In the Privacy of Your Own Home

That smart TV, your connected thermostat, even your washing machine—they're all tracking your daily habits. Why you need to know who's watching.

LAST SPRING, AS 41,000 RUNNERS made their way through the streets of Dublin in the city's Women's Mini Marathon, an unassuming redheaded man by the name of Candid Wueest stood on the sidelines with a scanner. He had built it in a couple of hours with $75 worth of parts, and he was using it to surreptitiously pick up data from activity trackers worn on runners' wrists. During the race, Wueest managed to collect personal info from 563 racers, including their names, addresses, and passwords, as well as the unique IDs of the devices they were carrying.

Fortunately, Wueest is not a data criminal. He's one of the good guys—a security researcher at Symantec, the company behind Norton antivirus software. His experiment was done to expose some of the risks associated with the growing constellation of "smart" devices known collectively as the Internet of Things.

Many of those devices are versions of familiar, even friendly, consumer products: thermostats, refrigerators, light switches, televisions, and door locks.

What Rights Should Consumers Expect?

Consumer Reports thinks that manufacturers of Internet-connected devices should tell consumers in easy-to-understand language about the types of information being collected by those devices and how that information could potentially be shared, sold, and used. Device manufacturers should also give consumers options to control the collection and use of their data. We also support the work of the Federal Trade Commission, whose recent report on the topic states that the agency "... will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the Internet of Things to promote appropriate security and privacy protections." The FTC also urges more self-regulatory efforts by industry, as well as better data security and broad-based privacy legislation.

PROP STYLING: PRISCILLA JEONG

PHOTOGRAPHS BY DAVID BRANDON GEETING

But the new versions connect to the Internet and can be controlled through an app on a phone, tablet, or computer. The smart devices communicate with each other, too, and they offer an appealing level of convenience. Your car can tell your home's thermostat to turn on the air conditioning as you're driving home. Your security camera can record a video clip if the smoke alarm goes off. And you can use your activity tracker to control lights in your house.

But that convenience comes with a trade-off: The devices can also send a steady flood of personal data to corporate servers, where it's saved and shared, and can be used in ways you can't control. Websites and smartphone apps have been following our activities for a long time, tracking where we go; what we read, watch, and buy; what we write in our e-mails; and who we follow on Facebook and Twitter. But now connected devices gather data from some of the most private spaces of our lives–the bedside table, the kitchen counter, the baby's nursery.

Without proper safeguards, all of the data that different devices and sites have collected about you can be combined, then exploited by marketers or stolen by hackers. U.S. Sen. Ed Markey, D-Mass., who released a report on automotive privacy this winter, says the Internet of Things deserves more scrutiny. (For more on connected cars, see "Can Your Car Get Hacked?" on page 60.) "Whether it is our cars, our thermostats or our household appliances, if these personal devices are connected to the Internet, they are a potential privacy threat," he says. "Consumers' most sensitive information is collected and turned into dossiers that are pure gold in the hands of marketers and pitchmen. We need strong, legally enforceable rules ... to ensure personal information is protected."

WHY IT MATTERS

Compared with websites and mobile apps, the Internet of Things is in its infancy, but the relatively modest constellation of

What Happens When You Check 'Agree'

When you click those ubiquitous "I agree" buttons on the privacy policies of many smart TVs from companies such as LG, Samsung, and Vizio, you are allowing your TV to communicate over the Internet with third parties that analyze your viewing behavior. Some companies also analyze your voice commands. Here's how it works:

What You Watch

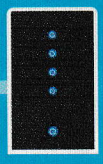
1. ON THE TV Many smart TVs have technology built in to identify what you're watching from any source (cable box, streaming services, and even your own DVDs).

2. OFF TO THE CLOUD The TV creates a "fingerprint" of that video, which is then sent to the servers of third-party companies.

3. BACK TO YOU The info that the third-party company gathers about what you're watching can then be used to serve customized content or advertising back to your set.

4. PART OF THE CROWD Some third-party companies also plan to aggregate the viewing habits of large groups of consumers and compete with established analytics companies such as Nielsen.

