on a foundation of fear and, in my professional opinion, some very creative marketing that skirts the edge of technical reality.

Corn

Well, that is a strong start! The prompt we are looking at today comes from someone who actually worked on the inside of the industry as a freelance reviewer. They are raising some serious red flags about where we place our trust. The core idea is that when you use a VPN to hide from the government or your internet service provider, you are really just moving that trust to a private company that might be even less transparent.

Herman

Precisely. It is a shell game. You are redirecting your data flow through a different pipe, but someone still owns the pipe. As a donkey who appreciates a sturdy fence, I can tell you that a fence is only as good as the person who holds the key to the gate.

Corn

I love that. But before we get too deep into the trust issue, I want to talk about the practical side. Our producer mentioned that they mainly use VPNs for public Wi-Fi, like in a hotel or a coffee shop, just to keep the local hackers out. That makes total sense to me. If I am sitting in a cafe, I do not want the guy at the next table seeing my banking password. Is that not a legitimate use case?

Herman

Oh, it is absolutely legitimate, but even then, it is becoming less necessary. Most of the internet now uses HTTPS, which is Hypertext Transfer Protocol Secure. That already encrypts the data between your browser and the website. A VPN adds another layer, which is fine, but the industry sells it like you are walking through a digital war zone without armor if you do not pay them ten dollars a month.

Corn

Okay, but hang on. Even with HTTPS, my internet provider can still see which websites I am visiting, right? They might not see the specific page, but they see I am on a certain bank site or a certain medical forum. A VPN hides that metadata. That feels like a real privacy win to me.

Herman

It is a win only if you trust the VPN provider more than your internet provider. Your internet provider is a heavily regulated utility in many countries. They have physical offices, legal departments, and strict data retention laws they have to follow. Many of these commercial VPNs are headquartered in tropical islands with zero oversight. You are taking your data out of a regulated environment and handing it to a company whose only promise of privacy is a flashy website and a slogan.

Corn

I do not know, Herman. I think you are being a bit hard on them. Some of these companies have had independent audits. They have proven in court that they do not keep logs. That has to count for something, right?

Herman

Audits are a snapshot in time, Corn. An auditor looks at the server configuration on Tuesday, but the provider can change that configuration on Wednesday with a single command. And as for court cases, yes, a few have stood up to scrutiny, but dozens of others have been caught quietly handing over data or being owned by massive advertising conglomerates. The lack of transparency is the feature, not the bug.

Corn

That is a fair point. It is a bit of a "black box" situation. But let's move to the really futuristic stuff in the prompt. Lately, these companies are starting to talk about "quantum resistance." They are claiming that their encryption can stand up to quantum computers. Is that even a real thing yet, or is it just more marketing fluff?

Herman

It is mostly fluff for now, but with a grain of theoretical truth. Current encryption, like the standard AES two hundred fifty-six, relies on math problems that are incredibly hard for traditional computers to solve. A powerful enough quantum computer could, in theory, crack those problems in seconds. However, those computers do not really exist in a functional, large-scale capacity yet.

Corn

So they are selling us a shield against a sword that hasn't been finished yet?

Herman

Exactly. And even if they are using post-quantum algorithms, those algorithms are brand new. They haven't been battle-tested. In the world of cryptography, new is often dangerous. I would much rather trust a standard that has been poked and prodded for twenty years than something a VPN company claims is "quantum-proof" just to stay ahead of the news cycle.

Corn

I see where you are coming from, but I think there is a value in being prepared. If the government is harvesting data now to decrypt it ten years later when they do have quantum computers, then shouldn't we be using the best stuff available today?

Herman

That is the "harvest now, decrypt later" theory. It is a valid concern for state secrets, but for the average person's browsing habits? It is overkill. And it brings us to a really controversial point in the prompt. The idea that maybe we should not have unbreakable encryption. Our producer suggested that law enforcement needs a way in to stop criminals.

Corn

Yeah, that part really made me think. It is a tough one. We all want privacy, but we also want the police to be able to catch the bad guys. If encryption is truly unbreakable, are we creating a safe haven for the worst parts of society?

Herman

This is where I have to strongly disagree with the premise of the prompt. The idea of a "mechanism" for law enforcement is just a fancy word for a backdoor. And a backdoor is a hole in the fence. If you build a door that only the "good guys" are supposed to use, I guarantee you the "bad guys" will find it and pick the lock.

