Submission to the Attorney-General's Department

regarding the

Privacy and Other Legislation Amendment Bill 2024

11 October 2024

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[1]

[1] Learn more about our work on our website: https://digitalrightswatch.org.au/

Who we are

Digital Rights Watch is a charity organisation founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness and freedom. Digital Rights Watch educates, campaigns and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website:

www.digitalrightswatch.org.au

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.

Contact

Elizabeth O'Shea | Chair | lizzie@digitalrightswatch.org.au

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Attorney-General's department regarding the Privacy and Other Legislation Amendment Bill 2024. As Australia's leading digital rights organisation, DRW is primarily concerned with the human rights, safety and wellbeing of individuals and communities in the digital age.

Digital Rights Watch has been actively participating in the consultation process throughout the review of the *Privacy Act 1988* (the Act) since it commenced in 2020. In addition to our formal submissions, we have hosted a range of community events and roundtables to better understand the needs and expectations of other advocacy and interest groups, as well as the community more broadly.

Our recent submissions relevant to this inquiry include:

- Privacy Act Review - Issues Paper, November 2020[2]
- Privacy Act Review - Discussion Paper, January 2022[3]
- Proposed Online Privacy Bill, December 2021[4]
- Senate inquiry into the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,* November 2022[5]
- Privacy Act Review Report, March 2023[6]

DRW welcomes the opportunity to participate in public hearings or further consultations and to provide comment and feedback on future specific proposals.

General remarks

Privacy is essential to upholding democracy, reining in corporate power, and building a safe and fair digital future.

---

[2] Digital Rights Watch submission to the Attorney-General on the Issues Paper regarding the review of the *Privacy Act 1988,* November 2020.
https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/
[3] Digital Rights Watch submission to the Attorney-General's Department on the Discussion Paper regarding the review of the *Privacy Act 1988*, January 2022.
https://digitalrightswatch.org.au/wp-content/uploads/2022/01/Submission_-Privacy-Act-Review-January-2022.pdf
[4] Digital Rights Watch submission to the Attorney-General's Department on the proposed *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021,* December 2021.
https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/
[5] Digital Rights Watch submission to the Senate Standing Committee on Legal and Constitutional Affairs regarding the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,* November 2022.
https://digitalrightswatch.org.au/wp-content/uploads/2022/11/DRW-Submission-Privacy-Legislation-Amendment-Bill.pdf
[6] Digital Rights Watch submission to the Attorney-General's Department on the 2022 Report regarding the review of the *Privacy Act 1988*, March 2023.
https://digitalrightswatch.org.au/2023/04/03/submission-privacy-act-review-report/

The bill has been described as a 'first tranche' in the process of reforming the Act.[7] The two central proposals, a statutory tort and the roadmap for a children's online privacy code, together represent a good first step, but Australia's privacy legislation remains decades behind other nations. In particular, we note the absence of an updated definition of 'personal information', a fair and reasonable test, and the continuing exemptions such as those that currently exist for small businesses. Delay in pursuing these reforms leaves gaping holes in Australia's legal regime for the protection of personal information.

We are past the time for incremental amendments to the Act. *The Privacy Act Review Report 2022* ("the Report") introduced 116 recommendations that would bring the Act up to an international standard, and they ought to be legislated in their entirety. Australians expect their privacy to be protected now.

If the Attorney-General's office intends on introducing these reforms in 'tranches', as is suggested, we expect to see a detailed roadmap and timeline for the introduction of the remaining tranche(s), else we risk the remaining reforms being delayed indefinitely. We concur with many other civil society organisations in calling on the government to implement the remaining reforms within six months of taking office, should they win the next election. We also call on the opposition to make a similar commitment should they win office.

Automated decision-making

The bill introduces enhanced transparency on automated decision-making (ADM), requiring APP entities to update their privacy policies, with a two-year notice period from the date the Bill receives Royal Assent until this change takes effect. Under these amendments, organisations will be required to disclose in their privacy policies where the use of ADM would "reasonably be expected to significantly affect the rights or interests" of the individual.

It is unclear what the threshold of this expectation would be, and we suspect many organisations may deem their actions to fall beneath this threshold and refrain from disclosing their activities. The government should introduce factors and/or examples that assist with the interpretation of this phrase. These could be borrowed from the guidance[8] already available for interpretation of the European Union's similarly worded phrase in Article 22 of the *General Data Protection Regulation 2016* which provides the following examples:

---

[7] Second reading speech – Privacy and Other Legislation Amendment Bill 2024, 12 September 2024, Available at: https://ministers.ag.gov.au/media-centre/speeches/second-reading-speech-privacy-and-other-legislation-amendment-bill-2024-12-09-2024

[8] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* <https://ec.europa.eu/newsroom/article29/items/612053>

- decisions that affect someone's financial circumstances, such as their eligibility for credit;
- decisions that affect someone's access to health services;
- decisions that deny someone employment opportunity or put them at serious disadvantage;
- decisions that affect someone's access to education, for example university admission.

We note that the bill does not introduce Proposal 19.3 from the Report, the right for an individual to request 'meaningful information' about how automated decisions are made. Nor does it introduce any right for individuals not to be subject to decisions based solely on automated decision making. These proposals are important to introduce greater transparency around ADM systems and give individuals more agency when navigating this data management relationship. If such reforms do not go through, we are concerned that it would give rise to circumstances where individuals are made aware that they are subject to automated decisions, but are not given any meaningful recourse to prevent this from occurring. If the intention is to introduce Proposal 19.3 alongside broader reforms for individual data rights, this needs to be explicitly communicated and a timeline provided.