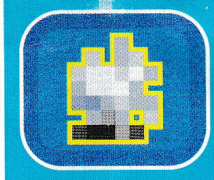
What You Say

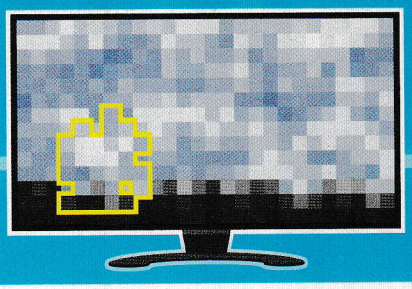


1. ON THE TV Certain smart TVs have built-in microphones for voice control. Some simple voice commands are processed locally on the set.

2. OFF TO THE CLOUD More complex commands, which require more horsepower, are sent out to a third-party company that handles voice recognition in the cloud. It's a process similar to the one used by Apple and Google for smartphone digital assistants.

3. BACK TO YOU Once processed, results for voice commands and search are sent back to your TV.

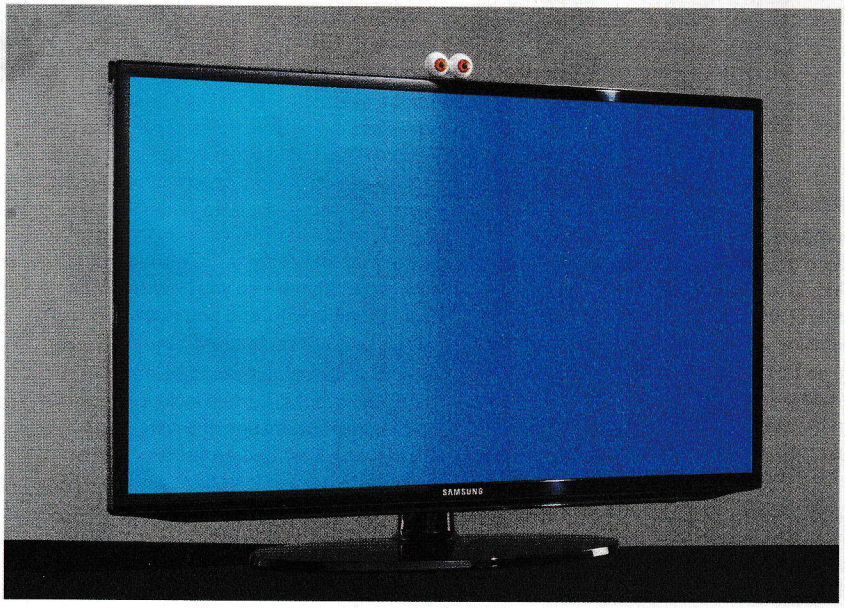




ILLUSTRATIONS BY DAVID PREISS

products out there is already generating a vast amount of information. According to Cisco Systems, the networking giant, there were almost 109 million wearable devices in use around the world by the end of 2014, generating millions of gigabytes of data each month. Those numbers are sure to balloon. Startups and established technology companies such as Apple, GE, Honeywell, IBM, LG, and Samsung are investing heavily in the race to dominate the Internet of Things. Google has recently been on a multibillion-dollar buying spree, purchasing the companies that make Nest thermostats, Dropcam security cameras, and Revolv connected-home hubs.

In March, Amazon announced its upcoming Dash program, which invites customers to install Wi-Fi connected buttons around their homes. Pressing one of the buttons will automatically order brand-name household supplies, such as Bounty paper towels and Tide detergent. Amazon already has lined up device makers, such as Whirlpool and Brother, who can build that technology directly into their products so that washing machines can order their own detergent and printers can order ink–all from Amazon, of course.



Home, Surveilled Home

The Crock-Pot Smart Slow Cooker SCCPWM-00-V1 (above), Nest Learning Thermostat (right), and Samsung H5203-Series Smart TV (below) all send data from your home out to corporate servers. That enables convenient features but also raises privacy concerns.

Companies are also offering incentives for consumers to share information from their devices. John Hancock is giving new life insurance customers a free Fitbit and plan discount in exchange for their fitness data. By design, such devices pay close attention to their owners and log many of the daily activities of their lives. Some of the companies that sell those products currently promise not to use the collected data for advertising and promotion. But in the absence of regulation, that can change at any time. Do you want the disappointing readout on your smart scale to translate into ads for diet plans on your smartphone? Maybe you do, maybe you don't–but the choice ought to be yours.

