# You Let That In?

**Hilarie Orman** • *Purple Streak*

The "things" in the Internet of Things (IoT) can get personal. They can be in your home, your car, and your body. They can make your living and working space smart, and they can be dangerous to your health, safety, and liberty. Clever electronic designers make more and more pervasive things that communicate, command, and control. Is our future a brave new world or a dystopian nightmare? Who decides?

The history of the Internet shows that industry treats security as something that might be added later should the product garner a market base and in response to customer demand. The IoT for the home market is following that pathway, but the disturbing difference is that new products are more numerous and invasive than previous disruptive products. Beyond that, there's no limit to the range of things that will be connected to the Internet. When the Internet was young, with fewer than 10,000 connected computers, the system's vulnerability was demonstrated by the Morris Worm.[1] To this day, malware attacks based on similar technology are a part of daily Internet life. Conservative estimates predict 25 billion Internet-connected sensors by 2020. It's unlikely that this horde will be protected by strong security.

Security experts are spooked about the dangers of IoT[2] and have recommended that the US federal government regulate the field to ensure that standard cybersecurity measures are part of the new devices. However, the current administration looks askance at new regulations, and even if they were to act, it would take some years to stop the current onslaught of an insecure IoT. We will be left to our own devices for cybersecurity protection for the immediate future.

Let's step back and look at the risks and what the educated consumer can do about mitigation. Perhaps there's a way to get the magic of the pervasive little things with minimal risk to our safety, security, and privacy.

## The Range of Devices

What are the small devices with wireless capabilities? They run a huge gamut, and almost everything about our environment can be sensed and reported by one or more IoT device. They vary in capabilities and they pose a variety of challenging threat models.

One of the earliest and most popular mainstream items has been embraced by athletes at all levels. On-the-wrist devices for measuring activity rates are almost de rigueur for the weekend warrior.

Many homeowners invest in surveillance cameras. Sometimes the objective is to collect evidence in the event of a break-in, malfeasance by employees or family members, or sometimes to watch the antics of pets while home alone (though, in my experience, pets spend the bulk of their time alone simply waiting for their owner to return). The cameras are easy to install, and the video is usually available over the Internet. Sometimes it's locally recorded as well.

But this is only the beginning. There are light bulbs with wireless control, voice-activated door and window locks and alarm systems, always-on voice-activated shopping apps, smart thermostats, smartphone-controlled appliances, and systems that learn your temperature setting preferences and adjust your heating and cooling systems automatically. One weirdly disturbing device is the smart plate that purports to recognize what's on your plate and to analyze the caloric content of the meal, warning you if you seem to be serving yourself too much.[3]

The modern car knows all its vital statistics, where it is, and how fast it's going. That data can be collected, analyzed, and used by the manufacturer to diagnose or warn about mechanical problems or to help the owner use the car more efficiently. With an Internet connection, the data can be shared in ways the manufacturer determines.

2469-7087/17/$33.00 © 2017 IEEE Published by the IEEE Computer Society October 2017

There are an increasing number of devices for the human body. Those that simply monitor vital functions are useful for the exercise-minded, but medical technology is rapidly incorporating CPUs and wireless communication and control into heart devices and infusion pumps. The opportunities for real-time insight into heart function or internal chemical balance is an alluring goal for improving lives.[4]

The human brain is the ultimate hackerspace. Although the invasive brain devices for controlling prostheses or enabling low-resolution vision require highly trained medical personnel for installation, the hobbyist today can buy kits for noninvasive brain signal sensing devices (see openbci.com). Thousands of people are in the brain-computer interface hobbyist community, and future cellphones might be able to do away with voice recognition and simply "listen" to the user's brain.

## The Range of Concerns

With this increasing range of devices comes an increasing range of concerns, starting with privacy and continuing onward to potential legal risks More devices in your personal space mean that more of your personal life is at risk of exposure, and your personal responsibility for overseeing those devices and making sure they don't harm others also increases. Even devices meant to increase personal security can be harmful.

