



Your Smart TV Is Spying on You

In the “Internet of Things” in which people now live, there are a variety of devices that use the Internet connectivity to improve functionality. Refrigerators can remind their owners via text or e-mail when to buy milk or eggs. Homeowners can adjust their thermostats and arm their home security systems with mobile apps. People can access Internet programming and change channels and volume levels on Smart TVs using voice and gestures. But how secure is the “Internet of Things” for those who are concerned about privacy?



A recent development in Smart TVs has caused a stir among privacy advocates. Samsung’s newest models have been called into question over the last few months for security issues related to the combination of WiFi connectivity, a built-in camera, and a built-in microphone. Cybersecurity experts are concerned about the “always on” feature of these components and the risks inherent in consumers having a device in their homes that is watching, listening, and reporting to a third party via the Internet.

Samsung spells out some of these risks in their SmartTV Supplement to their Global Privacy Policy in language that is fairly clear. Unfortunately they do it in a way that focuses on convenience instead of privacy. They sell the problems as features.

For instance, they make it very clear that the voice recognition feature, if activated, is always listening and transmitting to a “third party” that handles the voice to text translation, “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.” So, don’t say anything in front of your Smart TV that you wouldn’t want strangers to hear, because they will hear it.

Samsung also addresses the functionality and risks associated with the use of the built-in camera. “To provide you with the ability to control your SmartTV through gestures, the camera mounted on the top of your SmartTV can recognise your movements. This enables you, for example, to move between panels and zoom in or zoom out. We record information about when and how users use gesture controls so that we can evaluate the performance of these controls and improve them,” the privacy policy states. It goes on to say, “You can use facial recognition instead of, or as a supplementary security measure in addition to, manually inputting your password.” While the images users record are not transmitted via the Internet, “Your image will be stored locally, Samsung may take note of the fact that you have set up the feature and collect information about when and how the feature is used so that we can evaluate the performance of this feature and improve it.”

The Smart TV also monitors the content consumers view so as to make “recommendations” of other relevant content that they may find interesting. This is a buzz-phrase for advertisement-based programming. As it is explained in the policy, “In addition, if you enable the collection of information about video streams viewed on your SmartTV, we may collect that information and additional



Written by [C. Mitchell Shaw](#) on February 18, 2015

information about the network, channels, and programs that you view through the SmartTV. We will use such information to improve the recommendations that we deliver to you on the SmartTV.”

If a consumer chooses to use the “fitness features” of their SmartTV, they must provide “certain basic information about [themselves], including [their] height, weight and date of birth.” Along with the login credentials and facial photos many consumers will store on their Smart TV’s, this information is an identity thief’s mother lode.

Perhaps one of the most disturbing parts of the privacy policy supplement are the portions about how this information is shared with third parties. To view content from “third parties,” the Smart TV must make certain information available to the “third party.” According to the policy, “Samsung is not responsible for these providers’ privacy or security practices. You should exercise caution and review the privacy statements applicable to the third-party websites and services you use.” So, how is that different from what happens when you watch a movie on Netflix on your PC? Well, for one thing, your PC is not listening and watching when it’s turned off.

The chain of privacy/security is only as strong as its weakest link, and there are a lot of links in the Smart TV chain. If a hacker, or overreaching government agency, or irresponsible employee of one of those “third parties” gained access through any point in that chain, the consumer would have essentially provided the best device for spying that could probably be imagined. Hackers, government agencies, and irresponsible corporations have shown themselves to be more than willing to spy on individuals for any of a number of reasons, none of which matters to the individuals who are being spied on. Is it really smart for people to put Smart TVs in their homes and make it that much easier?

Samsung’s policy spells out ways to eliminate many of the risks associated with Smart TVs. As to the microphone, “You may disable Voice Recognition data collection at any time by visiting the “settings” menu. However, this may prevent you from using all of the Voice Recognition features, but “Samsung may still collect associated texts and other usage data so that we can evaluate the performance of the feature and improve it.” So, it’s not listening, but it’s still listening.

The solution for the camera is really no better. According to the privacy statement, “The camera can be covered and disabled at any time, but be aware that these advanced services will not be available if the camera is disabled.” It sounds like Samsung is saying the only way to be sure the camera is disabled is to cover it. So, consumers have a choice between duct tape or [these specially designed stickers](#) to cover a camera that should just have a hardware switch that is not dependent on software that can be hacked.

As for the advertisement-based content that is derived from having consumers’ Smart TVs monitoring their viewing habits, the solution follows the usual trend. “If you disable personalised recommendations, then the information and content displayed on your SmartTV may not be as relevant to you. Samsung may still collect information about your usage of the SmartTV for the purposes described in this Samsung Privacy Policy.” So consumers can disable the benefits of the monitoring, but not the monitoring itself.

It seems the only real option is to disable the Internet connection and keep the information that the Smart TV collects from ever leaving the Smart TV. Even then, it would still be storing that information and if ever stolen, could provide the thieves the ability to do much greater harm. Having your identity stolen is enough to make you miss the good old days when you just had your TV stolen.

So, consumers who are concerned about privacy can buy a Smart TV and disable the voice recognition, camera, recommendations, and WiFi connection and have a Smart TV that is only slightly more risky



Written by [C. Mitchell Shaw](#) on February 18, 2015

than a regular old TV — but wouldn't that sort of defeat the point of buying it in the first place?

(SmartTV is a trademark of Samsung. This article uses the term Smart TV to refer to all TVs that connect to the Internet and uses SmartTV only when referring specifically to the product made by Samsung.)



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe