DATA SECURITY

Yes, Your TV Is Probably Spying on You. Your Fridge, Too. Here's What They Know.

Miguel Porlan for NYT Wirecutter

Published June 25, 2025

This is not a conspiracy theory: Many of the devices living in your home are quietly collecting towering heaps of information about you. Your TV, your doorbell, your security system, your thermostat, even your earbuds — all of them are involved. Some of that data may be shared, analyzed, and then sold to the highest bidder, hundreds of times a day, by organizations you've never heard of.

To be fair, some of the information is what you voluntarily provide when you decide to use a smart device or sign up for a service. And some of it, you almost certainly agreed to share, accidentally, by clicking through boilerplate terms-of-service pages. Still, more than a thousand so-called data brokers have access to — and profit from — personal data, through a largely invisible marketplace.

As Peter Dolanjski, senior director of products at privacy-software company DuckDuckGo, characterized the amount of data collected: "It would blow the average person's mind."

READ MORE IN OUR SERIES ON DATA PRIVACY

Explore all articles

The data-industrial complex

The story of smart-home devices and your personal data is merely one chapter in a much larger tale, that

create a unique profile of every consumer. They package those profiles and sell them, to advertisers and research firms, to banks and credit card companies, to home and health and car insurance companies, to landlords, to government agencies, to law enforcement — essentially almost anyone willing to pay.

According to a 2021 report by the Duke Sanford Cyber Policy Program, which examined the collection and sale of sensitive personal data by 10 major brokers, all of them "openly and explicitly advertise data on millions of U.S. individuals, oftentimes advertising thousands or tens of thousands of sub-attributes on each of those individuals, ranging from demographic information to personal activities and life preferences (e.g., politics, travel, banking, healthcare, consumer goods and services)." The report also lists a number of other collected data types, ranging from individuals' political interests and activities to profiles of current and former military personnel to the current location of people's smartphones.

One of the foremost companies, Experian, boasts that its databases hold "insights on over 250 million US consumers and 126 million US households … and bring in 4 billion devices and 1 trillion device signals to definitively connect offline records to online identifiers."

These personal profiles are also used in what is called real-time bidding (RTB), yet another largely invisible technological layer that everyone unwittingly interacts with hundreds of times a day.

Smart devices, such as voice-controlled speakers, Wi-Fi security cameras, TVs, even modern kitchen

reasonably may not expect.

MORE IN THIS SERIES

I Tried, and Failed, to Disappear From the Internet

Every time you use a smartphone or computer to visit a web page that has ads, and every time you open many smartphone apps, a series of transactions takes place in a microsecond: Information about you and your smartphone or computer is offered up for auction, and automated bidders the world over get the chance to place an ad in your view. Their bids may be based on profiles that include highly specific traits, details about your smartphone, and your personal interests based on your online activities. This practice is controversial, because not only does the auction winner have access to personal details in your profile, but so do all of the other bidders. And while that data may be anonymized, it can include personally identifiable information about you — even your current location.

The issue has been known for some time, and in 2021 a team of US senators released a letter sent to a group of prominent tech companies that broker data, including AT&T, Google, OpenX, Twitter, and Verizon, demanding details on RTB in relation to consumer data sent to foreign countries. “Few Americans realize that some auction participants are siphoning off and storing ‘bidstream’ data to compile exhaustive dossiers about them,” the letter noted. “In turn, these dossiers are being openly sold

user-location data, which the FTC said could be used to track someone to "sensitive locations such as medical and reproductive health clinics, places of religious worship and domestic abuse shelters." (This Wired article details how RTB tech physically located Russian president Vladimir Putin.)

In January 2025, the Electronic Privacy Information Center, along with the Irish Council for Civil Liberties, submitted a complaint and request for investigation to the FTC. The complaint alleges that for a decade, Google, which makes Nest smart-home devices, knowingly sent sensitive user data via real-time bidding to "foreign adversary" countries in violation of federal law. At this writing the FTC has yet to respond to requests for confirmation of any pending investigation. We requested confirmation from Google as to whether data used for Google's RTB products and services "contains now or ever contained any data that could be collected from, or accessed by, Google Nest devices, the Google Home app, or Google Nest app." A Google Nest spokesperson responded with this official statement: "Google's Nest products do not sell ads through real-time bidding, nor does Google send sensitive personal data to RTB."

Data brokering is not a new business; it has been around as long as companies have collected information about their customers. But in the modern era, mass data collection has exploded, and a Senate report dating back to 2013 was already raising alarms about the industry. The report goes on to note that data sharing may happen without your consent or your knowledge of what data is being collected, who is seeing it, how it is used, and how you may be affected.