### Privacy, Privacy, Privacy

To me, the most unnerving feature of the home IoT devices is their enthusiasm for throwing the owners's personal data out into the Internet fog. Of course, it's often not just the owner, but the owner's family, guests, employees, and pets that are potentially subject to reporting. Be it a car, a television, or a smart refrigerator, the device might be disclosing more information to more people than the consumer realizes.

Many Internet-connected commercial devices for the home have an implied trust relationship with the manufacturer or other third parties. The data, be it sensor readings or audio or video, might be subject to storage on a webserver managed by a web service provider and owned by a cloud service provider. The data might be shared with other parties with whom the manufacturer has a business relationship. The advantages to the consumer are that the data are more readily available for sharing or viewing from multiple devices, the results of third-party analysis can provide insights for better management of daily activities or home energy consumption, and the software designer can get feedback that results in improvements in features and stability. What's not to like?

The problem with remote access and third-party management and sharing is that it poses huge privacy risks. The information about how far you ran, where you were, the calories you ate, your heart rate, what you watch on TV, and the video of your cat might wind up on a public website or in the hands of unnamed parties favored by the device manufacturer. Although disclosure of such sharing is required by the Federal Communications Commission (FCC), the regulation is difficult to enforce, as shown by a recent slap-on-the-wrist issued to TV manufacturer Vizio.[5]

Secretive third parties might be the least of the problems. Easy installation is an important aspect of consumer products, but security is usually at odds with ease. The devices are often pathetically easy to hack. The surveillance video might be being watched by would-be thieves. Perhaps they can watch you setting the security code for the smart alarm system, and perhaps they then watch you leave the house. Perhaps they can turn the system on and off, overriding your own instructions. Or maybe your refrigerator could give away your email password.[6] In the world of IoT, the personal can become public with distressing ease.

Devices that listen for voice commands are particularly problematic when they're connected to Internet services. The Amazon Echo with voice recognition service is always ready to take commands for controlling any nearby compatible smart devices (a sort of high-tech clapper) or make online purchases or summon an Uber car. It hears all, but is only supposed to forward the audio under limited, well-understood circumstances. Without carefully monitoring outgoing Internet packets, the consumer can't be sure about this assertion, and indeed, legal authorities have raised questions about it.[7]

### Malfunction and Damage

It's wonderful to control household devices from a phone; that phone might even observe your preferences over the course of several days and automatically create a customized control schedule. But controlling refrigerators, heating systems, coffee makers, and other 120-volt devices might be dangerous to your home if those devices are connected to the Internet. Anyone who gains administrative access to the devices would have the potential to run them too often, perhaps causing a fire hazard, or turning off power and letting food rot in an otherwise smart refrigerator.

Voice-activated devices have turned out to be indiscriminate in who they'll take commands from. A voice emanating from a television or speaker phone can wake them up, and from there, commands for controlling the house could wreak havoc. The house locks might be opened or the car started, for example. Because some smart locks have voice technology, homeowners rely on them for controls while they're at home, but in some cases a loud voice from outside has the same effect.

The ability to hack computer controls on cars remotely has been established in years past,[8] but self-driving cars offer a whole new world of opportunities for abuse. Without tight security controls, we might see a new form

of joyriding, in which hackers from anywhere on Earth can find and drive cars over the objections of their hapless passengers. Idle cars might be taken over and used to create massive traffic jams, perhaps impeding law enforcement and enabling crime sprees.

Even the lowly lightbulb, when imbued with smartness, is subject to remote attack. Researchers demonstrated that they could control the lights in an office building by flying a drone equipped with a radio communications device near the windows.[9] Hackers might have the ability to cause widespread blackouts if there's no access control on the lightbulbs.

But if malfunctions of cars, door locks, refrigerators, and light bulbs aren't unnerving, certainly the hackable heart should be a universal wake-up call. The FDA has issued warnings about implantable cardiac devices and infusion pumps[10] that have underpowered security protections. Those devices could be accessed over a computer network by unauthorized users, and that access gives the user complete control over the device. Although there are guidelines for medical device security, manufacturers, like all cutting-edge tech developers, often ignore them.

