Submission to the Joint Select Committee on Electoral Matters

on the conduct of the

2022 Federal Election

16 September 2022

DIGITAL RIGHTS WATCH

Who we are

Digital Rights Watch was founded in 2016 to fight for a digital world where all humanity can thrive, and where diversity and creativity flourishes.

Our digital world must be underpinned by equality, freedom and established human rights principles. Its evolution and future must be guided and driven by the interests of all people and the environments we live in.

Digital Rights Watch exists to defend and promote this vision – to ensure fairness, freedoms and fundamental rights for all people who engage in the digital world.

We ensure that Australians are equipped, empowered and enabled to uphold their digital rights. We believe that digital rights are human rights which see their expression online.

We conduct research on best practices in protecting privacy and personal information, limiting surveillance overreach, improving digital security, monitoring government use of data and technology and new digital economies and governance systems.

We publish an annual State of Digital Rights report bringing together Australia's leading activists, writers and critical thinkers to reflect on digital rights, identify our weaknesses and failings and chart a new path forward for a freer, fairer digital ecosystem.

Acknowledgement of Country

Digital Rights Watch acknowledges the traditional owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

General remarks

> *"Free elections do not require the absence of regulation. Indeed, regulation of the electoral process is necessary in order that it may operate effectively or at all. Not only that, but some limitations upon freedom of communication are necessary to ensure the proper working of any electoral system."*
>
> *Levy v Victoria (1997) 189 CLR 57*

Digital Rights Watch recognises the important role that an interconnected digital ecosystem has come to play in facilitating and empowering grassroots political engagement. We welcome the opportunity to make a submission to the Joint Select Committee on Electoral Matters regarding the 2022 Federal Election.

We note that the Senate Environment and Communications Legislation Committee had indicated in their 2020 report into the Telecommunications Legislation Amendment (Unsolicited Communications) Bill 2019 that the question of political party exemptions under the *Privacy Act 1998*, *Spam Act 2003* and *Do Not Call Register Act 2006* were better dealt with under this inquiry. We expect this committee to reflect on that committee's comments and address this issue after multiple inquiries have ignored it.

We hope that the current committee takes up that challenge and tackles the question of political party exemptions that have caused everyday Australians significant concern and frustration over the past few years.

Our core concerns are:

- The increasing availability and ubiquity of data-extractive technologies have increased the scale and scope by which harm can be caused to everyday Australians through inappropriate or invasive collection, use and disclosure of their personal information. These harms include invasions of privacy, voter manipulation, and misinformation and disinformation. This stands to weaken our democratic processes and undermine public trust. Political parties have a responsibility to exhibit best practices when it comes to handling data ethically, lawfully, and minimising digital technology facilitated harms to Australians.

- Without appropriate safeguards in place, unregulated access and use of Australians' personal information creates a concerning gap in Australia's approach to cyber security, putting not just individuals at risk, but also our digital security more broadly.

Removing political exemptions from the *Privacy Act 1998*, *Spam Act 2003* and *Do Not Call Register Act 2006* is essential to address these pressing issues.

Misinformation, voter manipulation and safeguarding democracy

These exemptions facilitate intrusive and sometimes harmful spam, notably SMS campaigns by Craig Kelly and Clive Palmer undermining the COVID-19 pandemic response. More insidious however, is how these exemptions facilitate active misinformation online. Over the last decade there has been an explosion in the profiling and targeting individuals for political messaging. Personalised news feeds, ads and other individual-targeted content online can more easily facilitate misinformation at a far larger scale than offline political advertising could possibly achieve.

While most regulatory attention has been put on overseas intrusions into our democratic systems, there are many ways other than hacking to interfere in a country's election. In addition to shoring up their cybersecurity, political parties also need to play a role in safeguarding voters and social media users against potential abuses of personal data for targeted political advertising.

Following the Cambridge Analytica scandal, the United Kingdom Information Commissioner conducted an investigation into personal information and political influence, and the ways it can impact and undermine democratic processes.[1] In it, it highlights that in order "to retain the trust and confidence of electorates and the integrity of the elections themselves, all of the organisations involved in political campaigning must use personal information and these techniques in ways that are transparent, understood by people and lawful." This is every bit as true of Australia as it is of the UK. Australians' trust in the political system and in their political representatives has plummeted in recent years.

