Law Council
OF AUSTRALIA

Privacy and Other Legislation Amendment Bill 2024

Senate Legal and Constitutional Affairs Legislation Committee

22 October 2024

Telephone +61 2 6246 3788
Email mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Table of contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level; speaks on behalf of its Constituent Bodies on federal, national, and international issues; promotes and defends the rule of law; and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts, and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 104,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2024 are:

- Mr Greg McIntyre SC, President
- Ms Juliana Warner, President-elect
- Ms Tania Wolff, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Mr Lachlan Molesworth, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.au.

Acknowledgements

The Law Council is grateful for the contributions of the Law Institute of Victoria, the Law Society of New South Wales, and the Queensland Law Society in the preparation of this submission.

The Law Council also acknowledges the guidance and input of:

- the National Human Rights Committee;
- the Business Law Section's Media and Communications Committee; and
- the Business Law Section's Privacy Law Committee.

Executive summary

1. The Law Council of Australia welcomes the opportunity to assist the Senate Legal and Constitutional Affairs Legislation **Committee** in its inquiry into the provisions of the Privacy and Other Legislation Amendment **Bill** 2024 (Cth).

2. The Law Council has long supported an holistic approach to privacy and data law reform that promotes, to the greatest extent, consistency and predictability in the relevant legislative frameworks. In this regard, we have repeatedly called for the Review of the *Privacy Act 1988* (Cth)—and any subsequent reforms—to be advanced as a matter of priority, the Act being the primary and authoritative source of privacy law in Australia.

3. To best assist the Committee in its lamentably short inquiry timeframe, this submission does not seek to repeat the detailed policy considerations raised in our April 2023 submission to the Attorney-General's **Department** to inform the Government Response to the Privacy Act Review Report.[1] This submission largely focuses on technical drafting suggestions and opportunities to minimise the risk of unintended consequences arising in relation to various aspects of the Bill. For ease of reference, the key issues and corresponding recommendations are set out in the table below. More detailed commentary is provided in the remainder of our submission.

4. We support the passage of the Bill, subject to the 18 recommendations below and any supplementary submissions we may make.

[1] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023).

Summary of key issues and Law Council recommendations

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
General matters		
There is no clear public understanding of the Government's intentions in respect of further tranches of reforms arising out of the Privacy Act Review Report, other than statements made in the Attorney-General's Second Reading Speech about upcoming 'targeted consultation'[2] on a second tranche of reforms. The proactive provision of clear details (i.e., what proposals will be addressed in each tranche of reform) will promote much-needed certainty for the multitude of sectors that expect to be impacted by these changes. This is important, noting that the practical impact of the reforms will be the outcome of a working combination of provisions in the Privacy Act, some already existing, some introduced by this tranche of reforms, and some by subsequent changes that are yet to be announced and considered.		**Recommendation 1** The Government must release a roadmap to outline its specific intentions for further tranches of reform arising out of the Privacy Act Review Report, including indicative timeframes.
Schedule 1—Privacy Reforms		
Part 1—Objects of the Act	As drafted, there is a risk that the new 'objects' paragraph 2A(aa) ('to recognise the public interest in protecting privacy') could be misconstrued or may fail to be interpreted in accordance with Australia's obligations under Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).[3]	**Recommendation 2** Amend proposed paragraph 2A(aa) (inserted by Item 1 of Schedule 1 to the Bill) to expressly refer to protecting the privacy of individuals, consistently with proposed paragraph 2A(a).