Statutory tort for serious invasions of privacy

A statutory tort for serious invasions of privacy has been the subject of significant law reform work over decades. There is a well-identified gap in the law, as well as a community expectation that privacy invasions give rise to legal rights, and this proposal addresses these issues.

Appropriately, the proposed tort is the model proposed by the Australian Law Reform Commission (ALRC) in their 2014 report.[9] However, there are some key differences, and in various ways they undermine the utility of the proposal.

We think the exemption for journalists should be revised. The current wording is too wide, and does not align with the ALRC's model. It is not appropriately limited, as is required by a human rights approach. We support the proposal put forward by our colleagues at the Human Technology Institute that the proposed exemption for journalism should be re-framed as a defence and confined to journalism in the public interest, with the onus of proof resting on the defendant.

We also see no justification for the exemption for enforcement bodies and national security organisations. These bodies would have access to the statutory defence that the conduct was 'authorised by law'. This should be sufficient for all lawful activities conducted by these bodies, and see no justification for an expansion of this.

[9] Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014).

We also have concerns about the proposed statutory defence on the basis of consent. In our view, it ought only apply to express consent, and implied consent only where consent was clear and unambiguous.

Greater powers for the OAIC and the proposed Children's Online Privacy Code

We welcome the greater enforcement powers the bill proposes to provide to the OAIC, and the tier level of penalties that the bill introduces. In particular, we are pleased that the OAIC will be given the ability to issue infringement notices for non-compliance, without the need to resort to litigation. This will disincentive entities to do the wrong thing. However, it will only work effectively if the OAIC is sufficiently funded.

We support the development of a Children's Online Privacy Code. We believe that greater data protections for all people benefit everybody online, including children, and suggest that greater effort should be directed to legislating fundamental privacy reforms that raise the bar to meet international standards as well as people's collective expectations for privacy.

Doxxing offences

In relation to Schedule 3, our view is that the provisions relating to doxxing offences be removed from the bill and reintroduced as a separate bill. These provisions have not been subject to the rigorous process for other reforms (most of which remain outstanding). We question the early inclusion of these provisions (and associated prioritisation over other more urgent reforms as recommended in the Report) and recommend they be postponed to allow for further consultation.

We support the Law Council of Australia's submission on *Doxxing and privacy reforms*: "Any regulatory framework designed to address doxxing must reflect a very careful balance between addressing the unacceptable harm to individuals caused by illegitimate doxxing behaviours, and ensuring that legitimate instances of information publication are not prevented."[10] We note existing State and Commonwealth laws legislating the use of "a carriage service to menace, harass or cause offence" and see no evidence of and gap or inadequacy that might give rise to the need for additional 'doxxing' laws.[11]

The Law Council of Australia also points out that "An overly-broad definition risks a chilling effect on disclosures that are in the public interest." We advocate for a human rights approach to analysing these provisions. We are particularly

[10] Law Council Submission to the public consultation on doxxing, 10 April 2024 https://lawcouncil.au/publicassets/8b377c40-d1f7-ee11-9494-005056be13b5/4514%20-%20S%20-%20Doxxing%20and%20Privacy%20Reforms.pdf

[11] *Criminal Code Act 1995* (Cth) s 474.17

concerned about the potential for a 'doxxing' provision to be used to target legitimate forms of speech and non-violent protests, for example, in cases where activists may share the names or email addresses of high profile executives and encourage people to send them a message.[12]

Reforms that are missing from this tranche

There are a number of very important proposals that are missing from this first tranche that must be advanced by the government without delay. All of these proposals have been subject to years-long consultation. Many are also very popular with the Australian public, and would bring Australia's laws up to date with similar comparable jurisdictions. The time for these further reforms is now.

- Definition of personal information: We note that the bill does not propose any changes to the definition of "personal information". This is a fundamental component of the recommended reforms, without which significant and important reforms (such as the Children's Online Privacy Code) will be limited in scope.
- A fair and reasonable test: We strongly recommend that the fair and reasonable test should apply to *all* instances of collection, use and disclosure of personal information, including those authorised under APPs 3.4 and 6.2. We encourage the implementation of a best-interests framework as part of the consideration of "reasonableness," rather than only considering best interests where it applies to children.
- Consent: We need a strengthened definition of consent, as in Proposal 11.1, such that consent must be voluntary, informed, current, specific and unambiguous. Consent cannot be considered to be ongoing, specifically to ensure that entities cannot rely on consent that has since been withdrawn. Deceptive or manipulative practices, such as those the use of "dark patterns" do not constitute valid consent.
- Amending exemptions: The Privacy Act cannot be considered meaningful when 95% of businesses operating in Australia are considered exempt. Small businesses are not only key actors when it comes to invasions of privacy as the collectors of extraordinary amounts data from individuals, but also vectors for potential cyber attacks. Meaningful privacy reform, which includes removing the small business exemption, is necessary to protect everyday Australians from the harm of cyber attacks. We also recommend the removal of the political parties exemption, and employee records exemption.

[12]Adani Australia, Submission to the Proposed Online Safety Act, 18 February 2021, Available at https://www.infrastructure.gov.au/sites/default/files/submissions/osb-adani-australia.pdf