'Smart' gadgets: Ways to minimize privacy and security risks

May 25 2018, by Barbara Ortutay And Anick Jesdanun

In this Sept. 27, 2017, file photo, an Amazon Echo device sits on a balcony outside an Amazon office as the Space Needle is reflected in windows behind it following a program announcing several new Amazon products by the company, in Seattle. Amazon says an "unlikely" string of events prompted its Echo personal assistant device to record a Portland, Ore., family's private conversation and then send the recording to an acquaintance in Seattle. (AP Photo/Elaine Thompson, File)

Revelations that an Amazon Echo smart speaker inadvertently sent a family's private conversation to an acquaintance highlights some

unexpected risks of new voice-enabled technologies.

According to Amazon, the Echo's Alexa voice assistant misheard a word as "Alexa"—a trigger to activate the device—and interpreted subsequent conversation as a "send message" request. That conversation in a home in Portland, Oregon, was then recorded and sent to an acquaintance in Seattle on the family's contact list.

Amazon blamed the situation on an "unlikely" string of events, and the company already has many privacy safeguards built into the device. Yet the incident shows that even with the best intentions, the risk is never zero. Gadgets these days come loaded with microphones and cameras. They are all vulnerable to hacking or programming errors, and there's nothing consumers can do to eliminate the risks short of unplugging entirely.

But there are ways to minimize the odds that gadgets will serve up unpleasant privacy surprises:

— KILL THE MIC: Most smart speakers have a physical button to disable the microphone, so a private conversation can't be recorded to begin with. You can hit that when you're having sensitive conversations. The button on the Echo will turn red; other devices have similar cues. It doesn't make sense to keep the mic disabled throughout the day, though. If the Echo can't hear you, it won't be able to order you more toilet paper or play smooth jazz.

This July 29, 2015, file photo shows Amazon's Echo speaker, which responds to voice commands, in New York. Revelations that an Amazon Echo smart speaker inadvertently sent a private conversation to an acquaintance shows the risks that come with using new technologies. According to Amazon, the Echo's Alexa voice assistant misheard a word as "Alexa" - a trigger word to activate the device - and interpreted subsequent conversation as a "send message" request. That conversation in a home in Portland, Oregon, was then recorded and sent to an acquaintance in Seattle on the family's contact list. (AP Photo/Mark Lennihan, File)

— LIMIT THE MIC: Disabling the microphone isn't practical on a smartphone, but you can limit what apps have access to it. Go to the settings and turn off mic access to all but essential apps such as voice recorders or video conferencing. Netflix doesn't really need voice access; you can simply type the name of the show you're searching for.

— ABOUT THAT CAMERA: Facebook CEO Mark Zuckerberg

famously puts a piece of tape over his laptop's camera to prevent spying if anyone were to hack his device. Buy yourself a roll. Or use bandages. If you have a home-security camera that's connected to the internet, turn the camera to the wall when you're home. Just remember to turn it back before you leave, or you defeat the point of having a security camera.

— BLOCK THE SIGNALS: For smartphones and other gadgets you carry with you, a "Faraday bag" that blocks electromagnetic waves can help prevent unwanted spying. The good ones will block cellular and other signals, meaning privacy-compromising information such as your location won't leak out either. Just remember, your phone won't get any calls while it's in the bag—that's the whole point.

In this Sept. 27, 2017, file photo, Amazon Echo Plus, center, and other Echo devices sit on display during an event announcing several new Amazon products by the company in Seattle. Amazon says an "unlikely" string of events prompted

its Echo personal assistant device to record a Portland, Ore., family's private conversation and then send the recording to an acquaintance in Seattle. (AP Photo/Elaine Thompson, File)

— BE INFORMED: Apple, Samsung and other tech companies have worked over the years to ensure that their products work "out of the box," without users having to pore through lengthy manuals and operating instructions. The downside is that users are often unaware of all the things their gadgets can do, good or bad. Checking reputable online reviews, how-to guides and even instructional videos will help you get the most out of new technologies. They'll also tell you about any known glitches and risks.

Of course, the safest approach is not to buy a new gadget in the first place. That might not be practical for smartphones these days, but do you really need a smart speaker or a television set that's connected to the internet? (As it turns out, it's actually difficult to buy a TV without "smart" capabilities these days, but nothing says you have to connect it at home.)

From toothbrushes to slow cookers to toys, if companies can dream it up, it's out there. Companies often release smart gadgets without thinking through the risks and ensuring their security. This makes them easy targets for malicious hackers. This is especially true with manufacturers that aren't well known or that specialize in toys and other non-tech businesses.

In this Sept. 27, 2017, file photo, an Amazon Echo Dot is displayed during a program announcing several new Amazon products by the company, in Seattle. Amazon says an "unlikely" string of events prompted its Echo personal assistant device to record a Portland, Ore., family's private conversation and then send the recording to an acquaintance in Seattle. (AP Photo/Elaine Thompson, file)