Digital Rights Watch recognises the legitimate need for political parties to communicate and engage with voters, as well as the importance of freedom of political communication. It is reasonable and expected for political parties to collect and use personal information of voters for this purpose. We also recognise that methods of communication to engage with voters develop over time in line with advances of digital technology.

However, these practices should be subject to the limitations and protections contained in those Acts to ensure that they are lawful, transparent, and respectful. Free and fair elections are a core tenet of a democratic society, and it is therefore essential that political parties operate from a level playing field, and embody best practices when it comes to handling Australians' data. In doing so, they would be playing a key role in minimising the power of misinformation, disinformation and voter manipulation.

[1] 'Democracy Disrupted? Personal information and political influence', UK ICO, July 2018. Available at: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

Building trust with the Australian public

The exemption of elected officials, political parties, and their contractors, sub-contractors and volunteers not only poses a data security risk but also a major reputational risk for political parties themselves. If political parties are not sure where their contractors and their subcontractors have acquired data from — whether it was collected with the full knowledge and consent of the people the data belongs to; exactly how it is being analysed, shared and used; and whether those uses will be accepted by the public at large — then it is possible that a breach in trust at the scale of Cambridge Analytica could occur in Australia.

The backlash from such an incident would not be limited to the particular political party responsible. The low trust in politicians generally makes it likely that all political parties would face public outrage. This means that political parties should consider not only how confident they are in their own data practices, but how much faith they have in the practices of their opponents. Maintaining public faith in the legitimacy of the democratic process is not a partisan issue.

There is clear public support for removal of these exemptions.

A 2021 survey found that 83% believe that political parties should not be able to contact people on the Do Not Call Register, and 78% think they should not be able to send out automated text messages.[2] With regard to the Privacy Act, the same survey found that 80% are in favour of making political parties subject to the full Privacy Act, and only 5% are against.[3] Similarly, the Office of the Australian Information Commissioner's 2020 Survey revealed that 74% of respondents believe political parties should be subject to the Privacy Act.[4]

Bringing political parties and their associated entities under the Privacy Act is not just about managing risk. It is also an opportunity to demonstrate leadership, build trust and prove to the public that they are serious about meeting community expectations and protecting the privacy rights of voters.

---

[2] 'Voters want to ban politicians from spamming them with texts and calls,' September 2021, *The Sydney Morning Herald.* Available at: https://www.smh.com.au/politics/federal/voters-want-to-ban-politicians-from-spamming-them-with-texts-and-calls-20210924-p58uko.html

[3] ibid.

[4] OAIC, *Australian Community Attitudes to Privacy Survey,* 2020, page 60. Available at: https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page

Improving Australia's cyber security

In 2019, major political parties were subject to cyberattacks and narrowly avoided being part of a data breach of unimaginable damage. Australia's Cyber Security Strategy also notes that malicious activity against Australian networks in 2020 included policial organisations being targeted by a sophisticated state based cyber actor.[5] Little has been done to address why and how political parties gather, retain and process data, including personal information. Better cybersecurity is good, but not storing sensitive data is better.

The more personal information an entity collects and holds, the higher the risk profile. By extending the Privacy Act to cover political parties, they would need to meet the requirements of the Australian Privacy Principles. In turn this would reduce the possible consequence of any future data breach, as the parties would have been required to do due diligence to ensure they are only collecting necessary personal information, as well as handling it in accordance with the protections offered by the Act.

Requiring political parties to comply with Principle 11 in particular would ensure that political parties are taking reasonable steps to protect Australians' personal information that they hold.

Without adequate digital security protections, political parties represent a weak spot in Australia's cyber security ecosystem.

[5] 'Australia's Cyber Security Strategy', Department of Home Affairs, 2020. Available at: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Recommendations

- Remove the exemption for political representatives, political parties, their contractors, sub-contractors and volunteers from the Privacy Act, Spam Act and Do Not Call Register Act.
- Consider implementing a requirement for disclosures identifying political advertising across all social media and narrowcast platforms, including forms of native advertising or sponsored content (such as influencer content). This should identify which organisation or party has authorised it, and who has paid for it.

Notes

Representatives of Digital Rights Watch are available to answer further questions from the Committee.

Contact

Samantha Floreani | Program Lead | Digital Rights Watch | [redacted]