### Increased Internet Attack Surface

Having billions of small, specialized devices connected to the Internet might seem like a problem only for the device owners, but it turns out that the Internet itself could be the victim of its own success in this area. As was pointed out in last year's congressional hearing,[2] poorly secured home devices have been harnessed to conduct large-scale distributed denial-of-service attacks against crucial points of Internet infrastructure. For years, security experts have lamented the destructive power of botnets from tens or hundreds of thousands of PCs; the IoT raises the specter of a factor of a million more devices participating in coordinated attacks.

### Legal Risks

The consumer might be a victim of his own devices if they malfunction, but he could also suffer if those devices are used to testify against him. When welcoming a new device, we might well review the advice attributed to the Twitter feed of Olivia Nuzzi of *The Daily Beast*: "dance like no one is watching; email like it may one day be read aloud in a deposition." Just as your cellphone might be used to implicate you in a crime, your home devices might be recording your conversations, and those might be the subject of a future subpoena.[7] Avoid talking to the IoT; it's not your best buddy.

## Trying to Be Safe in the IoT

As informed consumers and managers of our home networks, we have to be aware of the security configurations of each of our devices. This quickly gets to be a nuisance, and each new, attractive, time-saving, intelligent device comes with a security cost.

As with any Internet-connected device, make sure that you change the default passwords immediately. Failure to do this is probably the most-exploited loophole for home devices. If the device has remote management capability, you should probably disable it unless you have some special need to configure it from afar. Record the device's media access control (MAC) address and default passwords. Although devices used to come with a universally known initial password such as "admin," more and more have unique passwords that are printed on the box or a device label. Record the new passwords in a safe place.

When the device connects to your WiFi network, login to the WiFi router and make sure that the new MAC address shows up. There are so many WiFi networks in densely populated areas that it's entirely possible that your new device has connected to a neighbor's network, where it could be compromised before being returned to your home network.

Although the ability to automatically connect new devices or guest's devices to a WiFi network is a great convenience, it's also a point of great vulnerability. Besides having a good password for your WiFi router, consider applying more stringent access controls based on MAC addresses. Visitors to the house might be surprised to learn that their settings include that obscure information, and is easily accessed and can be added to the router's access control list with a few minutes of effort.

Routers usually have a list of active connections, and if the new device is opening connections to unexpected destinations, you might need to do some investigation of its traffic. Using a network utility like tcpdump, the home network administrator can look into the packet traffic from new devices. If the message payloads aren't encrypted, the devices are missing fundamental security technology and could leak personal data to the world at large.

Many devices use radio communication for local commands, and the smartphone is becoming the nexus for control. All of the aforementioned precautions apply to smartphone traffic after installing a new app for managing an IoT device. Where's the monitored data from the device going? Does it stay on the phone or is it uploaded to a remote server? Is the remote site on any lists of compromised or criminal sites?

A distressing fact of electronic life is that nothing lasts forever, and you might find that after carefully configuring all your devices, your phone or router undergoes catastrophic failure and must be replaced. You might need to reapply all your security measures, repair devices, and record MAC addresses all over again. Consumer demand for self-configuring security remains low, and the burden is inherited by the paranoid expert.

Will shaky security and complicated trust relationships always be part of the IoT ecosystem? From a

*This article originally appeared in*
IEEE Internet Computing, *vol. 21, no. 3, 2017*

basic technology viewpoint, authentication and encryption should be part of any but the most energy-starved IoT devices. For example, there are providers of IoT certificates[11] in the market today, and there are many ciphers that are fast and use little energy. Nonetheless, integrating certificate-based authentication into the management of home networks with potentially hundreds of small devices scattered about will remain a challenge for some time to come.

The call for regulation, should it fall on sympathetic ears, might result in uniform standards for new devices, and that could pave the way for better security management systems. This is only a small part of the overall security picture, but it would help ensure greater privacy for home systems and greater safety for automobile and medical systems. This must be addressed before we're overtaken by the Internet of implantables.

