

How to plan your smart home—and weigh privacy risks

December 10 2018, by Anick Jesdanun



In this Sept. 20, 2017, file photo the Nest Secure alarm system is seen on display during an event in San Francisco. Technology companies are pushing the "smart home," selling appliances and gadgets that offer internet-connected conveniences you didn't know you needed. (AP Photo/Eric Risberg, File)

You might have heard of lights that turn off with an app or voice command. Or window shades that magically rise every morning.

Technology companies are pushing the "smart [home](#)" hard, selling appliances and gadgets that offer internet-connected conveniences you didn't know you needed. But before you succumb to the temptation—for yourself or others—consider that these devices might also give companies and hackers a key to your homes.

Here's how to get started on your smart home and what to worry about along the way.

STARTING THAT SMART HOME

A smart home can encompass features as simple as remote-controlled lamps and as sophisticated as thermostats that know when you're home and turn up the heat automatically. Down the line, you may want to mix and match these tasks into routines, such as a wake-up ritual that automatically starts the coffee maker, lifts the window shades and plays the news.

With the right tools, you can check remotely whether you remembered to lock the doors—and lock them if you forgot. Some systems can also create temporary digital keys for guests and contractors.

Many people start thinking about a smart home when they get a voice-activated speaker such as Amazon's Echo or Google Home, although such gadgets aren't strictly necessary. Nor do you even need actual smart lights and appliances, as you can buy smart plugs, adapters that control existing lights or whatever you plug into them.



In this Aug. 16, 2018, file photo a child holds his Amazon Echo Dot in Kennesaw, Ga. Technology companies are pushing the "smart home," selling appliances and gadgets that offer internet-connected conveniences you didn't know you needed. (AP Photo/Mike Stewart, File)

If you catch the smart-home bug, you can add appliances with the smarts already built in as you replace your existing ones. Major remodels also offer an opportunity to make bigger smart-home plans. You probably wouldn't want to get new window shades now only to replace them with smart ones a year later.

THE RISKS

There are some concerns to keep in mind. Many devices are constantly listening for commands and connect to corporate servers to carry them out. Not everyone is going to be comfortable with live microphones in their homes (though your phone may already be doing the same thing, if

you had enabled assistive features such as "Hey Siri" and "OK Google").

For the most part, recordings will leave home only when you trigger the [device](#), such as by speaking a command phrase like "OK Google" or pressing a button to get the device's attention. But an Amazon device mistakenly recorded and sent a family's private conversation to an acquaintance after the device mistakenly thought it heard the trigger word followed by a "send message" request.

Check what safeguards a device offers before buying. Smart speakers, for instance, typically have a mute button to disable the microphone completely. Mozilla's Privacy Not Included project seeks to warn consumers about products with security or privacy problems. A general web search also might turn up complaints.

In general, it helps to stick with major brands, as their corporate reputations are at stake if they're caught taking shortcuts. Bigger companies can also quickly fix security holes that crop up. Gadgets from startups and no-name brands may offer little or no protection; those companies may be more concerned with rushing a product to market.



This Nov. 11, 2018, photo shows an Ecobee smart thermostat, room sensor and connection components in Hastings-on-Hudson, N.Y. Smart thermostats, which let consumers adjust their home temperatures remotely using any internet-connected device, are among the most popular smart home technologies, with the global smart thermostat market surpassing \$1 billion in 2017, according to Research and Markets. (AP Photo/Cathy Bussewitz, File)

Bigger companies, however, are also more likely to use your data for marketing. So consider the trade-offs.

LEAVING A DIGITAL TRAIL

Even if a product works as intended, it may be leaving a record that can resurface after hacks, lawsuits or investigations .

Manufacturers, for instance, typically store the voice commands their gadget send over the internet and use that data to help them personalize

their services—and, potentially, advertisements. These voice snippets may include music or conversations in the background. Reputable brands let you review and delete your voice history; be sure to do so regularly.

And think twice about smart locks and their digital keys. 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, a landlord might suspect an unauthorized occupant if you create a guest key that's used daily.



In this Oct. 9, 2018, file photo a Google Home Hub is displayed in New York. Technology companies are pushing the "smart home," selling appliances and gadgets that offer internet-connected conveniences you didn't know you needed. (AP Photo/Richard Drew, File)

CHOOSING A SYSTEM

As cable and internet services become commodities, the companies behind them are turning to smart homes for new sources of revenue. AT&T's Digital Life and Comcast's Xfinity Home offer cameras, door controls and other [smart-home](#) devices. The packages are good for those who prefer one-stop shopping, though you might save money and get more choices by shopping around.

For the do-it-yourself approach, consider which company's services you're already using heavily.

If it's Amazon, then devices powered by its Alexa digital assistant might work best. There's a range of Alexa products, including refrigerators and washing machines. You can command an Alexa microwave oven to "reheat one potato" instead of having to look up how many seconds. It'll also reorder popcorn with a command—from Amazon, of course.

Likewise, if you're a heavy Google user, choose devices that support Google's Assistant. Apple has products under the umbrella of HomeKit, while Samsung has SmartThings. Some products will work with more than one digital assistant.

Some devices, especially cameras, come with extra fees for extended storage and other features. But in most cases, you have to pay only for the product.

© 2018 The Associated Press. All rights reserved.

Citation: How to plan your smart home—and weigh privacy risks (2018, December 10) retrieved 20 April 2024 from <https://techxplore.com/news/2018-12-smart-homeand-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.