For consumers, it's not always clear what information stays on a connected device and what goes out to the Internet. And when people learn the details, they can get seriously creeped out. When Mattel announced plans to launch Hello Barbie, a Wi-Fi connected doll that holds conversations with children (by using remote servers), parents' groups cried foul. The Campaign for a Commercial-Free Childhood launched a petition aimed at stopping the toy maker from producing the doll. (As we went to press, the doll was still scheduled to hit store shelves in late fall.)

The prospect of ubiquitous, data-collecting smart objects troubles many privacy advocates, including Lee Tien, a senior staff attorney for the Electronic Frontier Foundation. "The selling and renting of your information is routine, it's happening all the time, and people can create a biography of you," he says.

Consumers may or may not worry about being monitored by their appliances–but they need to know if it's happening. And they need to be aware of how the collected information is being used. But it's difficult for most of us to determine just what's going on under the hood of those devices.

WHAT'S HIDDEN IN THE FINE PRINT

Coffeemakers didn't used to need privacy policies. Neither did dishwashers, thermostats, and cars. Yet today, connected versions of those products come with reams of legal language that you're asked

to agree to. Arguably, you shouldn't have to read a privacy policy to learn whether an appliance is tracking you–and if you *do* try to read those policies, you'll probably find them difficult to decipher.

An analysis by Consumer Reports in cooperation with Georgetown Law's Center on Privacy & Technology shows that many privacy policies for connected devices are vague, confusing, and sweeping. In the absence of strong privacy laws, that legalese matters, says Alvaro Bedoya, the center's executive director. "Your privacy protections on these devices largely turn on those policies–the little, fine-print promises that companies make about your data," he says.

When the effects of policies are revealed, consumers may be surprised, or even shocked. In February the media reported that LG and Samsung smart TVs allowed those companies to transmit household conversations to third parties. At first blush, the technology seemed truly unsettling; if you and your husband argued over your bills during an episode of "The Voice," would debt-consolidation companies suddenly start texting you?

In reality, sending your living-room chatter to a third-party company is just a matter of technological convenience for the TV makers. One of the features of those high-end TVs is voice control, and no television has the built-in processing power to do complex voice recognition. So when users hit the button on their remotes to engage voice control, the recorded audio is sent out to a partner company. (It's the same basic technology that enables Apple's Siri.) But the privacy policies didn't clearly explain when the TVs were recording or where the voice data was going–nor promise that the data wouldn't be used for other purposes in the future. The backlash caused Samsung, at least, to clarify its privacy policy, although the technology remains functionally the same.

We found other, more intriguing stuff buried in the policies of several smart-TV makers. Many of the sets automatically monitor and identify video that comes across consumers' screens, including broadcast TV, streaming videos, and even your own DVDs. Our subsequent investigation found that the TVs send the viewing data to partner companies few consumers have heard of, such as Cognitive Networks and Enswers.

Those companies make no secret of how they plan to use consumer data. In its pitch to advertisers and TV makers, Cognitive's website describes its business this way: "... we enable TV content providers to increase their revenues by offering enhanced advertising opportunities to their customers. And since they're using our [Cognitive's] technology on your [the manufacturers'] TVs, this generates an ongoing revenue stream back to you for every set in market."

In other words, the manufacturer can sell you a TV, then continue to make money by monitoring what you watch and sending customized ads to you, and also selling the aggregate viewing data to advertisers and content providers. It's a potential moneymaker for everybody–except you.

How Smart Devices Work

EXAMPLE: Activity tracker.

Data Collection

Most "smart" devices have a variety of built-in sensors. An activity tracker, for instance, can have an accelerometer for detecting motion and counting steps, a GPS antenna to record your location, and a heart rate monitor to detect your pulse. The data from those sensors can then be transmitted via Bluetooth to an app on your smartphone, which can then send it to servers on the Internet.

THE SECURITY GAP

Even companies that aren't trying to directly monetize your data can be putting consumer privacy at risk. Profiles of user habits and behavior stored on company servers could be subject to data breaches, as Target's and Home Depot's credit-card files were.

And the devices themselves can be vulnerable to hackers. HP Fortify on Demand, a security business owned by Hewlett-Packard, studied 10 connected products in 2014, including TVs, door locks, and home alarms. Daniel Miessler, the unit's head of security research, says that eight of the 10 devices did not require a complex password, seven failed to encrypt data during transmission, and six had user interfaces that were so insecure that attackers could reset passwords.

Poking holes in the security of connected-home devices has become a popular sport among researchers. Last year a security instructor named Joshua Wright took advantage of a vulnerability

in Z-Wave, a wireless standard used to automate home appliances. Using the hack, he was able to open smart locks from several feet away.

