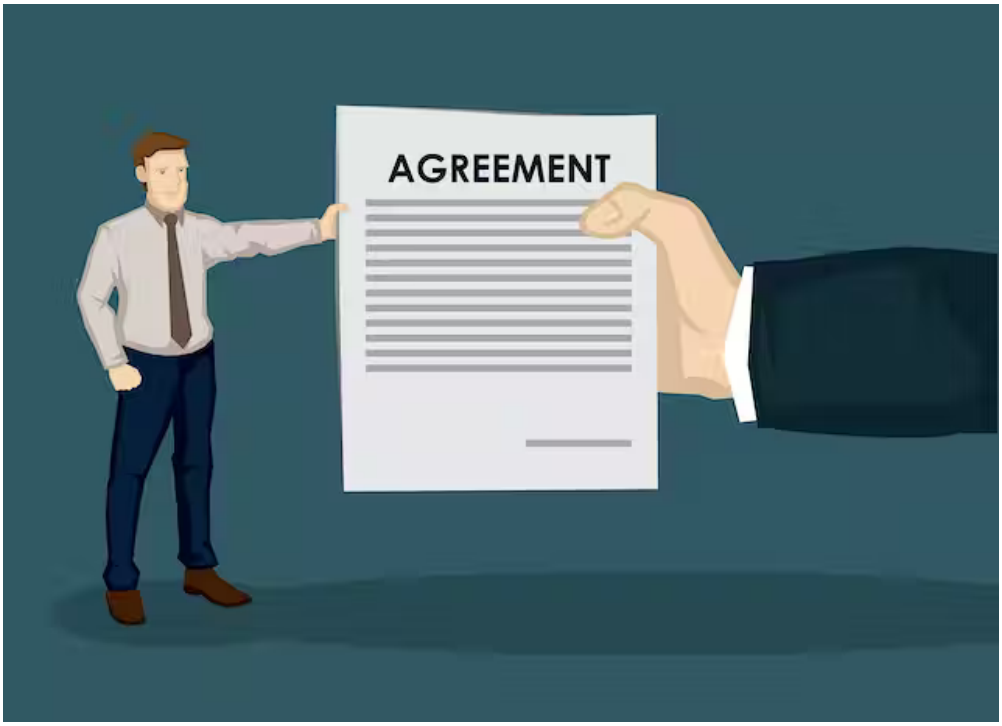
THE CONVERSATION

Academic rigour, journalistic flair



Shutterstock

The privacy paradox: we claim we care about our data, so why don’t our actions match?

Published: July 29, 2020 5.49am BST

Ivano Bongiovanni
Lecturer in Information Security, Governance and Leadership / Design Thinking, The University of Queensland

Karen Renaud
Visiting Professor, Rhodes University

Noura Aleisa
Assistant professor of Computer Science, Saudi Electronic University

Imagine how you’d feel if you discovered footage from your private home security camera had been broadcast over the internet. This is exactly what happened to several unsuspecting Australians last month, when the website Insecam streamed their personal lives online.

According to an ABC report, Insecam broadcasts live streams of dozens of Australian businesses and homes at any given time. Some cameras can be accessed because owners don’t secure them. Some may be hacked into despite being “secured”.

When asked if they care about their personal information being shared online, most people say they do. A 2017 survey found 69% of Australians were more concerned about their online privacy than in 2012.

However, a much smaller percentage of people actually take the necessary actions to preserve their privacy. This is referred to as the “privacy paradox”, a concept first studied about two decades ago.

To investigate this phenomenon further, we conducted a research project and found that, despite being concerned about privacy, participants were willing to sacrifice some of it in exchange for the convenience afforded by an internet-connected device.

Unpacking the privacy paradox

Any “smart” device connected to the internet is called an Internet of Things (IoT) device. These can be remotely monitored and controlled by the owners.

The projected growth of IoT devices is staggering. By 2025, they’re expected to reach 75.44 billion – an increase of 146% from 2020.

