Are your devices spying on you? Australia's very small step to make the Internet of Things safer

11 September 2020, by Kayleen Manwaring

Credit: Shutterstock

From internet-connected televisions, toys, fridges, ovens, security cameras, door locks, fitness trackers and lights, the so-called "Internet of Things" (IoT) promises to revolutionize our homes.

But it also threatens to increase our vulnerability to malicious acts. Security flaws in IoT devices are common. Hackers can exploit those vulnerabilities to take control of devices, steal or change data, and spy on us.

In recognition of these risks, the Australian government has introduced a new code of practice to encourage manufacturers to make IoT devices more secure. The code provides guidance on secure passwords, the need for security patches, the protection and deletion of consumers' personal data and the reporting of vulnerabilities, among other things.

The problem is the code is voluntary. Experiences elsewhere, such as the United Kingdom, suggest a voluntary code will be insufficient to deliver the protections consumers need.

Indeed it might even increase risks, by lulling consumers into a false sense of security about the safety of the devices they buy.

Many IoT devices are insecure

IoT devices designed for consumers are generally less secure than conventional computers.

In 2017 the Australian Communications Consumer Action Network commissioned researchers from the University of New South Wales to test the security of 20 household appliances capable of being connected and controlled via wi-fi.

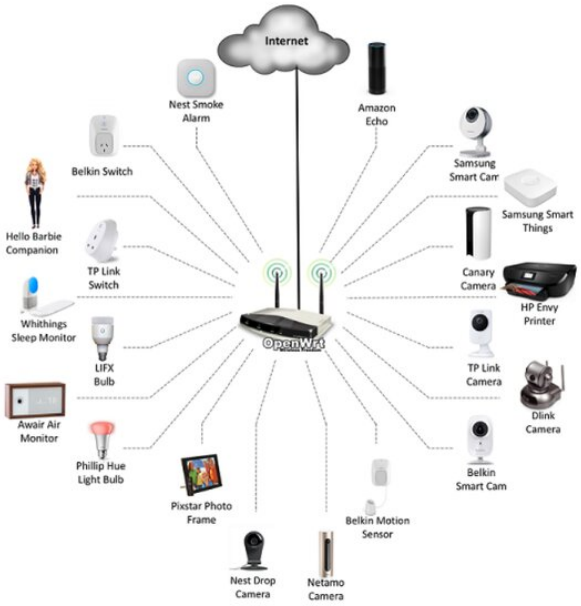
These included a smart TV, portable speaker, voice assistant, printer, sleep monitor, digital photo frame, bathroom scales, light bulb, power switch, smoke alarm and Hello Barbie talking doll.

While some devices (including the Barbie) were found to be relatively secure in terms of confidentiality, all had some form of security flaw. Many "allowed potentially serious safety and security breaches."

What this could potentially mean is that someone could, for example, hack into a household's wi-fi network and collect data from IoT devices. It might be as simple as knowing when lights are switched on to determine when a home can be burgled. Someone with more malicious intent could turn on your oven while shutting down smoke alarms and other sensors.

Risks to consumers, and society

Factors leading to poor security in IoT devices include manufacturers' desires to minimize componentry and keep costs down. Many makers of consumer goods also have little experience with cyber-security issues.



Devices tested by UNSW researchers for the Australian Communications Consumer Action Network. Credit: Inside Job: Security and privacy threats for smart-home IoT devices, 2017, CC BY-NC

Allied with the fact many consumers aren't technologically savvy enough to appreciate the risks and protect themselves, this creates the prospect of IoT devices being exploited.

On a personal level, you could be spied on and harassed. Personal pictures or information could be exposed to the world, or used to extort you.

On a societal level, IoT devices can be hijacked and used collectively to shut down services and networks. Even compromising one device may enable connected infrastructure to be hacked. This is a rising concern as more people connect to workplace networks from home.

Voluntary codes of practice

In recognition of these threats, IoT security "good practice" guidelines have been proposed by standards bodies such as the US National Institute of Standards and Technology, the European Telecommunications Standards Institute and the Internet Engineering Task Force. But these guidelines are based on voluntary action by manufacturers.

The UK government has already concluded the voluntary code of conduct it established in 2018 isn't working.

Britain's Minister for Digital Infrastructure, Matt Warman, said in July: "Despite widespread adoption of the guidelines in the Code of Practice for Consumer Internet of Things Security, both in the UK and overseas, change has not been swift enough, with poor security still commonplace."

The UK is now moving to impose a mandatory code, with laws requiring manufacturers to deliver reasonable security features in any device that can connect to the internet.

A case for co-regulation

There is little reason to believe Australia's voluntary code of practice will prove any more effective than in the UK.

A better option would have been a "co-regulatory" approach. Co-regulation mixes aspects of industry self-regulation with both government regulation and strong community input. It includes laws that create incentives for compliance (and disincentives against non-compliance) and regulatory oversight by an independent (and well-resourced) watchdog.

The Australia government has, at least, described its new code of practice as "a first step" to improving the security of IoT devices.

Let's hope so. If the UK experience is anything to go by, its next steps will include dumping a voluntary code for something with a greater chance of delivering the safety and security consumers—and society—need.

Provided by The Conversation