Beware of the smart device: Ways to stay private and safe

December 31 2019, by Anick Jesdanun

In this May 9, 2018, file photo a second generation Echo that controls the blinds as well as televisions and lighting at an Amazon Experience Centers model home in Dallas, Texas. Many of these internet-connected speaker devices listen constantly for commands and connect to corporate servers to carry them out. Typically, they will ignore private chatter and transmit sound recordings only when you trigger the device, such as by pressing a button or speaking a command phrase like "OK Google." Some gadgets also have a mute button to disable the microphones completely. But there's no easy way for consumers to verify those

safeguards. (Nathan Hunsinger/The Dallas Morning News via AP, File)

Did someone invite a spy into your home over the holidays? Maybe so, if a friend or family member gave you a voice-controlled speaker or some other smart device.

It's easy to forget, but everything from internet-connected speakers with voice assistants such as Amazon's Alexa to television sets with built-in Netflix can be always listening—and sometimes watching, too. As with almost all new technology, installing such devices means balancing privacy risks with the conveniences they offer.

The research firm IDC estimates worldwide shipments of 815 million smart speakers, security cameras and other devices in 2019, up 23% from 2018. Many of the sales are for gifts.

You could sidestep the risks altogether by returning the devices right away. But if you decide to keep them—and the artificial intelligence behind them—there are a few things you can do to minimize their eavesdropping potential.

THE SPEAKERS LISTEN ... AND WATCH

Smart speakers such as Amazon's Echo and Google Home let you check weather and appointments with simple voice commands. Fancier versions come with cameras and screens.

Many of these devices listen constantly for commands and connect to corporate servers to carry them out. Typically, they will ignore private chatter and transmit sound recordings only when you trigger the device, such as by pressing a button or speaking a command phrase like "OK

Google." Some gadgets also have a mute button to disable the microphones completely.

But there's no easy way for consumers to verify those safeguards. In one case, the Alexa assistant in an Echo device misheard background conversation as a command to send the chatter to an acquitance—and so it did.

One more catch: Voice commands sent over the internet are typically stored indefinitely and may include conversations in the background. They can be sought in lawsuits and investigations.

Reputable companies let you review and delete your voice history, Amazon now lets you request automatic deletions after three or 18 months—but you need to set that up, and there's no option to keep Amazon from saving your command history at all.

Until recently, tech companies allowed employees and contractors to review the voice interactions for quality control—and some of those details leaked. Following a backlash, many companies are at least making it clearer and easier to opt out of human review. Pay attention to your choices.

If you have kids, set up a passcode for shopping if your speaker allows it. Otherwise, it can be child's play for a kid to order toys and other goodies through Alexa.

As for those screen models, many also have cameras for video chats. When you're not using the device, consider turning it around to face the wall, especially in the bedroom and other private settings. Or stick a bandage or some tape over the camera. It shouldn't be recording, but why tempt fate?

SECURITY WITH SECURITY VIDEO

This Oct. 9, 2018 file photo shows a Google Home Hub displayed in New York. Many of these internet-connected speaker devices listen constantly for commands and connect to corporate servers to carry them out. Typically, they will ignore private chatter and transmit sound recordings only when you trigger the device, such as by pressing a button or speaking a command phrase like "OK Google." Some gadgets also have a mute button to disable the microphones completely. But there's no easy way for consumers to verify those safeguards. (AP Photo/Richard Drew, File)

Online security cameras let you check in on your pets or kids when you're not home. Amazon's Ring doorbell lets you check who's at the

door without getting up.

Here's the rub: If you can view video on an app, it's possible that a skilled hacker can, too.

When you use the same password at multiple services, a hacker stealing your password from one place can try it on the camera service, too. So don't reuse password. When available, enable two-factor authentication, which requires you to enter a temporary code sent as a text to ensure it's you.

Again, you might want to turn the camera to face the wall when you're home. It's a pain, though, and if you forget to turn it back when you leave, it defeats the purpose of having a security camera.

ARE SMART LOCKS SMART?

Smart locks let you unlock doors with an app, so you can let in guests even when you're not home. Burglars might try to hack the system, though it's often easier for them to just break a window.

As a precaution, disable any capabilities to unlock doors through a smart speaker voice command, especially if you have prankster kids—or teens who might want to sneak someone in.

Though digital keys can be convenient for letting in guests and contractors, they can also leave a digital trail. In a child-custody dispute, for instance, your ex might subpoena the records to learn that you've been staying out late on school nights. If you rent and create a guest key that's used daily, the landlord might suspect an unauthorized occupant.

ABOUT THOSE TVs

Many smart TVs and TV streaming devices come with mics for voice-activated playback controls and video search. That means having audio snippets transmitted over the internet. The same warnings for smart speakers apply here.

There's a simple fix if you aren't using the internet features on your smart TV: Just don't connect the TV to your Wi-Fi in the first place. Of course, this won't work if you're not using a separate gadget for streaming video.

TOYS THAT TALK

Kids might get a kick out of dolls and other toys that talk back. But if the toy is connected to the internet, pay attention to how much control it's giving parents and whether it's letting kids connect to the outside world. You can check online to see if other parents or consumer groups have identified problems.

And be sure to install the latest apps and other software updates, as they may come with fixes for flaws that can otherwise be exploited by hackers.