

## Amazon is about to share your Internet connection with neighbors. Here's how to turn it off.

You have no control over what sort of data flows over Amazon's new Sidewalk wireless network, which has been lying dormant in Echo smart speakers and Ring cameras ... until now



**Listen to article** 8 min

By Geoffrey A. Fowler

Technology columnist

June 7, 2021 at 7:00 a.m. CDT



818

There's an eyebrow-raising technology buried inside millions of Amazon Echo smart speakers and Ring security cameras. They have the ability to make a new kind of wireless network called Sidewalk that shares a slice of your home Internet connection with your neighbors' devices.

And on Tuesday, Amazon is switching Sidewalk on — for everyone.

I'm digging into my settings to turn it off. Sidewalk raises more red flags than a marching band parade: Is it secure enough to be activated in so many homes? Are we helping Amazon build a vast network that can be used for more surveillance? And why didn't Amazon ask us to opt-in before activating a capability lying dormant in our devices?

I recommend you opt out of Sidewalk, too, until we get much better answers to these questions.

[Instruction on how to turn off Sidewalk](#)

Sidewalk will blanket urban and suburban America with a low-bandwidth wireless network that can stretch half a mile and reach places and things that were once too hard or too expensive to connect. It could have many positive uses, such as making it easier to set up smart-home devices in places your WiFi doesn't reach. (That can help your neighbors, and you.) But by participating, you also have no control over what sort of data you're helping to transmit. In communities where Amazon Ring devices already over-police many doors and driveways, Sidewalk could power more surveillance, more trackers — maybe even Amazon drones.

Amazon seems oblivious to many obvious consumer concerns with its increasingly invasive technology. So let me say it: Remotely activating our devices to build a closed Internet of Amazon is not okay.

Amazon founder and CEO Jeff Bezos owns The Washington Post, but I review all tech with the same critical eye.

Amazon declined my request to interview an executive in charge of Sidewalk but over email said it was about making our tech work better. “We live in an increasingly connected world where customers want their devices to stay connected. We built Sidewalk to improve customers’ experiences with their devices and to benefit their communities,” said Manolo Arana, general manager of Sidewalk.

Reasons we would want Sidewalk, he said, include continuing to receive motion alerts from Ring security cameras when they lose WiFi or extending the range of smart lights. Later this month, Amazon is also adding Bluetooth lost-item tracker Tile and smart lock maker Level to the Sidewalk network. And it is partnering with CareBand, a maker of wearable sensors for people with dementia, on a pilot test including indoor and outdoor tracking and a help button.

But Sidewalk is also a vast new wireless network entirely controlled by Amazon — and paid for by us.

## How it works

Amazon is not the only big company working on getting more things connected to the Internet by piggybacking on us. But it’s doing it in a more aggressive way.

Modern iPhones collect and beam out tiny snippets of other people’s data for Apple’s Find My network, used to report the location of lost devices and AirTag trackers. The routers that Comcast puts in our homes automatically double as hotspots for other Xfinity customers, though they create a separate WiFi network for the public traffic.

With Sidewalk, Amazon is creating a more robust network. Your lowly Echo speaker (or other compatible device) is already connected to your home’s private Internet connection. When Amazon transforms it into a so-called Sidewalk Bridge, your device creates a new network of its own that’s not WiFi. Instead, it uses common Bluetooth to connect devices nearby, and another type of signal (using the 900 MHz spectrum) to connect to devices up to half a mile away.

This new Sidewalk network can’t carry as much data as WiFi, but it’s still impressive: Sidewalk signals from all the Amazon devices in your neighborhood overlap and join together to create what’s called a mesh network.

“WiFi is constrained mostly to your home; it doesn’t have the range to go into your backyard and into the neighborhood. Cellular offers long-range connectivity, but it is expensive. Sidewalk splits the difference between those two and allows us to put billions of things at the edge of the network,” Arana said.

But here’s the rub: Sidewalk authorizes your Echo to share a portion of your home’s Internet bandwidth. It’s up to 500 megabytes per month — the rough equivalent of more than 150 cellphone photos. Amazon caps it at a rate of 80 Kbps, which the company says is a fraction of the bandwidth used to stream a typical high-definition video. Still, this traffic could count toward your Internet service provider’s data cap, if you’ve got one. The bill will be paid by you, not Amazon.

Which raises the question: Shouldn’t Amazon be paying us?

It’s not hard to imagine Amazon could use Sidewalk for its own business, such as to track packages or connect up its delivery trucks.

Arana said: “Our focus right now is to make our customers’ devices work better. I’m not able to comment on future roadmap plans.”

