

Australia should strengthen its privacy laws and remove exemptions for politicians

Written by David Vaile, Teacher of cyberspace law, UNSW

As revelations [continue to unfold](#) about the misuse of personal data by Cambridge Analytica, many Australians are [only just learning](#) that Australian politicians have given themselves a free kick to [bypass privacy laws](#).

Indeed, Australian data privacy laws are generally weak when compared with those in the United States, the United Kingdom and the European Union. They fall short in both specific exemptions for politicians, and because individuals cannot enforce laws even where they do exist.

Read more: [*Australia's privacy laws gutted in court ruling on what is 'personal information'*](#)

While Australia's major political parties have [denied](#) using the services of Cambridge Analytica, they do engage in substantial data operations – including the Liberal Party's [use of the i360 app](#) in the recent South Australian election. How well this microtargeting of voters works to sway political views is [disputed](#), but the claims are credible enough to spur demand for these tools.

Greens leader Richard di Natale told [RN Breakfast](#) this morning that political parties “shouldn't be let off the hook”:

All political parties use databases to engage with voters, but they're exempt from privacy laws so there's no transparency about what anybody's doing. And that's why it's really important that we go back, remove those exemptions, ensure that there's some transparency, and allow people to decide whether they think it's appropriate.

Why should politicians be exempt from privacy laws?

The exemption for politicians was introduced way back in the [Privacy Amendment \(Private Sector\) Bill 2000](#). The Attorney-General at the time, Daryl Williams, justified the exemption on the basis that freedom of political communication was vital to Australia's democratic process. He said the exemption was:

...designed to encourage that freedom and enhance the operation of the electoral and political process in Australia.

Malcolm Crompton, the then Privacy Commissioner, argued against the exemption, stating that political institutions:

...should follow the same practices and principles that are required in the wider community.

Other politicians from outside the two main parties, such as Senator Natasha Stott Despoja in 2006, have tried to remove the exemptions for similar reasons, but failed to gain support from the major parties.

What laws are politicians exempt from? Privacy Act

The [Privacy Act](#) gives you control over the way your personal information is handled, including knowing why your personal information is being collected, how it will be used, and to whom it will be disclosed. It also allows to you to make a complaint (but not take legal action) if you think your personal information has been mishandled.

“Registered political parties” are [exempt from the operation of the Privacy Act 1998](#), and [so are](#) the political “acts and practices” of certain entities, including:

Australia should strengthen its privacy laws and remove exemptions for politicians

Written by David Vaile, Teacher of cyberspace law, UNSW

- political representatives — MPs and local government councillors;
 - contractors and subcontractors of registered political parties and political representatives;
- and
- volunteers for registered political parties.

This means that if a company like Cambridge Analytica was contracted to a party or MP in Australia, their activities may well be exempt.

Read more: [*Is there such a thing as online privacy? 7 essential reads*](#)

Spam Act

Under the [Spam Act 2003](#) , organisations cannot email you advertisements without your request or consent. They must also include an unsubscribe notice at the end of a spam message, which allows you to opt out of unwanted repeat messaging. However, the Act says that it has no effect on “implied freedom of political communication”.

Do Not Call Register

Even if you have your number listed on the [Do Not Call Register](#) , a political party or candidate can authorise a call to you, at home or at work, if one purpose is fundraising. It also permits other uses.

How do Australian privacy laws fall short?

No right to sue

Citizens can sue for some version of a breach of privacy in the UK, EU, US, Canada and even New Zealand. But there is still no constitutional or legal right that an individual (or class) can enforce over intrusion of privacy in Australia.

After exhaustive consultations in 2008 and 2014, the Australian Law Reform Commission (ALRC) recommended a modest and carefully limited statutory tort – a right to dispute a serious

breach of privacy in court. However, both major parties effectively rejected the ALRC recommendation.

No 'legal standing' in the US

Legal standing refers to the right to be a party to legal proceedings. As the tech giants that are most adept at gathering and using user data – Facebook, Google, Apple, Amazon – are based in the US, Australians generally do not have legal standing to bring action against them if they suspect a privacy violation. EU citizens, by contrast, have the benefit of the [Judicial Redress Act 2015](#) (US) for some potential misuses of cloud-hosted data.

Poor policing of consent agreements

Consent agreements – such as the terms and conditions you agree to when you sign up for a service, such as Gmail or Messenger – waive rights that individuals might otherwise enjoy under privacy laws. In its response to the Cambridge Analytica debacle, [Facebook claims](#) that users consented to the use of their data.

Read more: [*Consent and ethics in Facebook's emotional manipulation study*](#)

But these broad user consent agreements are not policed strictly enough in Australia. It's known as "bad consent" when protective features are absent from these agreements. By contrast, a "good consent" agreement should be simple, safe and precautionary by default. That means it should be clear about its terms and give users the ability to enforce them, should not be variable, and should allow users to revoke consent at any time.

New laws introduced by the EU – the [General Data Protection Regulation](#) – which come into effect on May 25, are an example of how countries can protect their citizens' data offshore.

Major parties don't want change

Australia should strengthen its privacy laws and remove exemptions for politicians

Written by David Vaile, Teacher of cyberspace law, UNSW

Privacy Commissioner Tim Pilgrim [said today in The Guardian](#) that the political exemption should be reconsidered. In the past, independents and minor party representatives have objected to the exemption, as well as the weakness of Australian privacy laws more generally. In 2001, [the High Court said](#) that there should be a right to sue for privacy breach.

Read more: [Why big data may be having a big effect on how our politics plays out](#)

But both Liberal and Labor are often [in tacit agreement to do nothing substantial](#) about privacy rights. They have not taken up the debates around the collapse of IT security, nor the increase in abuse of the “consent” model, the dangers of so called “open data”, or the threats from artificial intelligence, Big Data, and metadata retention.

One might speculate that this is because they share a vested interest in making use of voter data for the purpose of campaigning and governing. It’s now time for a new discussion about the rules around privacy and politics in Australia – one in which the privacy interests of individuals are front and centre.

David Vaile is Board or Committee Member of Internet Australia, The Australian Privacy Foundation, the Association of Social and Market Research Organisation, and various professional, government and civil society and policy organizations.

Authors: David Vaile, Teacher of cyberspace law, UNSW

Read more <http://theconversation.com/australia-should-strengthen-its-privacy-laws-and-remove-exemptions-for-politicians-93717>