How to keep your smart TV from spying on you

Opinion: You could worry about Windows 10 spying on you, or you could worry about something a bit more serious -- like your TV listening in on you and passing on the information to intelligence agencies.

By Steven J. Vaughan-Nichols for Networking | March 8, 2017 -- 14:29 GMT (06:29 PST) | Topic: Security

What do you know. The tin-foil hat brigade was right. Your smart TV may very well have been spying on you for the CIA and MI5. I can't say I'm surprised.

Smart TVs are dumb. They have little security, their interfaces tend to be crap, and, oh yes, many smart TV models were already spying on you for their vendors.

Sarah Tew/CNET

I'm not just talking about tracking what you watch and when. Everyone does that. Hulu, Netflix, YouTube, etc.

If that worries you, go back to rabbit-ear TVs and dumb DVD players. You aren't going to be a happy couch potato in today's internet-entwined television world.

But smart TVs go far beyond tracking what you watch. I'm talking about some far more sneaky actions. Your smart TV may well be listening in to your conversations and even watching you from its built-in video camera.

Sound like science fiction? Nope, it's already happened.

Take my Vizio M50-C1 50-Inch 4K Ultra HD Smart LED TV. It's a great TV with an excellent display. It just has this one little problem: When I first got it, it was tracking my viewing habits and sharing this data with advertisers... by default.

This Smart Interactivity "feature" works by watching what I watch -- whether it's by cable or streaming. It also records the date, time, and channel of programs and if I watched the show live or recorded. Vizio then takes all that data and connects it to my Internet Protocol (IP) address. With that much data, any big data analyst can know more about me -- and not just my television watching habits -- than my family does.

Vizio has changed its ways. The Federal Trade Commission (FTC) forced Vizio to stop its snooping.

Then, there's Samsung. It was revealed last year that some Samsung smart TV models can "capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features."

OK, I can buy that. But, "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

I'm not happy with that. And I'm downright ticked off that Samsung doesn't properly encrypt this data when it sends it home over the internet.

And we can't forget LG. In 2013, LG wasn't sure if its smart TVs were spying on you or not. I think we can safely assume it was spying.

So, what can you do? Well, it depends, as always, on the brand and model.

On the Vizio, which is the most troubling since it's the only company -- that we know of -- that spies by default, you can turn off Smart Interactivity by following these steps from your TV.

1. Press the menu button on your TV's remote.
2. Select settings.
3. Highlight Smart Interactivity.
4. Press right arrow to change setting to off.

The other TVs should be safe so long as you have the voice recognition features turned off.
"Should."

You see I really don't trust any of the TV vendors. The more data they can get about you, the better for their bottom line. And, come on, LG -- you didn't know if you were sucking data from your customers?

Even if you assume the TV vendors care about protecting their customers' data, they don't have the necessary security and network chops to protect your data. TV companies may be experts making great displays, but they're not networking or security pros.

For example, Samsung's data leak came about because its smart TVs were sending data over the 443 TCP socket. That sounds good. That's the default socket for the secure HTTP over SSL protocol. What it was actually sending over this port was a mess made up of XML, binary packets, and some raw, unencrypted data.
I'm no hacker, but I could crack that. When the news broke that intelligence agencies were hacking smart TVs, that really wasn't news. It would've been news if they hadn't cracked such easy targets.

As South Korean security expert Seung-Jin Lee showed in 2013, there's no security worthy of the name in most smart TVs. Lee showed 10 different vulnerabilities that would allow him to get a root shell on the device.

Root? Yes, you see this particular TV ran all of its applications as root. Which means, for those of you not from the Unix/Linux world, that a cracker would get absolute control over the "smart" TV.

I am absolutely sure there has been no improvement in smart TV security since then.

So, what can you do?

Well, for starters, don't buy smart TVs in the first place. Apple TV and Roku, to name two, supply pretty much everything a smart TV does and more. Sure, they can have security holes as well, but at least they're designed by people with a clue about security and network engineering.

What's that? You already have a smart TV? Bite the bullet, disconnect it from the internet, and turn it into a dumb TV. First, check to see if your TV will let you disconnect from your Wi-Fi network. If it won't, reset it to its factory default setting. When it turns on again and goes through its setup routine, don't give it your Wi-Fi password.

If you're using Ethernet, do the same thing -- except this time, you simply don't plug it into your network.

Yes, this is drastic. But you really can't trust smart TVs.

Don't want to go that far? Then go deep through your TV's list of commands and turn off anything that indicates it's listening to you or sending data back to its home company. That may not work, but at least you'll have tried.

And, if you think that's bad, just wait until you add more Internet of Things devices to your home. Are you going to be able to keep track of what your car is saying about your driving habits, or what your electrical use tells about when you're at home? Heck, what your health insurance provider thinks about the fact that you only use an IoT-enabled toothbrush once a day?

No, you're not going to be able to manage this non-stop bleeding of personal data.

Me? I've lived on the internet for longer than many of you have been alive. I appreciate what it gives me, especially with television, but I choose to keep the TV vendors out of my personal life. I think you should too.

Original article:
http://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/