Corn

But Herman, we have search warrants for physical houses. Why should the digital world be any different? If a judge says there is probable cause, why shouldn't the police be able to see the data?

Herman

Because physics doesn't care about search warrants, Corn. If you weaken the math to allow for a back door, you have weakened the math for everyone. You cannot have a lock that only opens for people with good intentions. It is mathematically impossible to guarantee that only the "right" people will use that access.

Corn

I don't know, I feel like we are smart enough to figure out some kind of multi-key system. You know, like how nuclear launch codes work? You need two different people to turn the key. Maybe the government and the tech company both have to agree?

Herman

You are oversimplifying a massive technical challenge. Every time a government has asked for this, security experts have screamed from the rooftops that it is a recipe for disaster. Look at the Clipper Chip in the nineties. It was a total failure. We have to decide if we want actual security or the illusion of it.

Corn

Well, before we solve the world's encryption debates, let's take a quick break for our sponsors. Larry: Are you worried about the invisible rays coming off your neighbors microwave? Are you tired of your thoughts being intercepted by low-earth orbit satellites? You need the Lead-Lined Sleep Cocoon! This heavy-duty, one thousand pound sleeping bag is crafted from genuine industrial-grade lead and lined with recycled wool from sheep that have never seen a cell tower. The Lead-Lined Sleep Cocoon guarantees a deep, silent sleep, free from all electromagnetic interference and telepathic intrusion. Warning: Do not use on second floors or near weak floor joists. May cause permanent immobility. The Sleep Cocoon—because your brain is a temple, and temples should be made of lead. Larry: BUY NOW!

Corn

...Thanks, Larry. I am not sure my floorboards could handle that, or my health for that matter. Anyway, back to VPNs and trust. Herman, we were talking about whether unbreakable encryption even exists. Do you think a regular person can really buy "unbreakable" security for five dollars a month?

Herman

It depends on what you mean by "unbreakable." If the math is solid, like AES two hundred fifty-six, then even the most powerful government on Earth can't just "brute force" it. They can't just guess the password. But they don't have to. They can hack your phone directly, or they can use a rubber hose—which is to say, they can just compel you or the provider to hand over the keys.

Corn

Right, the "rubber hose cryptanalysis." It is much easier to break the person than the code. But the prompt also mentions that the government likely has capabilities we don't even know about. Do you think the National Security Agency has already cracked the standards we rely on?

Herman

It is the billion-dollar question. History suggests they are always a few steps ahead. When the Data Encryption Standard was created in the seventies, the agency secretly convinced the designers to weaken the key size. But at the same time, they actually made it resistant to a type of attack that the public didn't even know about yet. It is a weird cat-and-mouse game.

Corn

So it is possible we are using encryption that they already have a master key for?

Herman

It is possible, but unlikely for modern standards like AES. The beauty of modern cryptography is that it is open. It is peer-reviewed by mathematicians all over the world. If there was a glaring weakness, someone would likely have found it by now. The real weakness isn't the math; it is the implementation. It is the buggy software, the weak passwords, and the human beings running the companies.

Corn

That brings us back to the VPN companies. If the math is good, but the company is sketchy, then the whole thing is a wash. I am starting to feel like these commercial VPNs are just selling a warm, fuzzy feeling rather than actual protection.

Herman

For many people, that is exactly what it is. It is "security theater." It makes you feel like you are doing something proactive about your privacy while you continue to post your entire life on social media and use a free email service that scans your messages for ads. It is a bit like putting a high-end deadbolt on a screen door.

Corn

Okay, I have to stand up for the users a little bit here. People aren't stupid. They know a VPN isn't a magic wand. But in a world where we are constantly being tracked, isn't some protection better than none? Even if it is just making it slightly harder for the trackers?

Herman

I would argue that it can sometimes be worse than none. It gives you a false sense of security. You might take risks you wouldn't otherwise take because you think you are "invisible." But you are never invisible online. Your browser has a unique fingerprint. Your behavior patterns are recognizable. A VPN only changes your IP address; it doesn't change who you are.

Corn

That is a bleak way to look at it, Herman. We're just digital ghosts being followed by ghosts?

