Submission to the Attorney-General

on the proposed

Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

6 December 2021

Overview

We welcome the opportunity to submit comments to the Attorney-General concerning the review of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Bill).[1] Digital Rights Watch has been actively following the development of privacy in Australia, and we have been particularly interested by the findings of the ACCC inquiry into Digital Platforms and its extensive emphasis on the need for privacy and data protection in order to protect consumers in the digital era.[2]

As with other pieces of legislation which seek to update and reform privacy rules, we would like to highlight our concern that the consultation process of the Bill is moving ahead in parallel to the review of the Privacy Act 1988.

Given the scope overlap and potential for new privacy reforms to fundamentally impact the way data protection and ownership is viewed in Australian legislation, it should remain a priority to update the Privacy Act before proceeding with any other fundamental changes to the way that personal information of Australians is treated. Some of our submissions relevant to the topics covered:

- Data Availability and Transparency Bill https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/
- UN Human Rights Council Australia Universal Periodic Review https://digitalrightswatch.org.au/2020/08/28/access-now-and-digital-rights-watch-joint-submission-to-the-un-human-rights-council/
- Privacy Act Review Issues Paper (November 2020) https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/

Digital Rights Watch

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.[3]

---

[1] https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf

[2] The Digital platforms final report provides several recommendations on how to strengthen the rights of consumers in the digital space, including stronger privacy protections and data rights: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

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

General remarks

At Digital Rights Watch, we are equally concerned about the lack of a federal level protection for privacy as we are by the ever-growing collection and use of personal data by public and private entities. In the ongoing review of the Privacy Act, we have urged the government to focus on addressing the most pressing systematic data collection and exploitation models that digital platforms, data brokers, and targeted advertisers thrive on—and ensure meaningful protections and actionable rights for individuals. We appreciate that the new OP Bill attempts to do this at a targeted level for children, but we believe it must remain a priority to update the system for everyone, regardless of age.[4]

Over the past two years, we saw our lives move increasingly online as many work, study and interact remotely with friends and families. The emphasis on technology was unprecedented across education sectors and remote workplace teams, and a lack of strong privacy safeguards left many Australians frustrated and questioning their rights and liberties.[5] At DRW, our concern grows over the unchecked predatory data collection and aggregation of many digital services and Internet platforms, many of which became an unavoidable (if not outright mandatory) fixture in people's everyday lives. Updating the privacy framework should give Australians the ability to control how their information is used and shared, and empower them to take action when their privacy is violated. It should also prioritise structural reform such that public and private entities are required to improve their data handling practices, and not place the burden upon individuals to protect themselves in an increasingly complex space. At the moment, internationally, we are falling behind in addressing the privacy (but also broader societal and economic) harms caused by the business models of digital platforms and services.

We are very concerned that the OP Bill is building on top of the Privacy Act's Australian Privacy Principles (APPs), rather than prioritizing making meaningful change to the underlying legislation. Using an Act which is currently undergoing a substantial overhaul as a basis for this new framework to protect children essentially codifies an outdated and inadequate system. It also restricts the potency of the new legislation to truly empower individuals to take control of their rights because of the way the APPs are currently drafted.

As a part of reviewing the privacy ecosystem in Australia, we therefore urge the government to enshrine in law a federal level right to privacy in line with Article 12 of the United Nations (UN) Universal Declaration of Human Rights to which the Australian government is a signatory. Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[6]

---

[4] Online Privacy Bill Explanatory Paper: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf

[5] Technology-and-Power-UWU-Submission.pdf (unitedworkers.org.au)

[6] Universal Declaration of Human Rights | United Nations

We believe that recognising the right to privacy at the federal level is critical, in part as it will create a rights-based relationship with the way Australians' data and privacy is treated online, as opposed to an economic or value-driven model which has been the case so far.[7] It should remain a priority of the government to implement the right to privacy outright.