[2] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 September 2024, 25 (Mark Dreyfus, Attorney-General).
[3] International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
Part 2—Australian Privacy Principle (**APP**) Codes	Enhancing the Information Commissioner's code-making powers carries the potential for conflict and uncertainty. If Part 2 of Schedule 1 to the Bill is to remain (noting the Government agreed to this proposal in its Response to the Privacy Act Review Report),[4] then it should be amended to empower the Information Commission to advise the Minister of the necessity for an APP code (or temporary code). This change would recognise the significant expertise of the Information Commissioner, including the Commissioner's knowledge of developments in the technological and privacy sphere.	**Recommendation 3** Amend Part 2 of Schedule 1 to the Bill to empower the Information Commissioner to advise the Minister of the necessity for an APP code (or temporary code), and so that the Minister is required to consider this request prior to issuing a direction under proposed sections 26GA and 26GB of the Privacy Act.
Part 4—Children's privacy	The proposed blanket exclusion of entities providing a health service will exclude many APP entities that should be covered by the Children's Online Privacy (**COP**) Code, given that 'health service' is broadly defined in section 6FB of the Privacy Act (and includes physical and psychological health). This exclusion is also much wider than entities providing 'preventative or counselling services', as was agreed to in the Government Response to Proposal 16.5,[5] and would potentially exclude many digital providers whose tools are targeted at children.	**Recommendation 4** The breadth of the exclusion of health service providers under Item 32 of Schedule 1 to the Bill, with respect to the COP Code, should be narrowed to exclude counselling services only, not health services more generally.

[4] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 15-16, 22.
[5] Ibid 13, 30.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
	The proposed definition of 'child' as 'an individual who has not reached 18 years' will apply to all matters under the Privacy Act, and by doing so, will erode many of the existing privacy-enhancing practices that respect the agency of young people under 18 years. The proposed definition of 'child' may also result in inconsistencies in existing approaches in the health and privacy spheres, where, as a general rule, an entity may assume an individual over the age of 15 has capacity to consent, unless there is something to suggest otherwise.[6]	**Recommendation 5** The proposed definition of 'child' (inserted by Item 30 of Schedule 1 to the Bill) should be limited to the use of that term in the COP Code only, not in the Privacy Act more broadly.
Part 6—Overseas data flows	Adding clarifications after APP 8.2(a) (as proposed by Part 6 of Schedule 1 to the Bill), without addressing the broad extraterritorial reach of the Act currently, under APP 8.2(a), will create unintended consequences for the operation of this paragraph. The existing overreach of subsection 5B(3) of the Privacy Act introduces unnecessary ambiguity and complexity to the proposed cross-border provisions—provisions that, by their nature, aim to simplify compliance for APP entities, and to protect the rights of individuals whose personal information is the subject of the transfer.	**Recommendation 6** Part 6 of Schedule 1 to the Bill should be amended to add a limitation to existing subsection 5B(3) of the Privacy Act that confines the scope of the extraterritorial application of the Privacy Act, such as to 'personal information from a source in Australia'.

