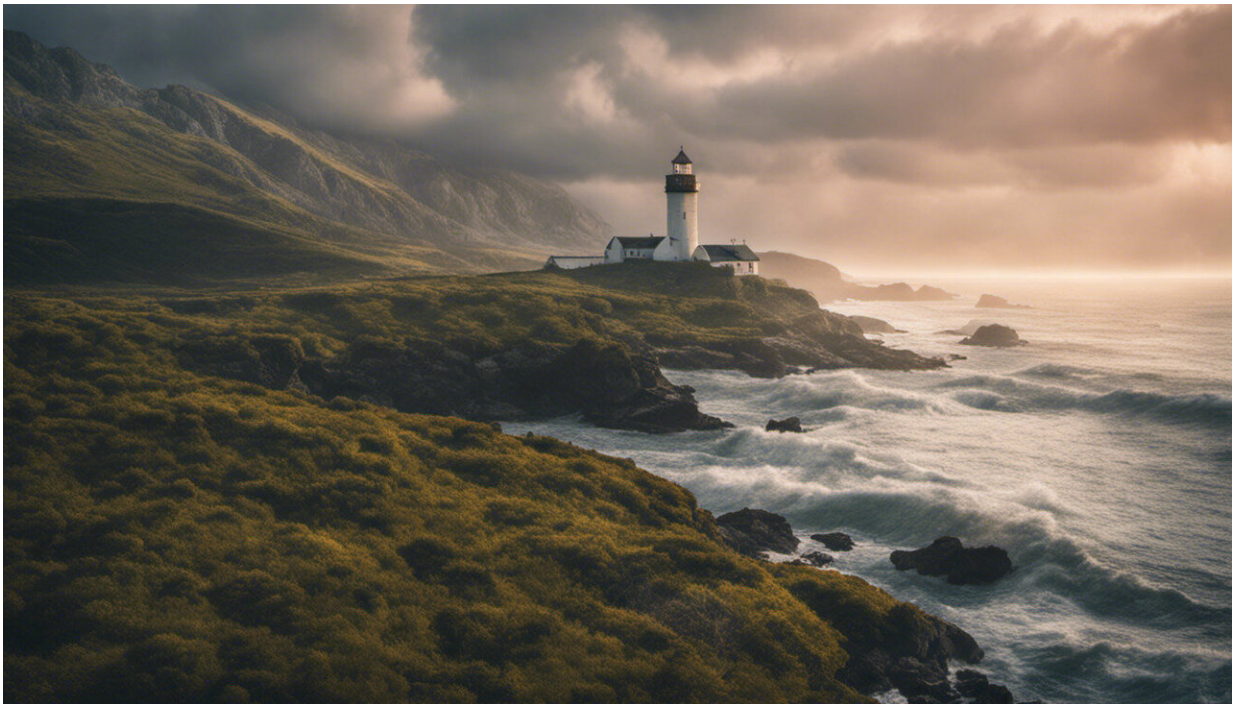# You may be sick of worrying about online privacy, but 'surveillance apathy' is also a problem

November 8 2017, by Siobhan Lyons

Credit: AI-generated image ([disclaimer](#))

We all seem worried about privacy. Though it's not only privacy itself we should be concerned about: it's also our *attitudes* towards privacy that are important.

When we stop caring about our digital privacy, we witness surveillance apathy.

And it's something that may be particularly significant for marginalised communities, who feel they hold no power to navigate or negotiate fair use of digital technologies.

In the wake of the NSA leaks in 2013 led by Edward Snowden, we are more aware of the machinations of online companies such as Facebook and Google. Yet research shows some of us are apathetic when it comes to online surveillance.

Privacy and surveillance

Attitudes to privacy and surveillance in Australia are complex.

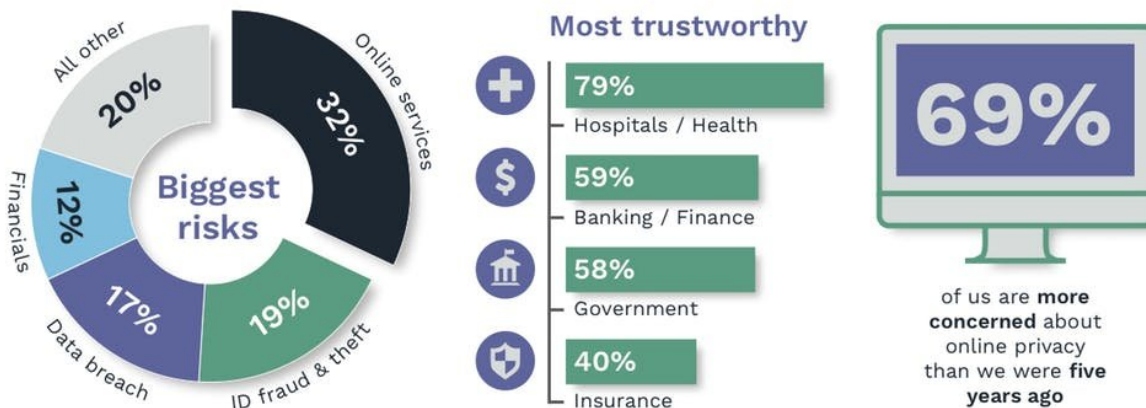According to a major 2017 privacy survey, around 70% of us are more concerned about privacy than we were five years ago.