Researchers at a startup called Synack said they found security flaws in 16 devices they tested, including cameras, thermostats, and smoke detectors. And HP's Miessler was able to gain control of home security cameras by intercepting and modifying software updates that were being transmitted to the devices.

That type of hacking requires patience and immense expertise–for the first person who attempts it. But hackers share information. Once a vulnerability has been exposed, any malicious actor with a little bit of technical skill can repeat many hacks. Device makers would do well to learn from the lessons of the computer industry. Good digital security is an act of vigilance, and manufacturers need to constantly update the security of their products as new threats emerge.

PROTECTING OUR FUTURE

Concerns about the Internet of Things have not gone unnoticed by government agencies. The Federal Trade Commission issued a detailed report on the subject this past January that recommended best practices for companies, such as building security into devices in the design process and requiring strong passwords. Then in March the FTC announced the creation of a new division devoted to those products, declaring that from a security and privacy perspective, particular challenges were posed by "the predicted pervasive introduction of sensors and devices into currently intimate spaces–such as the home, the car," and wearables.

But laws and policy move slowly, and technology evolves quickly. In March, Facebook launched a platform to help developers create apps for connected devices. Imagine what could happen if the company that mastered the science of turning personal relationships into corporate profit was monitoring the relationship between you and your smart fridge.

"The Internet of Things is perhaps the clearest example of how technology is outpacing our privacy laws," Bedoya says. "Our laws just aren't ready for it."

For now, it's up to consumers to shape the future of these technologies, by buying only products they feel comfortable with–and speaking up when they don't like what they see. Smart televisions offer convenience; they can also collect data to help TV makers target viewers with advertising. That may be an acceptable trade-off for some consumers but not for others. As the Internet of Things expands and policies shapeshift, the best consumer-protection advocates may be consumers themselves.

6 Ways to Reduce Your Exposure

If you don't like the idea of being tracked by your devices, you may think you have only two options: Avoid the technology altogether or simply surrender to the surveillance. But for most smart products, there are strategies that can at least restrict how much of your information gets collected. (See our related video at ConsumerReports.org.)

1.

Password-protect anything that collects personal information. Many smart devices are managed through Internet-based accounts. Some have pass codes you can enter on the device as well. Use both. And yes, you do need to pick unique and complex passwords. We suggest at least nine characters in a combination of letters, numbers, and symbols (see our video on creating better passwords at ConsumerReports.org). Also, if you haven't already done so, make sure to password-protect the settings on your router as well as its Wi-Fi connection.

2.

Read the privacy policy. We know they're often long and indecipherable. But if you want an indication of the kinds of information your device is tracking, that's where you'll find it. But bring your legal-to-English dictionary. Remember, however, manufacturers can change their policies at any time. And in case of a data breach, all bets are off. Hackers don't read those policies, either.

3.

Find the "off" toggle in the settings menu on your smart device. Often, features that track you are given a line-item on-off toggle. On smart TVs, for example, you can switch off voice control and "interactive" functionality. If anything seems suspicious to you, turn it off—you can always turn it back on later if it disables a function you need.

4.

Don't leave connected devices on when you're not using them. Certain Internet-enabled devices are hooked to the Internet 24/7 by necessity (a smart thermostat, for example), but a connected baby monitor doesn't need to be streaming video from junior's crib when your baby is in your arms. Just turn it off.

5.

Install security updates. Device makers need to get serious about automatically pushing out security updates. But consumers would be wise to periodically check the manufacturer's website to see whether their device has a patch, an update, or new firmware. If there is, install it quickly.

6.

Take it offline. If Wi-Fi or cellular connectivity in a product doesn't offer a tangible benefit to you, buy the nonconnected version. If a nonconnected version isn't available, you can still buy the smart product—just don't set it up on your Wi-Fi network. It may sound obvious, but it's worth stating: If a device isn't connected to the Internet, there's no snooping and no hacking.

Share Your Story

How is the Internet of Things affecting your life?

Do you own a smart TV, wearable device, connected car, or smart appliance, or are you planning to buy one? We want to hear your thoughts concerning the devices that collect data about you. Are you looking to integrate more connected objects into your life, or are you worried by the prospect of more smart devices in your home? Share your thoughts on the subject with us at ConsumerReports.org/cro/internet0615.