STREET LEVEL SURVEILLANCE

POLICE ACCESS TO IOT DEVICES

Long gone are the days when our computers were the only electronic devices in the house connected to the rest of the world via the internet. Now, everything from refrigerators to robot vacuum cleaners can be accessed via apps from anywhere in the world. This is often called "the internet of things" (IoT).

A privacy problem is that many of these IoT devices store personal data not locally on the device itself, or solely on-device, but instead on a remote company server somewhere, where it can be accessed by many individuals and entities, including law enforcement. Perhaps most concerning are networked devices that collect and store video and audio from in and around our homes, some in real-time. But lots of other IoT data might be of interest to police. For example, data from our networked thermostat or refrigerator might show whether we were home at a relevant time. That's enough to make a person feel very vulnerable in their own home.

It is bad enough that police are going to IoT companies in order to get data about our lives. Even worse, some of these IoT companies have chosen to build police involvement into their infrastructure. Especially with internet-connected consumer devices specifically geared toward surveillance, companies have built systems that facilitate police requesting data to aid in investigations. For example, companies catering to

in “emergency” circumstances, without a warrant or customer permission.

As of January 2021, 18% of U.S. homes have a surveillance doorbell. This is probably one of the largest networked surveillance systems in the country. As such, it’s necessary to dive a bit deeper to understand how IoT devices can enable a massive step forward for police surveillance.

How it works

Consumer IoT devices are connected to the internet. Some may be connected to one another–for instance if an electronic assistant like an Echo or Alexa can dim the lights in your house or turn your television on. Some can be controlled by an app. Others are controlled just by speaking out loud–meaning the microphone is always at least somewhat active waiting for the command word.

Some IoT security devices with both video and audio capabilities, like Amazon Ring doorbells, are triggered by motion. This activates both a camera and a microphone, which record the incident. The data is uploaded to remote company servers. Even without a motion-triggered event, users can use the app in real-time to look through, listen through, or talk through their device.

How Law Enforcement Use of the Internet of Things

SOURCE: EFF

A Ring doorbell camera

As of 2019, it was reported that 69% of U.S. homes had at least one IoT device.That means a tremendous amount of data in a majority of homes is potentially available to police to aid in investigations. Indeed, police have sought data from a person's Fitbit fitness tracker and from a Google Nest home thermostat. And make no mistake, where any data is collected on individuals, eventually police will come looking for it.

Police can get data from your IoT home devices in a number of ways. If police see a doorbell camera or security camera pointed at a crime scene, they can walk up to a person's door and request the footage. This can also happen digitally, with police emailing or having the manufacturer email the user to request footage. Such emails might go out en masse to many users at once. If there is no warrant, you always have the right to say "no." If police get a warrant, they can present it to the device's owner if the data is stored on-device, or to the company if the data is stored on a company server.

data to the police. Finally, some companies have a specialized form for police to request data directly from the company in an emergency, without a warrant or the consent of the user—as with Amazon Ring cameras.

Who Sells the Internet of Things

A vast number of technology and electronics companies now sell networked and internet-connected devices that collect user data, and sometimes even non-user data. Many users try to keep track of which ones control their data to evaluate whether they trust them or not. A challenge in doing so is the frequency that these IoT companies are bought and sold to one another. One example is the recent attempted sale of iRobot, the makers of the popular IoT vacuum Roomba, to Amazon–a company with a controversial past of working with law enforcement to hand over Ring doorbell camera data. This deal prompted fears that Amazon would inherit maps of people's homes–something that might be useful considering its own home robot devices and surveillance-based indoor drone.

Threats Posed by the Internet of Things

Police access to our IoT data stored in company servers, including audio and video recordings, is a large expansion of government surveillance. Absent necessary safeguards, including rigorous enforcement of the warrant requirement, unencrypted data collected inside your home would be stored in one of the largest police evidence lockers in history–the servers of IoT companies.

The ubiquity of these devices could lead to a world where there are large portions of a person's house, yard, and neighborhood where they don't feel comfortable having sensitive conversations. They may fear their conversation could be recorded and stored on a company server, ready for police access.

EFF's Work Related to the Internet of Things

EFF has worked tirelessly to make sure these companies protect your data and secure their devices. We pushed Ring to introduce end-to-end encryption for footage, which they did in early 2021. This increased user power to limit police access to their footage.

once to request footage, a policy they changed in June 2021. We also continue to push to make sure big tech companies use their considerable resources to fight overly broad warrants when law enforcement sends them. (We also discovered that the Amazon Ring app was full of undisclosed third-party trackers and pressured the company to stop.)

But the fight to make consumer IoT devices more privacy-oriented is far from over.

Suggested Additional Reading

When Police Surveillance Meets the 'Internet of Things' (Brennan Center)

TECHNOLOGIES