Submission to the Senate Standing Committee on Legal and Constitutional Affairs

regarding the

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

3 November 2022

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/

General remarks

Digital Rights Watch (DRW) welcomes the opportunity to provide a submission with regard to the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* ('the Bill').

As a leading Australian civil society organisation working to protect human rights as realised in the digital age, DRW has actively participated in the privacy reform process to date, as well as other proposals and developments in the privacy law space. Previous relevant submissions made by DRW include:

- Privacy Act Review Discussion Paper (January 2021)[2]
- Privacy Act Review Issues Paper (November 2020)[3]
- Online Privacy Bill (December 2021)[4]
- Data Availability and Transparency Bill (November 2020)[5]

We acknowledge that the proposed amendments in the Bill are not intended to cover the full range of reforms required to make the Privacy Act fit for purpose in the data-driven internet economy.

We wish to emphasise that while we generally welcome these amendments to the Privacy Act as an interim response to the recent major data breaches, they are not nearly comprehensive enough to establish meaningful, long-term privacy protections for everyday people.

Data breaches are just one of many possible privacy-related harms that can arise when people's personal information is collected, used, stored and shared inappropriately or unlawfully. Given that the Bill does not make any meaningful changes to the Australian Privacy Principles, this Bill alone will not address the long-standing gaps and issues, but rather increase the punitive measures for serious or repeated breaches under the current Act. As Dr Katherine Kemp has said, "in the absence of changes to the privacy principles themselves, and a properly resourced privacy regulator, you may be getting a bigger stick with no-one to swing it and not a great deal to swing it at."[6]

---

[2] Submission to the Attorney-General on the Privacy Act Review - Discussion Paper, January 2022. https://digitalrightswatch.org.au/2022/01/11/submission-privacy-act-review-discussion-paper/
[3] Submission to the Attorney-General on the Privacy Act Review - Issues Paper, November 2020. https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/
[4] Submission to the Attorney-General 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] Submission to the Office of the National Data Commissioner on the proposed *Data Availability and Transparency Bill 2020,* November 2020. https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/
[6] 'Data breach fine proposals in wake of Optus, Medibank hacks not enough say privacy advocates,' *ABC News,* 27 October 2022. https://www.abc.net.au/news/science/2022-10-27/data-breach-penalties-privacy-laws-not-enough-critics-say/101578160

Digital Rights Watch remains concerned regarding the ongoing lack of requisite and stable funding for the Office of the Australian Information Commissioner (OAIC) to be a strong, effective regulator. The additional $5.5 million allocated to the OAIC to investigate the Optus data breach in the most recent budget does not meet the *ongoing* funding needs of the OAIC. The digital ecosystem and privacy issues that come with it are only increasing in complexity, severity and frequency. The OAIC urgently needs increased funding that is not tied to one specific investigation to be able to meet its growing responsibilities.

Increased penalties that reflect the serious nature of privacy invasions and data breaches is a welcomed first step, but we can't stop here. **We look forward to seeing the full suite of proposed reforms in the Privacy Act review report later in 2023, and we welcome the opportunity to engage with the Attorney-General's Department further on this**, to ensure the reforms meet community expectations and meaningfully protect everyday people from the harms of the data-extractive internet economy.

Increased penalties are a good start, but not enough on their own

Digital Rights Watch welcomes the proposed increased penalties for serious or repeated interferences with privacy under the Privacy Act as an important improvement to the enforcement regime of the Act. The current fines available under the Act are woefully inadequate, and it is long overdue that they are raised to correspond with the seriousness of privacy non-compliance. Fines and private enforcement can serve as an important incentive for executives to prioritise privacy and digital security, as well as create accountability.

It is our hope that increased penalties will also contribute to changing the culture regarding data gluttony, and compel organisations to consider data lakes containing personal information to be a toxic asset. Too many organisations currently collect and retain far too much personal information for a variety of reasons. Without appropriate disincentives, many organisations consider retaining information to be easier than deletion, or opt to hold onto more data than they need 'just in case' there is a use for it later. However, we would emphasise that fines alone are not enough to change this culture of over-collection. For this to be effective we also need clear, strong rules that limit the collection of personal information, and promote data minimisation.

We also note that there is nothing in this Bill that alters that the OAIC still needs to ask the Federal Court to levy these fines, and that they can only be used for serious or repeated conduct. Without amendment to these factors, the application of these new penalties remains hard to reach.

Finally, we remain concerned that increased fines do not necessarily translate to redress to those who are harmed by interference with their privacy, including breaches. Stronger fines will not get people's personal information back once it has been compromised.

One area where this could be improved is compensation. The current test for compensation is based on harm suffered, yet data breaches such as Optus or Medibank require people to take proactive steps to guard against harm, and they may suffer harm much later and in unexpected ways. The test for compensation needs to change.

There is a serious need to give power to individuals to seek redress for the harm they have suffered as a consequence of privacy invasion. Digital Rights Watch strongly recommends establishing a statutory tort for serious invasion of privacy, as well as a direct right of action. It is clear that regulators cannot deal with this problem alone, and these changes would offer an important way for people to take their right to privacy into their own hands.

Clarifying extraterritorial application a welcome improvement

Digital Rights Watch strongly supports item 10, which repeals Paragraph 5B(3)(c), effectively removing the 'Australia link' requirement. This makes the Privacy Act more fit for purpose in the global internet economy, and will make it harder for foreign companies to avoid meeting the requirements of the Privacy Act. Abolishing the Australian link requirement for coverage under the Privacy Act brings it in line with extraterritorial provisions in international equivalents.[7]

We note that in response to proceedings being commenced by the OAIC against Facebook in relation to the Cambridge Analytica scandal, Facebook Inc applied to the Federal Court to have the OAIC's service set aside, based on whether an 'Australian Link' was present.[8] This shows how major technology companies and platforms are willing to try to use this, and any other, gap they can find in the Privacy Act to avoid being held accountable for their invasive and harmful practices, even where they break the law.

While the Federal Court decision does provide precedent and guidance on the Privacy Act's extraterritorial application, we welcome the proposal to remove 5B(3)(c) which will further clarify and simplify the extraterritorial application of the Privacy Act, and bring it in line with international counterparts.

Contact

Samantha Floreani | Program Lead | Digital RIghts Watch |

[7] Including the General Data Protection Regulation in the European Union, the California Consumer Privacy Act in California, and the Personal Data Protection Act in Singapore.
[8] 'Commissioner welcomes Full Federal Court Ruling on Facebook appeal', *Office of the Australian Information Commissioner,* February 2022. https://www.oaic.gov.au/updates/news-and-media/commissioner-welcomes-full-federal-court-ruling-on-facebook-appeal