THE CONVERSATION
Academic rigour, journalistic flair

Six things every consumer should know about the ‘Internet of Things’

June 8, 2017 6.11am AEST

What happens if your smart kettle is hacked? Shutterstock

Author

Kayleen Manwaring
Lecturer, School of Taxation & Business Law, UNSW

At least 40% of Australian households now have at least one home “Internet of Things” device. These are fridges, window blinds, locks and other devices that are connected to the internet.

While the Internet of Things (IoT) may lead to more efficiency in our daily lives, my research shows that consumers are exposed to many risks by the use of IoT devices, ranging from disclosure of private information, to physical injury and problems with the devices themselves.

Australia has no specific laws aimed at addressing IoT issues, and current laws intended to protect consumers have gaps and uncertainties when dealing with IoT devices.

1) Your devices can spy on you (and your kids)

Many IoT device manufacturers and suppliers show little regard for customers’ privacy. Some even make money from customer data.

Consumer electronics company Vizio recently agreed to pay US regulators US$2.2 million, after allegedly failing to get appropriate consent from users to track their TV viewing habits.

Late last year, the Norwegian Consumer Council found that a children's doll recorded anything said to it by children and sent the recordings to a US company. The company reserved the right to share and use the data for a broad range of purposes.

2) Many IoT devices are vulnerable to hacking

The same doll was also found to have a security flaw that allowed strangers to talk and listen through the doll. Security vulnerabilities such as these can be exploited to cause damage in both the physical and virtual worlds.

IoT devices were recently involved in some of the largest "distributed-denial-of-service" attacks - flooding websites with traffic until they crash. The recent huge attacks on internet company Dyn and on the security researcher Brian Krebs were in large part fuelled by hacked IoT devices.

But hacked IoT devices can also be dangerous by themselves. In 2015 Fiat Chrysler recalled 1.4 million vehicles when security researchers proved they could break into smart cars' systems remotely and control brakes, steering and transmission.

3) Your devices are never really yours, even after you pay for them

Most IoT devices come with some form of embedded software, and the devices won't work properly - or sometimes at all - without it. This software is usually licensed, not sold, and the conditions imposed through licence agreements can hinder users' repairing, modifying or reselling their devices.

This can be anti-competitive, as individual users are effectively "locked in" to one brand and one supplier.

For several years now, US farmers have been in a dispute with agricultural machinery manufacturers such as John Deere, over their rights to repair tractors that contain embedded software.

The farmers were granted a three-year exemption to certain copyright laws in 2015. However, John Deere is fighting back.

In October 2016, the company issued a new licence agreement which prohibits almost all software modification on its tractors. This action appears to be an attempt to ensure all repairs are done by John Deere contractors.

4) Your devices know your weaknesses

IoT devices have the potential to collect more intimate data about individuals than was possible with previous devices. This data can then be used to create profiles that give incredible insight into consumers, and can even predict their behaviour.

For a number of years now we've known that the embedded technology in smartphones can be used to detect users' mood, stress levels, personality type etc.

But some IoT devices can collect even more intimate and personalised data. This was evident after a recent out-of-court settlement by a wireless vibrator manufacturer allegedly collecting data without consent.

The consumer profiles that can be built with all this data can then be used to sell us products at times when our willpower is lowest. Retailers are currently using technology to track consumers through stores and send customised messages to mobile phones. This may be linked to our purchase history and what is known about our mood.

5) It's almost impossible to know what you're getting yourself into, or how long it will last

Many IoT products are complex hybrids of software, hardware and services, often provided by more than one supplier. What your rights are when things go wrong, and who best to fix it for you, can be hard to figure out.

A recent investigation of the Nest thermostat system revealed that if consumers wanted to understand all of the rights and obligations of those in the supply chain, they needed to read a minimum of 13 different contractual documents.

Even if you know and trust your supplier, they may not be around forever. And when they go, services essential to their products working may disappear as well.

Revolv, a maker of home automation devices, was shut down after the company was acquired by Nest, which was itself acquired by Google. Nest refused to support Revolv's products, and they stopped working less than two years after being released.

6) The law may not protect you

Many IoT devices put consumer privacy at risk, but the Privacy Act has significant limitations, as the definition of "personal information" is very narrow. The Act doesn't even apply to many Australian companies, as they do not meet thresholds such as having A$3 million in annual turnover.

Consumers and regulators may attempt to pursue device suppliers under the consumer guarantees in the Australian Consumer Law. But there are grey areas here too. We don't know what "acceptable quality" is when it comes to some of these devices, for instance. Is an internet-connected kettle that boils water perfectly well, but can be easily hacked, of acceptable quality?

Proceed with caution

Consumers are exposed to significant risks from IoT devices, from predatory use of data, to security flaws and devices no longer being supported. Meanwhile Australia has no specific laws aimed at addressing these IoT issues.

The most recent review of the Australian Consumer Law recommended investigating "emerging technologies" be made a priority. It is vital that a close examination of consumer protection relating to

IoT devices be included front-and-centre in this project.

In the meantime, consumers should think long and hard about the risks they are taking on with IoT devices. Do you really need that internet-connected hairbrush?

Privacy Internet of Things Consumer protection Consumer law Australian Consumer Law