And yet we still increasingly embrace online activities. A 2017 report on social media conducted by search marketing firm Sensis showed that almost 80% of internet users in Australia now have a social media profile, an increase of around ten points from 2016. The data also showed that Australians are on their accounts more frequently than ever before.

Also, most Australians appear not to be concerned about recently proposed implementation of facial recognition technology. Only around one in three (32% of 1,486) respondents to a Roy Morgan study expressed worries about having their faces available on a mass database.

A recent ANU poll revealed a similar sentiment, with recent data retention laws supported by two thirds of Australians.

Australian Community Attitudes to Privacy Survey 2017

······ People believe online services are the biggest privacy risk ·······

Biggest risks

- Online services 32%
- All other 20%
- Financials 12%
- Data breach 17%
- ID fraud & theft 19%

Most trustworthy

- 79% — Hospitals / Health
- 59% — Banking / Finance
- 58% — Government
- 40% — Insurance

69% of us are **more concerned** about online privacy than we were **five years ago**

······ Security concerns mean ······

93% don't want their data to be sent overseas

79% don't want their data shared with other organisations

58% decided not to deal with some businesses

44% avoid downloading smartphone apps

······ We could take more responsibility ······

61% check website security before giving personal information...

but we don't usually

- Read privacy policies — 65%
- Ask organisations why? — 54%
- Clear browsing history — 50%
- Shred documents — 50%
- Adjust privacy settings — 43%

HANDLE WITH CARE ✈ **VISIT WWW.PRIVACY.GOV.AU**

Australian Government
Office of the Australian Information Commissioner

napshot of Australian community attitudes to privacy 2017. Credit: Office of the Australian Information Commissioner

So while we're aware of the issues with surveillance, we aren't necessarily doing anything about it, or we're prepared to make compromises when we perceive our safety is at stake.

Across the world, attitudes to surveillance vary. Around [half of Americans](#) polled in 2013 found [mass surveillance](#) acceptable. France, Britain and the Philippines appeared more tolerant of mass surveillance compared to Sweden, Spain, and Germany, according to [2015 Amnesty International data](#).

Apathy and marginalisation

In 2015, philosopher Slavoj Žižek [proclaimed](#) that he did not care about surveillance (admittedly though suggesting that "perhaps here I preach arrogance").

This position cannot be assumed by all members of society. Australian academic Kate Crawford [argues](#) the impact of data mining and surveillance is more significant for marginalised communities, including people of different races, genders and socioeconomic backgrounds. American academics Shoshana Magnet and Kelley Gates agree, [writing](#):

"[…] new surveillance technologies are regularly tested on marginalised communities that are unable to resist their intrusion."

A [2015 White House report](#) found that big data can be used to

perpetuate price discrimination among people of different backgrounds. It showed how data surveillance "could be used to hide more explicit forms of discrimination".

According to Ira Rubinstein, a senior fellow at New York University's Information Law Institute, ignorance and cynicism are often behind surveillance apathy. Users are either ignorant of the complex infrastructure of surveillance, or they believe they are simply unable to avoid it.

As the White House report stated, consumers "have very little knowledge" about how data is used in conjunction with differential pricing.

So in contrast to the oppressive panopticon (a circular prison with a central watchtower) as envisioned by philosopher Jeremy Bentham, we have what Siva Vaidhyanathan calls the "crytopticon". The crytopticon is "not supposed to be intrusive or obvious. Its scale, its ubiquity, even its very existence, are supposed to go unnoticed".

Credit: AI-generated image ([disclaimer](#))

But Melanie Taylor, lead artist of the computer game Orwell (which puts players in the role of surveillance) [noted](#) that many simply remain indifferent despite heightened awareness:

"That's the really scary part: that Snowden revealed all this, and maybe nobody really cared."

The Facebook trap

Surveillance apathy can be linked to people's dependence on "the system". As one of my media students pointed out, no matter how much awareness users have regarding their social media surveillance, invariably people will continue using these platforms. This is because

they are convenient, practical, and "we are creatures of habit".

As University of Melbourne scholar Suelette Dreyfus noted in a [Four Corners](#) report on Facebook:

"Facebook has very cleverly figured out how to wrap itself around our lives. It's the family photo album. It's your messaging to your friends. It's your daily diary. It's your contact list."

This, along with the complex algorithms Facebook and Google use to collect and use data to produce "[filter bubbles](#)" or "[you loops](#)" is another issue.

Protecting privacy

While some people are attempting to [delete themselves](#) from the network, others have come up with ways to avoid being tracked online.

Search engines such as [DuckDuckGo](#) or [Tor Browser](#) allow users to browse without being tracked. [Lightbeam](#), meanwhile, allows users to see how their information is being tracked by third party companies. And MIT devised a system to show people the metadata of their emails, called [Immersion](#).

Surveillance apathy is more disconcerting than surveillance itself. Our very attitudes about privacy will inform the structure of surveillance itself, so caring about it is paramount.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation