Submission to the Attorney-General

on the proposed

Review of the *Privacy Act 1988*

29 November 2020

Overview

We welcome the opportunity to submit comments to the Attorney-General concerning the review of the Privacy Act 1988 as recommended by the ACCC after their exhaustive Digital Platforms Inquiry. Digital Rights Watch has been following the ACCC inquiry into Digital Platforms with great interest and we are encouraged by the final report's extensive emphasis on privacy and data protection in order to protect consumers in the digital era.[1]

In November we submitted comments to The Office of the National Data Commissioner on the exposure draft of the Data Availability and Transparency Bill 2020, in which we highlighted our concern that the consultation process of the Bill is moving ahead in parallel to the review of the Privacy Act 1988.[2]

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/
- ACCC News Media and Digital Platforms Mandatory Bargaining Code https://digitalrightswatch.org.au/2020/09/02/submission-news-media-and-digital-platforms-mandatory-bargaining-code/

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] The ACCC 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

[2] Our submission is public and is also available on our website with a summary: https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/

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

General remarks

At Digital Rights Watch, we have welcomed the findings of the ACCC Digital Platforms inquiry which made extensive recommendations regarding the need for a data protection framework and improved protections for privacy in order to protect Australian consumers.[4] In reviewing the Privacy Act, we urge 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.

This year more than usual, 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 Act can give Australians the ability to control how their information is used and shared, and empower them to take action when their privacy is violated. 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.

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]

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] While a statutory tort may also be considered (more on that in our recommendations below), it is only a partial substitute for implementing the right to privacy outright.

---

[4] The ACCC 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

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

[6] Universal Declaration of Human Rights | United Nations

[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.

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 under the GDPR, many of which should form a fundamental part of a truly modernised Privacy Act. 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 Privacy Act should seek to provide the same, or similar.

Some of the rights introduced by the GDPR were considered by the Australian Human Rights Commission as a part of their ongoing Human Rights and Technology project.[9] Given that Australians are increasingly asked to adapt to and trust in digital solutions—government-run or private—they must come with rights and guarantees. It is important to see these as mutually beneficial for the entity that is collecting/processing the personal information (or providing the service) just as much as for the individual. The "right to explanation" for instance, guarantees that individuals are able to understand how decisions affecting them were taken (which gives them the ability to take action if this was done with prejudice or in a way that violated the privacy protections in place), but it also helps them understand and develop trust with otherwise opaque decision-making systems and algorithms. Government programs in particular could benefit from this approach to earned trust, but it is equally important for consumer products such as insurance or banking, which take into account a trove of personal information with little insight into how or why.

Recommendations

- **Redefine the scope and reach of the Privacy Act**. The Privacy Act must apply to any and all entities which collect, process or otherwise handle personal information.
    - Privacy by design has been recognised as the international gold standard for new and emerging technologies and provides a great level of protection and certainty to individuals.
- **Update the definition of personal information**. While the definition of personal information under the Privacy Act is good, we would urge the government to reconsider the special category of "sensitive information" which receives a higher level of protection than other "personal information."[10] Given the ubiquity of technology and the way all our personal information interacts online and further information is inferred and generated continuously, this distinction seems arbitrary

[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] What is personal information? — OAIC

and all types of "personal information" deserve the same level of protection as afforded to sensitive information.[11]

- **Adopt 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 malicious parties to account.
    - We urge the Attorney-General to consider the rights granted under the EU GDPR as a starting point for developing a similar 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."[12]
    - 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.[13]
- **Introduce a statutory tort for invasions of privacy**. One of the key components of a functional privacy or data protection regime is the ability for individuals' rights to be enforced and for individuals to seek remedy. Establishing a statutory tort for invasions of privacy would greatly extend individuals' ability to exercise their rights and keep entities processing their data (public or private) accountable.
    - The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such an avenue has increased as data harvesting practices are skyrocketing in Australia.[14] It was further suggested in the final report of the ACCC's Digital Platforms Inquiry.
- **Do not use consent as a scape-goat to weak protections of personal information.** The current law places significant emphasis on consent, which we think is important. However, we recognise that in the current digital ecosystem, consent is not always an effective way for individuals to control personal information, and can lose meaning. Consent may not be necessary for the use or disclosure of personal information which is in pursuit of the primary purpose for which the information was collected in the first place. And while consent should remain an important part of how

[11] The European Union's GDPR has a much broader definition of personal data, which ensures a greater level of protection for consumers and very little leeway for loopholes. Under the GDPR: "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Art. 4 GDPR - Definitions - GDPR.eu

[12] 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)

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

[14] Should a new tort be enacted? | ALRC

individuals control personal information, it shouldn't be used as a way to circumvent complying with purpose limitation and other limits and protections. For consent to be meaningful, it needs to be provided as a result of a genuine choice that is made from a position of knowledge. It must not become a transactional, box ticking requirement, that then serves as a licence to use personal information without limit.

- **Abolish exemptions, namely the exemption for political messaging**. Since exemptions from the Privacy Act were crafted over twenty years ago, they must be reconsidered. As we have seen through reports and documentaries such as *The Great Hack*, the exemption for political messaging poses a unique threat to our democracies.[15] Over the last decade we have seen an explosion in the practice of profiling and targeting individuals for political messaging. Personalised news feeds, ads and other individual-targeted content online can more easily facilitate misinformation than offline political advertising could achieve. As a result, the risks posed to the privacy of individuals, the stability of our democratic government, and public trust in public institutions have exponentially increased.
- **Introduce a stronger definition of 'de-identified' data**. We suggest requiring a higher standard of de-identification to only allow data from which no individual is identifiable. The absence of standards with respect to de-identification is an aspect of the regime that needs to be urgently updated. In order to enable scrutiny and security research, the re-identification of such data for public interest purposes should not be an offence. Further, it should be a requirement that any person who is affected by the release of personal information in a manner that did not meet the requisite standards for de-identification should be notified.[16]

Contact

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

[15] The Great Hack: the film that goes behind the scenes of the Facebook data scandal | Cambridge Analytica | The Guardian

[16] The simple process of re-identifying patients in public health records | Pursuit by The University of Melbourne (unimelb.edu.au)