The average American home has 17 internet-connected devices silently observing their activities — and more than 40% of households have smart devices (or 66% if you count smart TVs). They might have an Amazon Echo and a Roku TV. Or perhaps a Google Nest Thermostat and a few iPhones.

If you've ever wondered whether these pieces of technology are passively ingesting information about you — listening as you go about your daily life, synthesizing information about your habits and preferences to help you, sure, but also to sell you things and perhaps sell your data to unknown actors — well, so have we.

Personal data and the smart home

When we speak about smart devices, we're referring to internet-connected devices in your home that you can access using an app, many of which can be automated. That includes your smart thermostat, for example, but also your smart TV, your security camera, your smart kitchen appliances, your smart speakers, and so on. In order to do smart stuff, these devices rely on different types of data, including data that they detect — motion, voices, the temperature — but also data that they access from the internet, as well as data that is specific to you or your home, such as your location. Data is the fuel of the smart home.

Enjoying the benefits of smart devices involves a fundamental trade-off: They and their associated

That data creates a unique profile of you.

Some of that harvested data is used for product development and refinement. Companies refine their products, discover and fix bugs, and create new and better smart devices. But sometimes that data is also used to market other products to you — as well as to other people like you.

What is especially concerning is how difficult (impossible, we'd argue) it is for a device owner to grasp what data is being collected, especially if you link one of your smart devices from one company with a device or platform from another company, such as linking your Tapo camera to your Alexa speaker.

Although companies, especially large, well-known ones, do take meaningful precautions in the way they handle your personal data, they may also be overconfident in their ability to secure your privacy at best. And at worst, they fail to exercise restraint when monetizing your personal data.

So if you're interested in using smart devices, and internet-connected devices in general, you need to use your own best judgment to determine whether that trade-off is comfortable for you. One of the experts we spoke with, Omar Alrawi, a scientist at Georgia Institute of Technology, noted that he operates under the assumption that a data leak of security camera footage is always going to be possible. So while he wouldn't put security cameras inside his home, he does have them outside, where he is less concerned.

Similarly, if you have smart speakers, it's prudent to consider where you place them. We also strongly advise adjusting the privacy settings in the speaker's companion app to ensure that you are comfortable with what data you allow it to access.

Peter Dolanjski of DuckDuckGo noted that it's common for tech companies to rely on third-party analytics and advertising tools in their smartphone apps, including some used to manage smart devices. "We tested the top Android free apps in Google Play, and 96% of those popular free apps contained trackers, companies that were different from the owners of the app — 87% of those send data to Google, and 68% send data to Facebook," Dolanjski said. The issue is that when you use those apps, your personal data is shared with those third parties, which you may be unaware of. In tests of a few smart devices conducted by Wirecutter, we confirmed that some were indeed sending data to third-party endpoints.

We should note, too, that data is part of the cost of affordably priced technology. It helps device makers keep track of bugs and make improvements or add new features. And as long as the companies employ proper security measures, and you as a device owner take standard privacy precautions, you should feel safe using your devices as usual.

Part of our investigation was to find out if all that is true.

Smart speakers are studying you

Let's begin with the always-on devices that many people have invited into their homes. It's useful to think of voice-controlled smart speakers such as Amazon Echo devices, Apple HomePods, and Google Nest models as part quirky entertainment devices and part data-collection machines.

You generate a ton of tempting data. When you set up a smart speaker, you need to use a companion app to set it up, and in doing so you are asked to provide a lot of personally identifiable information: an email address, your physical address or zip code, your smartphone's location, your contacts, and potentially even your photos.

But what makes smart speakers unique is that almost every interaction you have with them is an expression of your interests. The music you like, the news stations you choose, the sports you ask about, the places you mention, the definitions you ask about — all of those add rich details that refine your profile.

Your speaker is always listening, but not like you might think. Smart speakers have microphones that are always on. But Amazon, Apple, and Google Nest confirmed with Wirecutter that their speakers must hear a precise sonic pattern, a wake word, in order to begin recording (though they do make mistakes).

about the reputational damage from getting caught being sneaky. “The data-care policies that every Google employee has taken are extensive,” Oberman said. “There are numerous, numerous privacy reviews — nobody needs the drop in stock price that would come [from a data leak].”

The more you connect, the more you share. Amazon, Apple, and Google each have their own privacy policies, which state what types of data they collect, how they use it, and whether they share it. And all of them note in some form that once you integrate a third-party device with one of those respective platforms, how your data gets treated may change based on the policies of that device. (For example, Nest’s policy states: “When you use third-party services integrated with Google services, their own terms and privacy policies will govern your use of those services.”)

