

Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Via online submission

11 October 2024

Privacy and Other Legislation Amendment Bill 2024 [Provisions] Inquiry

We thank the Senate Legal and Constitutional Affairs Committee for the opportunity to make a submission on the Privacy and Other Legislation Amendment Bill 2024. The submission of the Jeff Bleich Centre for Democracy and Disruptive Technologies is enclosed as an annexure to this letter. The enclosed submission has been prepared by members of the Jeff Bleich Centre with backgrounds in law.

Submission Executive Summary

The authors welcome the introduction of the Privacy and Other Legislation Amendment Bill 2024 to the Parliament. The primary comments of the authors in the annexed submission include:

1. recommendations that further tranches of privacy law reforms to implement the significant volume of recommendations and proposals that have emerged between 2019 and 2024 be advanced as a matter of urgency.
2. concerns about excluding parliamentary processes for the disallowance of statutory instruments.
3. noting the need to ensure that any Children's Online Privacy Code should factor in recent policy announcements related to social media bans for young people.
4. comments on the proposed APP 11.3, its alignment with international equivalents and its implementation.
5. support for the introduction of additional mechanisms regarding the transfer of personal information overseas, but notes that these steps will ensure Australian laws meet the requirements of other international data privacy frameworks.
6. noting the introduction of new civil penalty provisions.
7. raising concerns with the introduction of provisions regarding automated decision making and the need to disclose such matters in privacy policies.
8. noting support for the introduction of a statutory tort for serious invasions of privacy.

About the Jeff Bleich Centre

The Jeff Bleich Centre for Democracy and Disruptive Technologies is a research centre within Flinders University's College of Business, Government and Law. It is the mission of the Jeff Bleich Centre to be the expert voice on how to strengthen the core values and institutions of democratic societies in a world where technology constantly disrupts the status quo. The Jeff Bleich Centre undertakes transdisciplinary work across multiple lines of effort, with research concentrations in:


- Democracy, Participation and Human Rights;
- Defence, Security and Space; and

- Artificial Intelligence, Social Media and Disruptive Technologies.

We hope the enclosed submission is of assistance and we would be happy to discuss the submission or answer any questions that might arise. Queries can be directed to jbc@flinders.edu.au.

Yours Sincerely,

**Jeff Bleich Centre for Democracy
and Disruptive Technologies**

 **Dr Joel Lisk**
Media and External Engagement Lead
Jeff Bleich Centre

Privacy and Other Legislation Amendment Bill 2024

Submission by the Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University to the Senate Legal and Constitutional Affairs Committee

11 October 2024

1. Preliminary

For the purposes of this submission, the following terms are used:

- 1.1. **Bill** means the Privacy and Other Legislation Amendment Bill 2024 as tabled in the House of Representatives on 12 September 2024.
- 1.2. **Privacy Act** means the *Privacy Act 1988* (Cth) as in force as at the date of this submission.
- 1.3. **APP** means Australian Privacy Principles.
- 1.4. **OAIC** means the Office of the Australian Information Commissioner.

2. Approach to Reform

- 2.1. The authors recognise that the path to developing the Bill has been long. The Australian Competition and Consumer Commission (**ACCC**) recommended amendments to the *Privacy Act* in its 2019 Digital Platforms Inquiry Final Report.¹ This was followed by:
 - 2.1.1. the Privacy Act Review Issues Paper released by the Attorney-General's Department in October 2020 and subsequent consultation period;
 - 2.1.2. the Privacy Act Review Discussion Paper released by the Attorney-General's Department in October 2021 and subsequent consultation period;
 - 2.1.3. the Privacy Act Review Report released Attorney-General's Department in February 2023 and subsequent consultation period; and
 - 2.1.4. the response from the Australian Government to the Privacy Act Review Report in September 2023.
- 2.2. The Privacy Act Review Report included more than 100 proposals for changes to the *Privacy Act*. The majority of these changes are not included in the Bill. We strongly recommend the Government proceed with implementing the remainder of the proposals in the Privacy Act Review Report as a matter of urgency.
- 2.3. Due to the fragmented approach to implementing the proposals in the Privacy Act Review Report, it is difficult to forecast the full range of potential impacts of drafting and legislative design in the present Bill.

¹ Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) 34-7, 437-42, 455-96.

3. APP Codes and Emergency Declarations - Schedule 1, Parts 2 & 3

- 3.1. The authors note that caution should be exercised with respect to proposed ss 26GB(8), 80J(3), and 80K(3) that exclude the operation of s 42 of the *Legislation Act 2003* (Cth).
- 3.2. Unless exceptional circumstances apply, Parliament should retain ultimate oversight over the exercise of legislative or quasi-legislative power. The proposed ss 26GB(8), 80J(3), and 80K(3) would undermine the ability for the Parliament to review decision making with respect to delegated legislation.

4. Children's Privacy - Schedule 1, Parts 4

- 4.1. The authors have no substantive comments on the mechanism for the proposed Children's Online Privacy Code but note that the Government should consider how these powers interact with recent announcements related to prohibiting young people from accessing social media platforms.