Until that time, there's another way to tackle IoT. The small devices don't need complicated software, and they're intellectually accessible to anyone with an elementary programming background. This makes IoT a fertile ground for the open source community. Indeed, there are a plethora of open source projects and kits with the electronic components.[12]

A popular platform for IoT control stations can be found in the Raspberry Pi computer running Linux. The small form factor and low price make it the machine of choice for many hobbyists. It's not difficult to build a video surveillance device, an intercom, or a motion-activated alarm system from open source software and a small computer.

The advantage of an open source DIY system is the opportunity to examine the security components and to augment or replace it with customized software. If the owner bases his access control on Pretty Good Privacy (PGP), then that can be added to the software. If the monitored data's destination is a cloud-based storage and analysis system, then owners have the assurance that the data are transmitted and stored with strong encryption and no crypto backdoors.

Before rushing to adopt an open source solution, though, look carefully about what that means. There are many proprietary systems that provide an open source API for some of their functions, but the service itself might be costly. The other downsides of commercial services might be present as well: data sharing with third parties, targeted advertising, and cooperation with law enforcement investigations.

The billions of IoT devices will probably transform our relationship with the physical world and the way we live and behave in the future. History shows us that security will lag far behind adoption, and we'll have to deal with those consequences when they arrive. At present, we must keep questioning the security risks of consumer devices and mitigating them where we can. Sometimes it might be best to operate a new toy as a dumb device or even return it to the store.

## References

1. K. Hafner and J. Markoff, *Outlaws and Hackers on the Computer Frontier*, Touchstone Press, 1991.
2. House Energy and Commerce Committee Hearing, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, 16 Nov. 2016; https://energycommerce.house.gov/hearings-and-votes/hearings/understanding-role-connected-devices-recent-cyber-attacks.
3. P. Lamkin, "Connected Cooking: The Best Smart Kitchen Devices and Appliances," *Wareable*, 1 Dec. 2016; https://www.wareable.com/smart-home/best-smart-kitchen-devices.
4. Medix, "Top 10 Implantable Wearables Soon to Be in Your Body," *WT VOX*, 27 Oct. 2015; https://wtvox.com/3d-printing/top-10-implantable-wearables-soon-body.
5. H. Tsukayama, "These Smart TVs Were Apparently Spying on Their Owners," *The Washington Post*, 6 Feb. 2016; https://www.washingtonpost.com/news/the-switch/wp/2017/02/06/these-smart-tvs-were-apparently-spying-on-their-owners.
6. J. Leyden "Samsung Smart Fridge Leaves Gmail Logins Open to Attack," *The Register*, 24 Aug 2015; www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar.
7. J. Swearingen, "Can an Amazon Echo Testify Against You?" *New York Mag.*, 27 Dec. 2016; http://nymag.com/selectall/2016/12/can-an-amazon-echo-testify-against-you.html.
8. A. Greenberg, "Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles," *Wired*, 4 Aug. 2016; https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles.
9. E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," *Proc. IEEE European Symp. Security and Privacy*, 2016; doi:10.1109/EuroSP.2016.13.
10. FDA Safety Communication, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter," 9 Jan. 2017; www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.
11. DigiCert, "DigiCert Launches Digital Certificate Auto-Provisioning for IoT Devices," 6 Feb. 2017; https://www.digicert.com/news/2017-02-06-digicert-launches-auto-provisioning-for-iot-devices.htm.
12. E. Brown, "21 Open Source Projects for IoT," *Linux.com*, 20 Sept. 2016; https://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTS-IOT.

**Hilarie Orman** is a security consultant and president of Purple Streak. Her research interests include applied cryptography, secure operating systems, malware identification, security through semantic computing, and personal data mining. Orman has a BS in mathematics from the Massachusetts Institute of Technology. She's a former chair of the IEEE Computer Society's Technical Committee on Security and Privacy. Contact her at hilarie@purplestreak.com.