A rights-based approach to privacy and data protection is ensured in key jurisdictions, such as the United States, United Kingdom, and across the European Union's (EU) 27 member states, and it will prove increasingly critical for the Australian economy to keep pace with this approach if we seek to continue cooperation and e-commerce with these jurisdictions in the future. While we recognise that a copy and paste of the EU's General Data Protection Regulation (GDPR) is not the penultimate solution, we would encourage the consideration of the rights guaranteed to individuals, many of which should form a fundamental part of a truly modernised Australian approach to privacy online. Chapter 3 of the GDPR entitled "rights of the data subject" ensures that there are clear and actionable rights for individuals.[8] The review of the Australian privacy framework should seek to provide the same, or similar. Indeed, some of the rights introduced by the GDPR were considered by the Australian Human Rights Commission as a part of their Human Rights and Technology project.[9]

Duplication of efforts

The OP Bill is described as addressing the "unique and pressing privacy challenges posed by social media and online platforms".[10] While digital platforms do require updated privacy protections that are fit for purpose for our interconnected world, we are concerned that many of the objectives of the OP Bill such as how to deliver notice and gain consent in practice, as well as how to protect children and other vulnerable groups, are not necessarily unique to social media or online platforms, and would be best dealt with wholesale; in the review of the Privacy Act. With the exception of age verification, all of the issues listed under Section 26KC that the OP Code would be required to cover are under active consideration as part of the Privacy Act review.

Importantly, the proposals in the Privacy Act Review Discussion paper would be applicable to *all* regulated entities and protective of *all* individuals. By contrast, the OP Bill places emphasis on *one* sector, and *one* group of individuals (children). As such, by pursuing both simultaneously, there is risk of creating a two-tiered privacy regulatory system, in which some organisations are covered by the OP Code and some are covered by the Privacy Act. It is our view that this risks creating an unnecessarily complicated regulatory framework, and as stated above, risks codifying an outdated and inadequate system.

---

[7] The emphasis on Consumer Data Rights (CDR) is evidence of this, as is the consideration by the Australian Bureau of Statistics to merge privately held datasets into the public census data to improve results and the "economic contribution" of the census. This value-driven calculation of privacy infringement vs economic benefit fundamentally shifts when we consider a rights-based system.
[8] More at: Chapter 3 (Art. 12-23) Archives - GDPR.eu and a user's guide by Access Now at Know your rights: How to protect your data with the GDPR - Access Now
[9] Human Rights and Technology | Australian Human Rights Commission
[10] Privacy Act Discussion Paper, page 9, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/

Finally, we have not seen compelling evidence that the proposals included in the OP Bill would be effective in protecting privacy in practical terms until there are meaningful changes to core aspects of the Privacy Act, including the definition of 'personal information'. In fact, many social media companies and data brokers benefit from being able to consider their activities as falling outside the scope of the Privacy Act, thanks to that very narrow definition. For instance, the website of data broker LiveRamp (formerly Acxiom) states that they remove personally identifiable information.[11] This means that for instance information about behaviours, while readily understood to be privacy-invasive when aggregated, would not be covered by those provisions of the Privacy Act nor many of the protections offered in the OP Bill. It is essential that the underlying shortcomings of the Privacy Act are amended before attempting to tack on additional mechanisms.

Age verification

DRW is deeply concerned about the requirement for social media services to take 'all reasonable steps to verify the age of individuals to whom the OP organisation provides an electronic service'.[12]

We disagree with this proposal for two key reasons:

1) **Age verification is privacy-invasive, which undermines the objective of the Bill.**
   Most forms of age verification require the provision of additional personal information in order to be effective. The inclusion of this requirement for an OP code is likely to compel social media platforms to collect, use, and store additional personal information in order to meet this requirement. This not only creates significant privacy and security risks, but it also works in *favour* of data-hungry social media platforms.

   We have explored this issue at length in our recent submission to the eSafety Commissioner regarding the draft Restricted Access System (RAS) Declaration.[13]

2) **Age verification, or the requirement of parental consent, achieves nothing to change the surveillance-based business models underpinning social media, nor the harms that arise from it.**
   Many of the harms caused by social media that the OP Bill seeks to ameliorate are a result of data-extractive, surveillance-based business models. These models rely on the collection of immense amounts of information in order to be able to target us individually, conduct hyper personalisation, and to shape, curate and manipulate what we are exposed to online. It is clear that these practices do indeed cause significant harm to individuals, especially children. Age verification does nothing to combat these harmful business models, and in fact may cause additional

[11] https://liveramp.com/our-platform/security-privacy/
[12] Section 26KC(6)(a) of the Online Privacy Bill Exposure Draft
[13] DRW submission to the eSafety Commissioner on the draft Restricted Access Systems (RAS) Declaration, 25 November, 2021. Available at: https://digitalrightswatch.org.au/2021/11/25/submission-draft-restricted-access-systems-declaration/

privacy-related harms in the long run, as it relies on collection of additional information.

Finally, we hold some reservations regarding the requirement to 'obtain the consent of a parent or guardian of a child who has 15 not reached 16 years before collecting, using or disclosing 16 personal information of the child'.[14] We wish to emphasise that for many young people, especially those in rural or regional areas, or who may be part of a vulnerable or marginalised group (for instance, part of the LGBTQ+ community or a racial minority), the Internet and social media may be their only point of connection to vital community support and health information.