That means that if you use, say, a WiZ smart bulb in a bedroom lamp, you can look up that company’s privacy policy and know how your data is protected. If you then decide that you want to control your bulb with Alexa, Apple Home, Google Home, or any other third-party service, however, the data that WiZ has access to also gets shared with that third party, and that company may use the data differently than WiZ would. As the Philips Hue privacy policy notes, once you pair your Hue bulbs with a third-party service, “We may collect and process functional data (such as registration data, usage and diagnostic information) and your usage thereof.”

Gen AI is changing the playing field. The current versions of Alexa and Google Assistant rely on AI to perform their tasks, and on relatively basic levels they "learn" and are improved, but only in general, not specifically tailored to you.

In contrast, powered by generative AI, the emerging Alexa+ and Google Gemini (gen AI Siri is still in the distance) are intended to be highly personalized and far more proactive. During an Alexa+ demonstration event that Wirecutter attended, the presenter noted that users will be able to tell Alexa their personal preferences, including likes and dislikes in foods, songs, movies, and so on, which will get incorporated into future interactions.

So if you tell Alexa+ that you are allergic to mushrooms and also music by Bob Seger, Alexa+ will filter those out when you ask for recipes or request music. Alexa+ will also make inferences about you — the more you interact with it, the more it will extrapolate.

Similarly, Google says that a substantial amount of user data is collected by Gemini, and while you can prevent your data from being reviewed, it's still collected: "Even when Gemini Apps Activity is off, your conversations will be saved with your account for up to 72 hours." The company claims that data won't be used to serve you ads, but it leaves the option open for future changes.

them, they're paying attention to you, too.

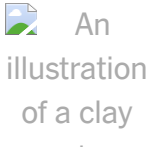
Your smart TV is screenshotting your shows. When you first set up your TV, you probably inadvertently agreed to enable software called Automatic Content Recognition (ACR). This technology takes a screenshot of whatever shows or movies you watch, identifies them, and sends that info to your TV's manufacturer (and potentially its partners, too). Yash Vekaria, co-first author of a study of ACR published last year, told us that ACR is "like someone has installed a camera 24-7 in your living room."

Some TVs capture your viewing as much as multiple times a minute.

Although companies are now required to ask TV buyers to opt in to ACR (following a 2017 FTC action against TV maker Vizio), most people end up doing so without knowing it. To opt out, you have to wade through your TV's settings menus to find a specific privacy setting (more details below).

ACR takes in everything on your screen, not just TV shows. The built-in ACR software in your TV isn't just monitoring and reporting on your devotion to *Today* or even your Netflix binge sessions of *Love Is Blind*. ACR is capturing anything that appears on your screen, including YouTube videos, personal photos, security or doorbell camera streams, and video or photos you send via Apple AirPlay or Google Cast. ACR can even snag content from other devices connected to your TV by HDMI, including personal laptops, video game consoles, and Blu-ray players.

MORE IN THIS SERIES



Your Data Appeared in a Leak. Now What?

A study published in 2024 by the advocacy group Center for Digital Democracy looked at commercial surveillance in the streaming era. The authors cite a number of ways in which personal data harvested by ACR could be used to micro-target people individually, including through personalized pharmaceutical ads or manipulative political ads.

ACR is tenacious. The Center for Digital Democracy's study found that in the smart TVs they tested (from LG and Samsung), ACR continued to run and capture data even when the smart TV was offline. So even if you disconnect your TV from the internet, should you ever reconnect it to your home's network, perhaps for firmware updates, it'll forward saved data to the content-recognition servers as soon as it can ping them. Short of disconnecting your TV, if you want to prevent ACR from sharing your TV viewing, you'll need to turn it off (see below).

Security cameras and video doorbells get personal

Home security cameras alert you when packages are delivered and tell you when someone is at the door.

Security cameras do more than watch. According to a 2024 Surfshark report, home security cameras collect more data points than any other consumer smart devices. Luís Costa, research lead at Surfshark, further told us, "Outdoor security camera apps are among the top collectors of user data. On average, they gather 12 types of data, which is 50 percent more than what's usual for other smart home devices." That includes video and audio, but also data from motion, light, and temperature sensors.

The Surfshark report, which focused on popular camera models (from brands such as Arlo, Eufy, Nest, Ring, TP-Link, and Wyze), notes that many cameras collect personally identifiable information (PII), such as email addresses, phone numbers, payment information, and precise location. And of that data, seven out of the 12 data points are linked by the app to your actual identity.

