Written by **C. Mitchell Shaw** on May 31, 2018

Amazon Echo Story Illustrates Dangers of Putting Surveillance Devices in Your Home

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.

As KIRO 7 in Seattle reported, the couple initially did not believe him. The woman — who only went by Danielle in the interview to protect her privacy — said, "At first, my husband was, like, 'no you didn't!' And the (recipient of the message) said 'You sat there talking about hardwood floors.' And we said, 'oh gosh, you really did hear us.'"

They unplugged all of the Echo devices in their home. They had one in every room — including the bedroom — controlling lights, heating and air conditioning, music, and their security system. As *The New American* reported previously, Alexa is set to come standard with many new homes. As IoT devices become more and more a part of people's lives, society is closer and closer to crossing a line into the panopticon.

Concerns about privacy have come up several times over IoT devices. As this writer reported in August 2015, a teenager in Issaquah, Washington, became so concerned about her mother's new Amazon Echo and its ability to listen in on all conversations in the living room that she removed it and hid it from her mother. Her mother told the *New York Post*, "I guess there is a difference between deciding to share something and having something captured by something that you don't know when it's listening." Now — almost two years later — that statement has been punctuated by proof positive.

As this writer wrote in that 2015 article:

> So, was [the teenager's] decision to hide the device and keep her mother from using it reasonable? While some may think she went too far, this writer is not sure she has gone far enough. The Echo is simply the most recent (though certainly not the most egregious) example of the myriad of ways the Internet is used to spy on ordinary people living ordinary lives. Back in February, *The New American* reported on the ability of smart TVs to do the same type of spying. In the case of the TVs, though, it is even worse, because many of them also have a built-in camera.

The article linked above about the spying nature of smart TVs was only the first time this writer addressed those particular devices. In a subsequent article, this writer addressed the "Smart

Interactivity" feature in Vizio's newest line of Smart TVs that monitors the users' viewing habits and reports back to the company so that it can sell that information to advertisers. By capturing your IP address and linking that to any other connected devices (like your laptop, tablet, and smartphone), the company is able to offer advertisers a comprehensive profile of you that permits them to reach out to you on all your devices.

So, the idea of devices that you purchase and install in your home being used by manufacturers (and others) to spy on you is not a new phenomenon. But that is probably of little consequence to Danielle and her husband. After all, she admits that they sort of saw this coming.

KIRO 7 reported that Danielle told them, "My husband and I would joke and say I'd bet these devices are listening to what we're saying." As Shakespeare wrote, "Many a true word hath been spoken in jest." But thinking it may be so and joking about it are a far cry from learning the hard way that it is so. "I felt invaded," Danielle said. "A total privacy invasion." She added, "I'm never plugging that device in again, because I can't trust it."

When Danielle called Amazon — several times — the company had an Alexa engineer investigate. She said the engineer went through the logs and saw that what Danielle said happened really did happen. "He apologized like 15 times in a matter of 30 minutes and he said we really appreciate you bringing this to our attention," Danielle said. She said he added, "This is something we need to fix!" But, the engineer did not provide any specifics as to how or why it happened.

The company later provided a statement to KIRO 7 saying, "Amazon takes privacy very seriously. We investigated what happened and determined this was an extremely rare occurrence. We are taking steps to avoid this from happening in the future."

Amazon spokeswoman Shelby Lichliter provided a later response. Rather than take responsibility, the company dodged all blame, saying:

> Echo woke up due to a word in background conversation sounding like "Alexa." Then, the subsequent conversation was heard as a "send message" request. At which point, Alexa said out loud "To whom?" At which point, the background conversation was interpreted as a name in the customer's contact list. Alexa then asked out loud, "[contact name], right?" Alexa then interpreted background conversation as "right." As unlikely as this string of events is, we are evaluating options to make this case even less likely.

Danielle asked the company to refund her for all of the devices, since she will no longer use them. Amazon initially refused, offering to de-provision the devices' communications so that Danielle and her family could continue using all of the features that don't require communication. Only after the story began to get out did Amazon back down and agree to a refund and a return of the devices.

But what of the millions of other Echo users across America and the rest of the world? Amazon should be prepared for massive returns, if people who hear of this value privacy. After all, consider that many people — like Danielle and her husband — have these devices in every room of their homes, including their bedrooms. The implications of buying and installing an Internet-connected, always-on listening device in you home is staggering. Not only does it require blind trust in the company and the technology, but it also requires blind trust that no one will ever hack the device to allow them to listen in.

In the end, Amazon's Echo is just another device that offers what this writer calls surveillance as a feature. Sure, it's convenient, but is it worth the cost of privacy? This is only the most recent example of

how these devices are designed to betray the privacy of their users. As noted above, there have been other examples and there will certainly be more moving forward.

Photo: AP Images