The global IoT network is a collection of all the interconnected devices that can communicate online. This includes smart devices, appliances and wearable tech. Shutterstock

Are device owners genuinely concerned about their privacy? Recent worldwide anxiety about personal information shared through COVID-19 tracing apps seems to suggest so.

But as the privacy paradox highlights, users expressing privacy concerns often fail to act in accordance with them. They freely divulge personal information in exchange for services and convenience.

Explanations for the privacy paradox abound. Some suggest:

- people find it difficult to associate a specific value to their privacy and therefore, the value of protecting it
- people do not consider their personal information to be their own and thus might not appreciate the need to secure it

- people completely lack awareness of their right to privacy or privacy issues and believe their desired goals (such as a personalised experience) outweigh the potential risks (such as big tech companies using their data for profiling).

The likely explanation for the privacy paradox is a mix of all these factors.

Read more: How Facebook uses the 'privacy paradox' to keep users sharing

---

What if we *proved* your device harvests data?

To understand whether and how the privacy paradox applies to IoT devices, we conducted an experiment involving 46 Saudi Arabian participants. This is because in Saudi Arabia the use of IoT is exploding and the country does not have strong privacy regulations.

We gave participants a smart plug that let them switch a table lamp on or off using an app on their smartphone. We then showed them the device's privacy policy and measured participants' privacy concerns and trust in the device.

None of the participants read the privacy policy. They simply agreed to commence with the study.

After two hours, we presented evidence of how much of their data the IoT-connected plug was harvesting, then remeasured their privacy concerns and trust.

After the participants saw evidence of privacy violation, their privacy concerns increased and trust in the device decreased. However their behaviour did not align with their concern, as shown by the fact that:

- 15 participants continued to use the device regardless
- 13 continued to use it with their personal information removed
- only three opted to block all outbound traffic to unusual IP addresses.

The rest preferred "light-touch" responses, such as complaining on social media, complaining to the device's manufacturer or falsifying their shared information.

After one month, we measured participants' attitudes a third time and discovered their privacy concerns and trust in the device had reverted to pre-experiment levels.

How to prevent complacency

Two decades since the first privacy paradox studies were conducted and despite a great deal of research, there is still a mismatch between people's stated privacy concerns and their protective behaviours. How can we improve this?

Every time you connect a new device to the internet, or opt-in to a new service, ask yourself: ‘do I really need this?’
Shutterstock

The first step is to simply be aware our judgement of IoT device risks and benefits may not be accurate. With that in mind, we should always take time to read the privacy policies of our devices.

Besides informing us of the risks, reading privacy policies can help us *stop* and *think* before connecting a new device to the internet. Ask yourself: “is this really going to benefit me?”

As citizen surveillance increases, it’s not wise to mindlessly scroll through privacy policies, tick a box and move on.

Read more: The ACCC is suing Google for misleading millions. But calling it out is easier than fixing it

---

Second, we should not assume our personal information is trivial and would not interest anyone. Time after time we have witnessed how our digital traces can be valuable to malicious individuals or large corporations.

And finally, always change the default password on any new IoT device to a stronger one. Write down this password and secure it, perhaps with other physical valuables, so you don’t have to worry about forgetting it.

Simon Willison · Dec 13, 2019
@simonw · **Follow**
Replying to @simonw

To their credit, they do at least recommend two-factor authentication... though it looks like it's only SMS based, hence vulnerable to SIM-jacking support.ring.com/hc/en-us/artic...

Simon Willison
@simonw · **Follow**

Hacking into Ring cameras is so easy there's a podcast that does it

vice.com
Inside the Podcast that Hacks Ring Camera Owners Live on Air
In the NulledCast hackers livestream the harassment of Ring camera owners after accessing their devices. Hundreds of people can listen.

12:34 AM · Dec 13, 2019

2 **Reply** **Copy link**

Read 1 reply