# Is Sidewalk secure?

Amazon says it built Sidewalk with three layers of encryption, so that nobody can view the raw data passing through it — not Amazon, not the person who's sharing their Internet.

Tech industry analyst Patrick Moorhead told me he is impressed by Amazon's efforts to keep snoopers out. "I haven't seen very many triple-protected, triple-encrypted systems out there," he said. "That said, there's no infallible system." Even security standards for WiFi have been cracked over the years.

Some other security pros just aren't keen on opening any kind of portal outside your home network's secured perimeters, no matter what Amazon promises.

There's no evidence hackers or independent researchers have found problems with Sidewalk — but it also has yet to become a high-profile target.

## Building out Big Brother

There are also big-picture concerns. Today Amazon talks about Sidewalk as a way to help the roughly quarter of American homes with smart-home appliances get and stay connected. But Amazon doesn't usually have small ambitions.

At the very least, Sidewalk could massively increase the reach of Amazon's thriving but controversial Ring security business, which police forces tapped for more than 20,000 requests for footage in 2020. Sidewalk would allow people and organizations to put Ring devices in places that weren't possible before.

"It is slowly eliminating the notion of 'off-the-grid,'" says Matthew Guariglia, a policy analyst at the tech-liberties-focused Electronic Frontier Foundation. Even though Amazon is a private company, that doesn't mean the surveillance tech it sells can't be dangerous.

"As long as Amazon is storing all that data ... all of that can be accessible to police. It's impossible to think of things as just private or public surveillance anymore."

Amazon has been vague about what types of data will be able to transfer across the network, aside from innocuous-sounding examples, such as receiving alerts, software updates and the location of lost items. "As a low-bandwidth network, Sidewalk is intended to transmit small amounts of data," Arana said.

## Lacking consent

Last but not least, Amazon should have made sharing our Internet connection something we opt in to, rather than just turning it on.

Amazon is activating Sidewalk on devices going back to at least the third-generation Echo speaker, from 2018, though it tells me they can only join the Bluetooth part of the network. (Amazon disclosed those devices had Bluetooth, but not that it might someday use them to build a network.) Echo devices capable of joining the long-range part include the latest Echo and Echo Show 10, both announced in 2020.

“We believe Sidewalk will provide value for every customer and we want to make it easy for them to take advantage of benefits,” Arana said. “Customers setting up an eligible Echo device for the first time have the opportunity to disable Sidewalk during device setup and will also receive a separate notification shortly after setup as well.”

When I set up a new Echo speaker last November, the Alexa app popped up a page about it with only two choices: “enable” and “later.” Amazon said earlier this year it changed that screen to make it clearer customers had the ability to opt out.

Is Sidewalk capability still lurking in even older Amazon devices to be activated in the future? Amazon’s Arana would only answer: “We can’t comment on future plans.”

## How to turn off Sidewalk

Turning Sidewalk off isn't hard, but involves digging through some settings.

- If you've got Echo devices, go to the Alexa app on a phone, then tap the More icon. Then tap on Settings, then tap on Account Settings, then tap on Amazon Sidewalk. In there, make sure "Enabled" is set to off.
- If you've got Ring devices, go to the Ring app on a phone, then tap the three bars at the top left corner to get to the menu. Then tap Control Center, then scroll down to Amazon Sidewalk.

If you turn off Sidewalk on one kind of device, it should cover you for all of them. (Some people have complained they switched off the Sidewalk setting, but it turned itself back on. Amazon says it fixed the problem.)

One more thing to keep in mind: There's no halfway option. If you turn off Sidewalk, you won't be sharing your network with your neighbors, but your devices also won't be able to access its network.

[Back to the top](#)

Updated April 21, 2021

## The secret life of your data: What you need to know

For all the good we get from technology, it can also take a lot from us. The Post's tech columnist Geoffrey A. Fowler examines the personal information streaming out of devices and services we take for granted.

**Alexa:** By default, Amazon keeps a copy of everything Echo smart speakers record.

**Browser extensions:** Add-ons and plug-ins can see and share everything you do on the Web.

**Cars:** Automakers use hundreds of sensors and an always-on Internet connection to record where you go and how you drive.

**Credit cards:** A half-dozen kinds of companies can grab data about purchases, from your bank to the store where you're shopping.

**Don't sell my data:** The California Consumer Privacy Act (CCPA) can help even residents of other states see and delete their data — and tell companies to stop selling it.

**iPhones and Android phones:** Hidden trackers in apps share personal information — even while you and your phone are asleep.

**TVs:** Once every few minutes, smart TVs beam out a snapshot of what's on your screen.

**Web browsers:** Google's Chrome loaded more than 11,000 tracker cookies into our browser — in a single week.

**Have a question about data privacy?** [Ask The Post.](#)