[6] Ibid 13.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
	Part 6 of Schedule 1 to the Bill, as drafted, does not expressly harmonise with existing cross-border mechanisms that are widely used by many APP entities to address the requirements of the European Union's *General Data Protection Regulation* (**EU GDPR**) (particularly Article 46—'transfers subject to appropriate safeguards') and APP 8. This is of concern, given that some countries may be added, or subsequently removed, by the regulations that are proposed by Part 6 of Schedule 1 to the Bill.	**Recommendation 7** APP 8.2(a) and the *Privacy Regulation 2013* (Cth) should be amended so as to reference some of the mechanisms that are widely used by APP entities to address Article 46 of the EU GDPR, such as Standard Contractual Clauses, as approved by the European Commission.
Part 8—Penalties for interference with privacy	The challenge with the proposed civil penalty provision in section 13K is that many of the matters that would give rise to the contravention are expressed as matters of principle under the APPs, and steps that require 'reasonable' (as opposed to absolute) steps to address compliance. These are typically not prescriptive or binary matters that lend themselves to a simple determination of liability. Infringement notices may be issued without entities (particularly small and medium enterprises that are not exempt small businesses under the Privacy Act) fully understanding how they should comply with sections 26WK and 26WL of the Privacy Act. There is a risk that, over time, this may disincentivise—rather than promote—open and consultative communications with the Office of the Australian Information Commissioner (**OAIC**).	**Recommendation 8** Given the principles-based obligations in the Privacy Act, further clarity is needed as to the list of factors that will give rise to infringement notices as an enforcement tool under Part 8 of Schedule 1 to the Bill. **Recommendation 9** Proposed section 13K (inserted by Part 8 of Schedule 1 to the Bill) should be amended to require, in the first instance, an OAIC notice that clearly outlines what is required to remedy the issue.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
		Recommendation 10 Sections 26WK and 26WL of the Privacy Act should be updated to address and align with the proposed provisions in Part 8 of Schedule 1 to the Bill to ensure that, together, they are facilitating a workable, consistent, and comprehensive compliance framework.
Part 15—Automated decisions and privacy policies	Key terms in Part 15 of Schedule 1 to the Bill are ambiguous and require clarity to be effective. Alignment to existing frameworks is needed to address the need for consistent practices and harmonisation with existing regimes that already regulate these types of use cases and technologies, such as the EU GDPR. The need for clarity is further reinforced by the fact that non-compliant disclosures will be the subject of new civil penalty provisions under the Bill.	**Recommendation 11** The terminology in Part 15 of Schedule 1 to the Bill should be aligned with Article 22 of the EU GDPR, which regulates 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.
	It is difficult to ascertain whether Item 88 of Schedule 1 is drafted to capture circumstances where a private sector entity has followed a series of 'decision trees', some of which may include the use of computer programs in deciding what branch of the decision tree is taken next. If the intention is to capture those decisions, it is not clear how a private sector entity would apply the test in proposed APP 1.7. It is likely that any organisation that regards itself as being captured by the requirement in new APP 1.7 will provide generic disclosure in its privacy policy (e.g., 'any information you provide	**Recommendation 12** It should be clarified whether Item 88 of Schedule 1 to the Bill, relating to automated decision making, is intended to apply to private sector entities and, if so, how private entities would apply the test in proposed APP 1.7 in circumstances where a series of decisions are made, some of which may include the use of computer programs and commercial-in-confidence information.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
	in the application process may be used by a computer program to assist with processing your application'). Such a statement will simultaneously fulfil the new obligation, but will provide no substantive information to meet the commendable objective of providing meaningful information to individuals. There is no provision in the Bill that provides for a right for individuals to request meaningful information about how substantially automated decisions with 'legal or similarly significant effect'[7] are made, consistent with Proposal 19.3 of the Privacy Act Review Report,[8] to which the Government agreed in its Response.[9] Without the introduction of this right, it is unclear how—in practice—individuals may understand how automated decisions are made through disclosure in a privacy policy alone, as this is likely to be a generic and broad statement.	**Recommendation 13** Part 15 of Schedule 1 to the Bill should be amended to include a list of factors that must be considered by APP entities, prior to determining whether an automated decision may reasonably be expected to affect the rights or interests of an individual. **Recommendation 14** Part 15 of Schedule 1 to the Bill should be amended to provide for a right for individuals to request meaningful information about how substantially automated decisions with 'legal or similarly significant effect' are made, consistent with Proposal 19.3 of the Privacy Act Review Report. **Recommendation 15** Should Part 15 of Schedule 1 to the Bill pass, significant guidance must be developed by the OAIC to assist entities to understand—and meaningfully comply with—their disclosure obligations.