"The risk of sharing this information with these vendors is the same as any other company that may offer digital services like Google, Apple, or Microsoft," said Alrawi of Georgia Tech. "As a consumer, I have no control [over] how these vendors secure my information, and if it were to be leaked, I would simply get an apology letter with an offer for one year of fraud monitoring." Companies that leak customer data are at risk of potentially steep regulatory penalties and civil actions — but once personal data is leaked, there's no way to undo it.

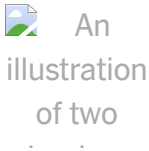
Although security camera companies may not be sharing your video, audio, and still photos, we looked at the privacy policies for Eufy, Google, Ring, and TP-Link, all of which state that they do share personal data for marketing purposes. All of these policies also include a clause that the companies will respond to

had been hit by a cyberattack; the company said that the attack didn't involve access to customers' systems but did include theft of customer information.

AI supercharges, and complicates, everything. AI is commonplace in security cameras, serving to discern what the cameras have detected. Some models, such as Nest video doorbells, can identify specific people by name using facial recognition (which some states, such as Illinois and Texas, and localities like Portland, Oregon, have banned). Some can detect sounds such as alarms, breaking glass, or crying. All of those capabilities require AI, and AI requires training in order to work its magic.

Representatives from Eufy, Google, and TP-Link (maker of Tapo cameras) all told us that user videos are not used to train their AIs and that instead they use publicly available and open-source data. Domek Yang, product security director and chief information security officer for Eufy Security, also noted that "videos voluntarily donated by users are used to improve the models." For example, if you send a report through the app because a video is mislabeled, it could be used for training.

MORE IN THIS SERIES



specific people, or moments, or objects. For instance, you can ask for videos of every time your spouse enters or leaves, or when a red car drives by your house, or whenever the raccoons visit. Those capabilities are possible because of updated versions of the companies' AI, in this case Gemini and Ring IQ, respectively, which are in the process of being rolled out. This may change the way user data is put to work, especially with smart cameras. For instance, Google's privacy policy for its AI specifically notes that Gemini employs human reviewers of user data; the policy also urges customers not to expose "confidential information in your conversations or any data you wouldn't want a reviewer to see or Google to use to improve our products, services, and machine-learning technologies."

That may be a technically correct solution to prevent device owners from accidentally sharing confidential information, though the notion that people who own Gemini-powered smart speakers have to adjust their everyday behavior to cater to their device is concerning.

What you can do to protect your data

All of this doesn't necessarily mean that your data is in jeopardy and that you are at risk. It may simply mean that the way you use devices impacts the way they function, and some of that may make you a valuable target for marketers and advertisers. But if you take simple precautions, you'll have less to

forward by the Biden administration in 2024 that would have curbed the sale of some types of private data by data brokers in line with the way credit bureaus and background-check companies are restricted.

However, the Federal Trade Commission, one of the federal agencies with regulatory power, has launched investigations into some of the related practices that have emerged, such as surveillance pricing.

And the Federal Communications Commission is also in the process of launching an Energy Star–like program for certifying smart-home products, called the U.S. Cyber Trust Mark. The program aims to provide the public with an easy-to-understand way to verify that a device meets a set of security and privacy standards.

In the meantime, here are a number of simple steps you can take that will have profound impact, plus a few device-specific ones:

Opt out of data brokers

The Privacy Rights Clearinghouse outlines the basic process: Go to a data broker's privacy policy on its website, locate where it keeps its instructions for deleting personal data (usually under wording like "consumer privacy rights," "delete your information," or similar), and then file a request. You'll need to verify your identity, which may require submitting personal information.

For instance, to delete your personal information and prevent the sale of your data by Acxiom, one of the largest data brokers, go to Acxiom's opt-out page and enter your details. Click the + icon beside each type of data to add it to your request, and then click Submit. You will receive an email with a confirmation link. Rinse, repeat. This Vice article contains a useful list of brokers with links on how to opt out for each one.

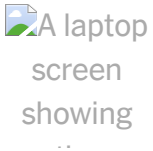
Keep smart devices separated

A common feature of home Wi-Fi routers is the ability to create a secondary or guest Wi-Fi network, which stays disconnected from your own. Use that network only for your smart devices, so they don't have access to the internet activity of all the other devices you use at home on your regular Wi-Fi network.

To set it up, log in to your gateway (combo modem and router, if you rent one from your ISP) or router (if you have your own) and enable a "guest network," giving it a name and a new password.

together all the various logins and subscription services you have.

MORE IN THIS SERIES



The Best Data Removal Services

We've written before about ways to protect your privacy, including services that allow you to relay your email address. Apple's Hide My Email is one good option built into iOS devices and is free with an iCloud+ subscription; **Firefox Relay** provides five addresses for free or 99 cents per month for unlimited addresses.

