3-5-2015

Your Samsung Smart TV May Not be Spying On You, But Here's Why You Should Still Be Careful

Jessica Zeichner
Cardozo Arts & Entertainment Law Journal

Your Samsung Smart TV May Not be Spying On You, But Here's Why You Should Still Be Careful

BY JESSICA ZEICHNER / ON MARCH 5, 2015

Samsung has come under fire more than once in recent weeks. In one incident, owners of its Smart TVs have been complaining that Samsung is inserting Pepsi ads during the playback of their own locally stored movies. Samsung initially tried to sell ads on its Smart TVs, but quietly stopped the distribution of paid apps for its Smart TVs and connected Blu-ray players about a year ago because it realized that most people simply didn't want to pay for TV apps. This isn't a huge surprise, considering that publishers generally prefer subscription models such as Netflix that allow them to monetize their content across different platforms. (With Netflix, consumers pay Netflix directly, which allows the company to make its service available on mobile as well as connected devices without having to share its revenue with any platform operator.)[1]

In a second and more concerning incident, the company fell under criticism when an owner of a Samsung Smart TV discovered that the company's privacy policy included warnings not to disclose private information while in front of the TV, with the implication that the device might be listening in on our all your conversations. The privacy policy cautions its customers with the following warning: "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."[2] Samsung hands over the data to third parties in order to convert speech commands into text as well as to help the company improve its services. It isn't clear from the privacy policy who the third party is, nor is it clear whether the transmissions are encrypted. Thus, although Samsung says it doesn't retain the voice data or sell it to others for profit, the possibility remains that the recorded data could be extracted before transmission to the third party. In other words, if the data isn't encrypted, it's possible that the televisions could be hacked and used to eavesdrop on customers.

Since the discovery, Samsung has tried to allay its customers' privacy concerns. The company has clarified its policy to explain that the Smart TVs are not continuously monitoring conversations but are rather only capturing voice commands when a user presses the microphone button on his or her remote control. Samsung said that the TVs will collect interactive voice commands only when the user makes "a specific search request to the Smart TV by clicking the activation button either on the remote control or on the screen and speaking into the microphone on the remote control."[3] Otherwise, the devices use "hot words" or phrases such as to monitor for voice commands.

So what can users do to make sure their information is safe? Customers who are still worried about a potential spy lurking in their living room can disable the voice recognition function in

the settings menu of their device, or even disconnect the TV from its Wi-Fi connection. However, Smart TVs (Samsung's as well as others') don't have a great security track record. In the past, hackers have found ways to access built-in microphones and cameras and even to steal account credentials.[4]

To make matters worse, high-level users who want to take their Smart TVs apart to see how they work or to attempt to disable or modify the underlying software (for example, to disable the eavesdropping software) could face felony charges under the Digital Millennium Copyright Act. The reason for this is that most producers of Smart TVs (and other similar platforms) have taken technological measures to prevent users from accessing or modifying firmware in order to prevent illegal copying and distribution of copyrighted material. Users could technically face felony charges for circumventing lockdown restrictions, even if the modifications they're trying to make are legal under copyright law.[5]

Samsung's TVs are not the only devices that have an "always on" listening mode: in fact this issue doesn't just lie with Smart TVs alone. Other voice-activated services, such as Siri, Amazon Echo, and Google Now, require a connection to operate and may be sending signals back to their manufacturers or to third parties. Hackers have shown that they can even break in to some seemingly innocent personal gadgets and household appliances, such as printers, fitness trackers, and VoIP phones.[6] This recent incident clearly indicates that companies like Samsung have to be more transparent about the data collection capabilities of their devices and provide higher levels of protection for their users.

[1] https://gigaom.com/2014/04/21/free-for-all-samsung-stops-selling-apps-for-its-smart-tvs/

[2] http://www.pcmag.com/article2/0,2817,2476476,00.asp

[3] http://www.pcworld.com/article/2883532/us-senator-quizzes-samsung-lg-on-smart-tv-privacy.html

[4]http://www.slate.com/blogs/future_tense/2015/02/10/samsung_s_smarttv_disabling_its_eavesdropping_could_violate_dmca.html

[5]http://www.slate.com/blogs/future_tense/2015/02/10/samsung_s_smarttv_disabling_its_eavesdropping_could_violate_dmca.html

[6]http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html

Jessica Zeichner is a second-year law student at the Benjamin N. Cardozo School of Law and a Staff Editor of the Cardozo Arts & Entertainment Law Journal.