Two computer scientists explain how the Internet of Things can violate your privacy

March 14 2022, by Roberto Yus, Primal Pappachan

The Nest smart thermostat tracks your presence and is connected to the internet. Credit: Smart Home Perfected/Flickr, CC BY

Have you ever felt a creeping sensation that someone's watching you? Then you turn around and you don't see anything out of the ordinary. Depending on where you were, though, you might not have been completely imagining it. There are billions of things sensing you every day. They are everywhere, hidden in plain sight—inside your TV, fridge, car and office. These things know more about you than you might imagine, and many of them communicate that information over the internet.

Back in 2007, it would have been hard to imagine the revolution of useful apps and services that smartphones ushered in. But they came with a cost in terms of intrusiveness and loss of privacy. As computer scientists who study data management and privacy, we find that with internet connectivity extended to devices in homes, offices and cities, privacy is in more danger than ever.

Internet of Things

Your appliances, car and home are designed to make your life easier and automate tasks you perform daily: switch lights on and off when you enter and exit a room, remind you that your tomatoes are about to go bad, personalize the temperature of the house depending on the weather and preferences of each person in the household.

To do their magic, they need the internet to reach out for help and correlate data. Without internet access, your smart thermostat can collect data about you, but it doesn't know what the weather forecast is, and it isn't powerful enough to process all of the information to decide what to do.

But it's not just the things in your home that are communicating over the internet. Workplaces, malls and cities are also becoming smarter, and the smart devices in those places have similar requirements. In fact, the

Internet of Things (IoT) is already widely used in transport and logistics, agriculture and farming, and industry automation. There were around 22 billion internet-connected devices in use around the world in 2018, and the number is projected to grow to over 50 billion by 2030.

What these things know about you

Smart devices collect a wide range of data about their users. Smart security cameras and smart assistants are, in the end, cameras and microphones in your home that collect video and audio information about your presence and activities. On the less obvious end of the spectrum, things like smart TVs use cameras and microphones to spy on users, smart lightbulbs track your sleep and heart rate, and smart vacuum cleaners recognize objects in your home and map every inch of it.

Sometimes, this surveillance is marketed as a feature. For example, some Wi-Fi routers can collect information about users' whereabouts in the home and even coordinate with other smart devices to sense motion.

Manufacturers typically promise that only automated decision-making systems and not humans see your data. But this isn't always the case. For example, Amazon workers listen to some conversations with Alexa, transcribe them and annotate them, before feeding them into automated decision-making systems.

But even limiting access to personal data to automated decision making systems can have unwanted consequences. Any private data that is shared over the internet could be vulnerable to hackers anywhere in the world, and few consumer internet-connected devices are very secure.

Understand your vulnerabilities

With some devices, like smart speakers or cameras, users can

occasionally turn them off for privacy. However, even when this is an option, disconnecting the devices from the internet can severely limit their usefulness. You also don't have that option when you're in workspaces, malls or smart cities, so you could be vulnerable even if you don't own smart devices.

Therefore, as a user, it is important to make an informed decision by understanding the trade-offs between privacy and comfort when buying, installing and using an internet-connected device. This is not always easy. Studies have shown that, for example, owners of smart home personal assistants have an incomplete understanding of what data the devices collect, where the data is stored and who can access it.

Governments all over the world have introduced laws to protect privacy and give people more control over their data. Some examples are the European General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Thanks to this, for instance, you can submit a Data Subject Access Request (DSAR) to the organization that collects your data from an internet-connected device. The organizations are required to respond to requests within those jurisdictions within a month explaining what data is collected, how it is used within the organization and whether it is shared with any third parties.

Limit the privacy damage

Regulations are an important step; however, their enforcement is likely to take a while to catch up with the ever-increasing population of internet-connected devices. In the meantime, there are things you can do to take advantage of some of the benefits of internet-connected without giving away an inordinate amount of personal data.

If you own a smart device, you can take steps to secure it and minimize risks to your privacy. The Federal Trade Commission offers suggestions

on how to secure your internet-connected devices. Two key steps are updating the device's firmware regularly and going through its settings and disabling any data collection that is not related to what you want the device to do. The Online Trust Alliance provides additional tips and a checklist for consumers to ensure safe and private use of consumer internet-connected devices.

If you are on the fence about purchasing an internet-connected device, find out what data it captures and what the manufacturer's data management policies are from independent sources such as Mozilla's Privacy Not Included. By using this information, you can opt for a version of the smart device you want from a manufacturer that takes the privacy of its users seriously.

Last but not least, you can pause and reflect on whether you really need all your devices to be smart. For example, are you willing to give away information about yourself to be able to verbally command your coffee machine to make you a coffee?

Provided by The Conversation

Citation: Two computer scientists explain how the Internet of Things can violate your privacy (2022, March 14) retrieved 23 March 2023 from https://techxplore.com/news/2022-03-scientists-internet-violate-privacy.html