Herman

I prefer to think of us as very well-documented donkeys in a very large pasture. Speaking of being followed, I think we have someone on the line who has some thoughts on this.

Corn

Oh, you are right. We have Jim on the line from Ohio. Hey Jim, what is on your mind today? Jim: Yeah, Jim from Ohio here. I have been listening to you two yapping about these VPN things, and honestly, it sounds like a bunch of malarkey. Back in my day, if you wanted privacy, you just closed the curtains and didn't talk to the neighbors. Now you're telling me I gotta pay some company in the Cayman Islands to hide my grocery list? It's ridiculous.

Corn

Well, Jim, it is more about protecting your personal data and banking info... Jim: Personal data? Please. The government already knows what I eat for breakfast because of my loyalty card at the Piggly Wiggly. My neighbor, Dale, thinks he's being real sneaky with his "private browsing," but I can see him through his window plain as day. He forgot to buy curtains! That's the real privacy crisis in this country—the decline of quality window treatments.

Herman

You make a colorful point, Jim, but digital privacy is a bit different from physical curtains. Jim: Is it? Seems to me like you're just paying for a fancy curtain that the wind can blow right through. And don't get me started on "quantum computers." I can barely get my toaster to work without it trippin' the circuit breaker. My cat, Whiskers, is more of a genius than these computers you're talking about, and he spent twenty minutes this morning trying to fight his own tail. You guys are just overcomplicating things to feel smart. It's all just a big scam to get ten bucks a month out of honest people.

Corn

Thanks for the perspective, Jim. I think there is definitely a segment of the population that feels exactly like you do. Jim: You bet there is. Now, I gotta go. The weather's turning, and I need to make sure my bird feeder is secure. Those squirrels are getting bold. They don't need a VPN to steal my sunflower seeds, I'll tell you that much. Goodbye!

Corn

Thanks for calling in, Jim! Wow, he really doesn't buy the hype, does he?

Herman

Jim is a skeptic, and honestly, we need more skeptics when it comes to the tech industry. He is right that we've traded a lot of our privacy for convenience long before VPNs even entered the chat.

Corn

So, let's get practical. If someone is listening to this and they're thinking about their own VPN subscription, what should they actually do? If the "trust" is just moving from the ISP to the VPN, how do we decide who to trust?

Herman

First, stop looking at the marketing. If a VPN claims they can make you "anonymous," they are lying. No one is anonymous on the internet. Look for companies that have a long track record, transparent ownership, and have undergone multiple, rigorous third-party audits of their infrastructure. And most importantly, use a VPN for a specific purpose—like protecting yourself on public Wi-Fi—rather than as a general "invisibility cloak."

Corn

And what about the "unbreakable" encryption part? Should we be worried that the government might be able to see everything eventually?

Herman

We should be aware of it, but not paralyzed by it. For the average person, the biggest threats aren't the National Security Agency; they are phishing scams, weak passwords, and data breaches at the companies where you actually store your information. Your VPN won't save you if you use "password one two three" for your email.

Corn

That is a great point. It is about the whole ecosystem of security, not just one tool. I think I disagree with our producer on one thing, though. I don't think we should ever intentionally weaken encryption for law enforcement. It just feels too dangerous. Even if it makes the police's job harder, the cost to everyone else's security is too high.

Herman

I am glad to hear you say that, Corn. It is a rare moment of clarity for a sloth. Encryption is one of the few tools we have that actually shifts the power balance back toward the individual. We shouldn't give that up lightly.

Corn

Hey! I have plenty of moments of clarity. They just happen at a slower pace.

Herman

Fair enough. I think the takeaway here is that there is no such thing as a "set it and forget it" solution for privacy. It requires constant skepticism and a real understanding of what these tools can and cannot do.

Corn

Absolutely. Well, this has been a deep dive into the digital weeds. We want to thank our producer, Daniel, for sending in this prompt. It really forced us to look at the reality behind the slogans.

Herman

It certainly did. And it reminded me why I prefer the simplicity of a good, sturdy fence.

Corn

You can find "My Weird Prompts" on Spotify and all your favorite podcast platforms. We'll be back next time with another deep dive into whatever strange ideas come our way.

Herman

Until then, keep your data close and your encryption keys closer.

Corn

Thanks for listening, everyone. Goodbye!

Herman

Goodbye.