New American

Written by **C. Mitchell Shaw** on January 24, 2019

Privacy at Risk: Security Expert Warns "Smart Device" Users to Beware

Smart Homes — with features powered by Internet-connected devices — are all the rage in some circles and the trend is growing. But is the convenience of being able to control everything from lights to sprinklers, from thermostats to door locks, from refrigerators to security cameras worth the accompanying risks? Warnings from an expert at IBM Security indicate that the answer is "No."

That expert, Charles Henderson, was quoted in two articles for the *New York Times* earlier this week. Henderson is the global head of X-Force Red, a professional hacking team at IBM Security. He told the *Times* that convenience is the major selling point of turning a home into a Smart Home powered by Internet of Things (IoT) devices. "Consumers don't just want this convenience, they expect it — they demand it." The result is that too often, common sense and security — especially where privacy is concerned — take a back seat to that convenience. Many people seem never to consider the risks involved.

The New American has already written about some of these risks in previous articles. In a May 11 article, we noted the various security issues associated with reports that Amazon's "Alexa-powered" Echo will be an standard "appliance" in many new homes:

> Once a "wake" word is given, Alexa listens to what is going on in your home, unless the device is muted. It hears and records what is happening in your home — your choice of television shows, your private conversations, your arguments. Alexa has the capability of sending private voice recordings to the cloud. According to Amazon, Alexa uses these recorded conversations to enhance responses to future questions it is asked. Under the right circumstances, law enforcement can subpoena these conversations. And with legislation such as the National Defense Authorization Act (NDAA) now law, our Fourth Amendment rights don't seem as secure as they used to. Having Alexa seems sort of like having a helpful spy in your home.

Then, almost as if to further illustrate that point, a couple in Portland, Oregon, reported that they had learned — the hard way — that inviting Alexa into their home was a very bad idea. As we explained in a May 31 article:

> With the report that Amazon's Echo recorded a family's private conversation and sent the audio file to a person in the family's contact list, privacy concerns about the Internet of Things (IoT) are in the news again. And while Amazon is downplaying this example, the reality is that Alexa — Echo's voice assistant — like many other IoT platforms and features, is a very real threat to privacy.
>
> Last week, a Portland, Oregon, family was having a private conversation in their Echo-equipped home. Among other things, they discussed hardwood flooring. Later, the man received a call from an employee of his who lives in Seattle, more than 170 miles away. The employee told him he had received a message with the audio of the conversation.

And as far back as February 2015, *The New American* warned readers of the dangers of Internet-connected "Smart TVs." The bottom line is that with embedded cameras and microphones that are always watching and listening and transmitting what they see and hear to the Internet, your Smart TV is spying on you. In fact, many of the so-called smart devices that make up the Internet of Things are designed to spy on you. By packaging them in terms of "convenience," the companies behind them are guilty of selling what this writer calls "surveillance as a feature."

But not everyone is ready to plunge headlong into the panopticon. As the *Times* points out:

> But the road to mass adoption of the smart home will likely be a long and bumpy one. Although the number and nature of smart devices is surging by the day, people have been relatively slow to actually buy and install them.
>
> "It's a really messy space and there's a lot of noise in this," said Frank Gillett, principal analyst at Forrester.
>
> Buying, setting up and connecting smart devices can be costly, cumbersome, and time-consuming. Indeed, as many as one-third of smart speakers are still in their boxes, according to Forrester.

One of the driving forces behind such slow adoption is that nearly half of consumers are still actually concerned about privacy. The *Times* mentions that "security, privacy and trust remain a big concern among owners of smart speakers." In fact, according to a 2017 survey of smart speaker owners by research and advisory firm Gartner, 44 percent of respondents in the United States, the United Kingdom, and Germany said they would be more willing to use a "virtual personal assistant" such as Alexa, Siri, or Google Assistant if all of their personal data were kept on the device rather than being sent to the Internet.

This writer — who can certainly not be accused of hating technology — is firmly in that 44 percent.

Henderson understands better than most what risks are associated with IoT devices. He told the *Times* of "a major electronics firm" which he would not name "for privacy reasons." The firm "started seeing strange documents being printed out remotely on more than 100 of its smart printers late last year" and called in Henderson's elite team of hackers to ferret out the problem.

X-Force Red discovered an unpatched vulnerability in the remote access function of the printers and was able to secure the devices. The salient point, though, is that the manufacturer of the printers did not discover the vulnerability. In fact, Henderson's team was at least second in discovering it, because some hacker or hackers somewhere had already discovered it and used it to breach the printers.

Since those printers were connected to the firm's network, hackers could have used any one of those printers as a point of entry to compromise the entire network. "If you've got rogue devices connected to your network, it's not your network anymore. It's a shared network," warned Henderson. "If you had access to somebody's home hub — and that hub had a sprinkler system, light switches and garage door opener connected to it, you could open their garage door, turn on the sprinkler systems, and start flashing the lights." Add cameras and microphones into the mix, and it is immediately apparent that the problem is exponentially worse.

Henderson adds that with manufacturers rushing products to market to get their share of the IoT pie, "security features take a back seat" to the convenience features that help sell the devices. "We've received roughly five times the number of requests for security testing of IoT devices in the last year," said Henderson. "Growth has been immense over the last year to 18 months."

And while it may seem that the simple solution to protecting one's privacy in this arena would be to eschew IoT smart devices, that is much easier said than done. It is not just about *not* buying and installing them. What happens when you visit the home of a friend or family member who has installed an Echo, Google Home, or similar device? Or you have a friend or family member as a guest in your home and he brings his Android phone with Google Assistant (or iPhone with Siri) along? The end result is that you are still a resident of the panopticon, even if you only live in the outskirts. Your conversations are still being captured and sent to the "cloud."

One thing is certain: As the IoT continues to emerge, the days and years ahead will continue to show a shift in the way people view privacy — if they even think about it at all.

Image: metamorworks via iStock / Getty Images Plus