While we empathise with the objective to protect children from online harms, including privacy invasion, we question whether requiring parental consent may cause additional harm, distress, and isolation, in instances where their parents or guardian do not necessarily have the child's best interests in mind. We suggest that the Attorney-General's department conduct additional research into the efficacy and genuine harm-reduction of this proposal before further pursuing this proposal.

Data brokers

We are pleased to see the Government considering the impact of data brokerage services on the privacy of Australians. However, we are concerned that the OP Bill places too much emphasis on social media platforms, rather than the data brokers or regulating the industry as a whole. For example, the explanatory memorandum states:

> *"The potential risks social media platforms pose to children are higher than those posed by data brokers or large online platforms due to the number of children who use social media services, the nature of the interactions that can occur via social media platforms, and the wide range and volume of personal information that social media platforms handle"*

We wish to emphasise that while the harms caused by data brokers and big data analysis may not be as readily apparent to the public as those caused by social media, the business models of data brokers are exceptionally invasive, predatory, and in many ways act as the engine of surveillance capitalism. In order to have a meaningful impact upon the privacy of Australians, focusing on regulation of the entire industry which collects and handles personal information, including data brokers, should be made a priority.

[14] Section 26KC(6)(b) of the Online Privacy Bill Exposure Draft

Recommendations

- **Finalize the review of the Privacy Act prior to enacting further privacy legislation**. The Privacy Act must apply to any and all entities which collect, process or otherwise handle personal information. Creating a framework on the basis of the existing APPs before the review is complete only codifies an outdated framework and creates a fragmented regulatory landscape which will not serve the exercise of individual's rights.
- **Remove the threshold for compliance based on the size and reach of a digital platform.** The protection of individual's rights should be absolute, and the rules should be written in a way which makes them tenable for all entities processing and collecting data—not just those which have reached a certain size. One of the key shortcomings of the Privacy Act has been the small business exemption which has created a significant gap in the privacy protections offered to Australians. It is important that we do not replicate this oversight in the OP Bill. The Bill must apply to any and all entities which collect, process or otherwise handle personal information.
- **Prioritize a rights-based approach.** In a data-driven economy, the rights of individuals should be the foundation of this review, and ensuring that Australians have direct rights of action when their privacy is violated or their personal information mistreated is essential in holding internet platforms, advertisers and all third parties to account.
    - We urge the Attorney-General to consider the rights granted under the EU GDPR as a reference point for developing a rights-based system for the Australian context. While some rights, such as "the right to portability" already exist in Australia, there are other vital rights under the GDPR such as the "right to explanation", "right to rectification" and "right to erasure."[15]
    - Specifically, the "right to explanation" is critical in helping individuals understand how their personal information was used in making decisions, creating accountability between individuals and the entity processing their information. This matter has been considered by the Australian Human Rights Commission in their discussion paper on Human Rights and Technology.[16]
- **Restrict secondary uses and disclosures of personal information which are currently in the Privacy Act.** This should be an opportunity to strengthen and protect the privacy of individuals, not perpetuate the flaws currently inherent in existing legislation. Access 'to assist a law enforcement body undertake an enforcement-related activity' should be restricted along with the other secondary uses provided for by the current version of the Privacy Act.
- **Remove any requirements for age verification systems as they run counter to the intention of the legislation.** In an effort to apply protections by age, one of the

[15] We recognise that the "right to erasure" has been misinterpreted globally and applied in very different ways across the EU member states. We would encourage the AG to consider the best practices for the Australian context. More in Access Now's paper on the Rights to be Forgotten globally: RTBF_Sep_2016.pdf (accessnow.org)

[16] Human Rights and Technology | Australian Human Rights Commission

key parts of the Bill appears to be the requirement for platforms to implement age verification. This proposition has been widely criticised by privacy and security experts for years. We need to be careful that in an attempt to protect children online, we do not end up introducing measures that actually undermine privacy for everyone.

- **Strengthen the rules for all entities collecting or handling personal information, including data brokers.** Limiting the Bill based on the size or focus of a business fragments the protections guaranteed to individuals. Similarly to making any distinction between public and private use of personal information; key principles, such as data minimization, consent, and other relevant data rights should apply in all circumstances.

Contact

Lucie Krahulcova | Executive Director | Digital Rights Watch | lucie@digitalrightswatch.org.au