Limit what smartphone apps can collect

When installing a new app, you get a prompt to allow or deny permissions for the app to access data, including your location, contacts, and photos, as well as Bluetooth or other devices on your network. At the point of install, deny all of those; then, turn them on only as needed when an app prompts you. For location, choose ***Only when using app***.

Disable, delete, or reset advertising identifiers

Unlike computers, all smartphones have a unique advertising identifier — representing your unique profile — that is stored on your device, and which by default is accessible to advertisers on apps and

Privacy & Security page, scroll down to Apple Advertising and turn off ***Personalized Ads***.

On an Android device, go to Settings and then Privacy, select ***Ads***, tap ***Delete advertising ID***, and confirm.

Thwart ad trackers

You have a few ways to prevent ad services from collecting data on you and your devices. There are services that allow you to block ad tracking for all the devices on your Wi-FI network, though we don't currently review them.

Apple iPhones have a pair of built-in do-not-track features for both the Safari web browser and Mail. When you're using Safari, iCloud Private Relay (included in a subscription to iCloud+) is a system that keeps the unique IP address of your smartphone separated from your web activity, which is encrypted. Mail also prevents trackers that are embedded in email messages.

On an Android device, you can download the free **DuckDuckGo web browser**, which includes a feature called App Tracking Protection. Once enabled, it blocks most trackers in all the apps on your phone. (Some trackers are allowed, as turning them off may cause apps or sites to malfunction.)

The Electronic Frontier Foundation's **Privacy Badger**, one of our picks, is a good and free choice.

Consider using a VPN

Smart speakers: Prevent or delete recordings

Each of the smart-speaker platforms handles voice requests and recordings differently. And the newer Alexa+ and Google Gemini, powered by generative AI, will bring changes.

Using the Alexa app, you can view or listen to all of your voice interactions and correct them or delete them. You can also limit how long Alexa keeps recordings before automatically deleting them. Amazon says that it takes up to 48 hours for a deletion to complete. Amazon does not record video calls.

Google Nest does not save chats with Google Assistant unless you specifically opt in, and it doesn't save video calls, either. Google Nest states that it keeps "video footage, audio recordings, and home environment sensor readings separate from advertising, and we won't use this data for ad personalization." However, interactions with Google Assistant may be used for personalization. Google does offer comprehensive controls for limiting what data can be collected, used, and stored, including the ability to delete history. (Note that Google has announced that Google Assistant is in the process of being replaced by Google Gemini on Google and Google Nest devices.)

your interactions with Siri, though you can opt to delete your history by opening Settings and going to ***Siri***, choosing ***Siri & Dictation History***, and then tapping ***Delete Siri & Dictation History***.

Smart security cameras and doorbells: Store recordings locally

The golden rule of internet-connected security cameras is to never point them at anything you wouldn't want the world to see — your driveway or porch might be fine, but your living room, maybe not so much. Otherwise, several models of smart cameras, such as this Eufy camera, allow you to store recordings on the device itself using a removable memory card, or sometimes on a hub. By keeping your recordings in your devices, you lower the risk of recordings being leaked in a data breach or otherwise abused. That said, the devices we recommend encrypt their recordings, so we generally recommend a cloud subscription for most people.

Smart TVs: Disable ACR

If you didn't explicitly choose not to allow ACR when you set up your TV, you'll need to do it now, manually; fortunately, federal law requires TV makers to let you opt out. Doing so may take some digging around, as the process sometimes changes between TV model years and software versions. This SlashGear article has directions for TVs from a number of popular brands, though they may have changed.

Here's the short version of how to disable or limit ACR on the TVs that we currently recommend:

- **Hisense:** Toggle off ***Viewing Information Services*** in the Privacy menu.
- **LG:** First, find Additional Settings in the System menu, and turn off ***Live Plus***. Then go to the Advertisement submenu and turn on ***Limit AD Tracking***.
- **Roku:** Find Smart TV Experience in the Privacy menu and toggle ***Use Info From TV Inputs*** *to off*.
- **Samsung:** In the menu, find Privacy Choices and toggle off ***Viewing Information Services***.
- **Sony:** Go to the Initial Setup menu and disable ***Samba Interactive TV***.

This article was edited by Jon Chase, Grant Clauser, and Jason Chen.

I Tried, and Failed, to Disappear From the Internet

Your Data Appeared in a Leak. Now What?

A Loved One Dies. No One Knows Their Passwords. Here's What to Do.

Yes, Your TV Is Probably Spying On You. Your Fridge, Too. Here's What They Know.

Your Phone Is Stolen. Your Laptop Gets Lost. Here's What to Do.

The Best Data Removal Services