5. Security, retention and destruction – Schedule 1, Part 5

- 5.1. The authors note the inclusion of a new APP 11.3. This paragraph requires that the reasonable steps be taken to protect or de-identify personal information once that information is no longer needed should include technical and organisational measures.
- 5.2. However, the proposed APP 11.3 does not bring Australian privacy law in line with that in other jurisdictions. Most notably, Article 32 of the European Union's General Data Protection Regulation (**GDPR**) requires data controllers and processors to implement appropriate technical and organisational measures to ensure an appropriate level of security. Article 32 of the GDPR then goes on to supply a list of techniques which can be used to ensure security. These include the pseudonymisation and encryption of personal data, ongoing monitoring of confidentiality, the ability to restore access to personal data and regular testing.
- 5.3. It is arguable that the existing APPs 11.1 and 11.2 already mandated the use of technical and organisational measures – as well as physical measures – as described in the APP Guidelines.² There is also a line of decisions by the Information and Privacy Commissioners that support an assertion that organisational, technical and physical measures must be taken by entities subject to the APPs in order to satisfy their obligations under APPs 11.1 and 11.2.³
- 5.4. The OAIC must, as a matter of urgency, publish guidelines on the use of technical and organisational measures following the passage of the Bill through the Parliament.

6. Overseas Data Flows – Schedule 1, Part 6

- 6.1. The Bill seeks to modify s 100 and APP 8 so that the Government (through the Governor-General) can declare that privacy laws in other countries offer substantially similar privacy protection to the *Privacy Act*.

² See, Office of the Australian Information Commissioner, *APP Guidelines* (22 July 2019) Chapter 11.

³ See, Joel Lisk, 'Data Security in Australia: The Obligation to Protect' (2023) 97(10) *Australian Law Journal* 749.

- 6.2. At present, for an APP entity to transfer personal information overseas, the entity must reasonably believe the personal information is governed by a law or scheme substantially similar to Australian privacy law. Further, the entity must be also satisfied that there is a mechanism for individuals to exercise their rights under that law or scheme.
- 6.3. The revisions to APP 8 are a welcome addition that could help APP entities to determine whether they can send personal information. Other privacy laws, such as the GDPR, contain a scheme by which the European Commission (**EC**) can declare other countries as offering equivalent privacy protection to the GDPR (commonly referred to as 'adequacy decisions').
- 6.4. Nevertheless, because of the limited reforms in the Bill, Australian privacy law may not meet the privacy standards of other countries and jurisdictions. This lack of adequacy will represent a problem for data controllers or processors attempting to transfer data to Australia.⁴ This lack of adequacy may act as an impediment for scientific research between Australia and European Union countries.⁵

7. Penalties for Interference with Privacy – Schedule 1, Part 8

- 7.1. The authors welcome the introduction of a range of new penalty provisions associated with contraventions of the APPs and the *Privacy Act*.
- 7.2. The authors wish to query the underlying rationale for the APPs listed in the proposed s 13K(1)(b), noting that certain APPs, such as APPs 3, 4, 5, 8-12, are not listed.

8. Automated Decisions and Privacy Policies – Schedule 1, Part 15

- 8.1. The Bill amends APP 1 to require an APP entity to set out in their privacy policies whether they use automated decision making. This requirement is limited to circumstances where the decision could reasonably be expected to significantly affect the rights or interests of an individual.
- 8.2. In addition, for the obligation under the proposed APPs 1.7 – 1.9, personal information must be used for the making of a decision.
- 8.3. While the authors welcome the addition of provisions on automated decision making that bring openness and transparency to the processing and use of personal information, the proposed measure fails to bring Australian privacy law in line with other jurisdictions.
- 8.4. Article 13(2)(f) of the GDPR requires a data controller to inform a data subject whether their personal data will be processed as part of automated decision making. Article 13(2)(f) requires meaningful information about the logic used in processing. Further, Article 22 of the GDPR allows a person to opt out of automated decision making if would produce legal

⁴ Julian Wagner, 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?' (2018) 8(4) *International Data Privacy Law* 318, 330.

⁵ James Scheibner et al, 'Data Protection and Ethics Requirements for Multisite Research with Health Data: A Comparative Examination of Legislative Governance Frameworks and the Role of Data Protection Technologies' (2020) 7(1) *Journal of Law and the Biosciences* <<https://academic.oup.com/jlb/article/7/1/Isaa010/5825716>>, 22.

effects that significantly effect this person. This provision of the GDPR has been subject to academic critique on the grounds that it only applies decisions made solely using automated decision making.⁶

8.5. The authors recommend the Australian Government reconsider the content of the proposed amendments to reflect emerging regulatory practices and the need for openness and transparency in data processing.

9. Serious Invasions of Privacy - Schedule 2

9.1. The authors welcome the introduction of a cause of action for a serious invasion of privacy.

9.2. The primary concern of the authors with the schedule as drafted is, due to the fragmented nature of the Government's approach to privacy reform, it is unclear how this cause of action will interact with a direct right of action for interferences with privacy that the Government has indicated that it agrees to in-principle (ie are there instances where both causes of action can be enlivened concurrently?).

10. About the Authors

10.1. [Dr Joel Lisk](#) is a Lecturer in Law at Flinders University and the Media and External Engagement Lead for the Jeff Bleich Centre. Joel primarily researches the regulation of technology, with a focus on consumer protection, privacy and emerging operating domains. Joel is also a lawyer, advising businesses on a range of legal compliance matters.

10.2. [Dr James Scheibner](#) is a Lecturer in law at Flinders University and an Affiliate Member of the Jeff Bleich Centre. James' areas of research include intellectual property and industrial property law, data privacy law and health law.

10.3. The comments expressed in this Submission are from Jeff Bleich Centre for Democracy and Disruptive Technology. The views and content of this Submission may not reflect the views of Flinders University or its various component parts.

⁶ Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34(2) *Computer Law & Security Review* 398, 400-1.