[7] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 192-193.
[8] Ibid.
[9] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 11, 32.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
	Several of the proposed provisions in Part 15 of Schedule 1 of the Bill use the phrase 'substantially and directly related to making' a/the decision. As drafted, this phrase could have application beyond what is intended, as there are many ways in which personal information can be used in automated processes. For example, there is the process of filtering, or pre-screening, information to achieve a more manageable dataset that a human can make a decision on.	**Recommendation 16** The provisions in Part 15 of Schedule 1 to the Bill that refer to 'substantially and directly related to making a decision' should be redrafted to ensure that they do not apply beyond what is intended.
Schedule 2—Serious invasions of privacy		
Further consideration of Schedule 2 to the Bill, including redrafting, is required to ensure that the parameters of the tort are sufficiently clear and precise, and, by extension, fit-for-purpose, with regard to the following matters: • As drafted, the objects in clause 1 leave scope for misinterpretation and/or the risk of non-application. • Clarity is needed as to how the statutory tort for serious invasions of privacy will interact with matters currently exempt from the Privacy Act, by virtue of sections 7B and 7C. • The defences and exemptions are narrow and are not clear. For example, the proposed journalism exemption does not appear to have specific regard to publishing organisations that, in some cases, will not be the employing entity of the journalist. Harmonisation with existing regimes, such as the Australian Consumer Law, and defences relevant to defamation matters, provide a useful basis for much-needed consistency and harmonisation.	**Recommendation 17** Schedule 2 to the Bill should be redrafted to: • expressly reference the ICCPR in paragraph 1(e); • provide guidance on the meaning of 'consent' for the purpose of a defence; • clarify the interaction between matters that are currently exempt from the Privacy Act by virtue of sections 7B and 7C; and • expand the journalist exemption in clause 15 to include organisations that are involved in the publication process.

Privacy and Other Legislation Amendment Bill 2024	Issue	Recommendation
Schedule 3—Doxxing offences		
There is potential for the proposed offences in Schedule 3 to be misused. We have received feedback that proposed offences are so broad that they may unintentionally criminalise many forms of conduct that they were not intended to cover or may be misused to stifle legitimate public debate. As drafted, there is no clear definition of what behaviour constitutes 'harassing'—the term most likely applicable to doxxing. Schedule 3 to the Bill should, therefore, provide further guidance on what constitutes menacing or harassing behaviour. Moreover, the concept of 'personal data' is defined very broadly in proposed subsections 474.14C(2) and 474.14D(2) to mean information about the individual or group members that allows them to be 'identified, contacted or located'. There also appears to be no clear differentiation between penalties for certain types of 'personal data' being released.		**Recommendation 18** Schedule 3 to the Bill should be redrafted to address the concerns raised in this submission about: • the doxxing offences being drafted too broadly; • the need for guidance on what constitutes 'menacing' or 'harassing' behaviour; and • the lack of differentiation between penalties for the release of certain types of 'personal data'.

Introduction and general comments

5. The Bill, introduced into the Parliament on 12 September 2024, proposes to enact a 'first tranche'[10] of reforms to the Privacy Act to implement some of the legislative proposals that were agreed to by the Government in its September 2023 **Response** to the Privacy Act Review.[11] In addition, the Bill seeks to introduce a new statutory tort for serious invasions of privacy, and targeted criminal offences to respond to doxxing.

6. The Law Council strongly supports reform to Australia's privacy regime. The Privacy Act has now been in operation for more than 30 years, and the *Privacy Amendment (Private Sector) Act 2000* (Cth) was introduced almost 25 years ago, extending privacy obligations to the private sector to provide a minimum set of privacy protections for individuals. More recently, in 2014 changes made by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* came into force, in which all entities covered by the Privacy Act became subject to a single set of privacy principles, known as the APPs.

7. During this time, there have been significant changes to the landscape in which these pieces of legislation operate, with the advent of the internet and smartphones facilitating a proliferation of data and information, in addition to the sharing of that data. Social media, new banking and payment methods, and the movement of business to online formats (including legal transactions such as conveyancing, and anti-fraud measures) have substantially altered the way in which we use, treat and generate information. The COVID-19 pandemic also highlighted some of the shortcomings of the Privacy Act, and of Australian privacy regulation more generally.

8. Personal information is particularly vulnerable in the digital age. The volume of personal information—much of which is sensitive—being collected, stored, and shared has expanded exponentially. We are concerned that people generally do not understand how their data will be obtained, protected, or used, and that there is little to no transparency about how this is occurring.[12]

9. We recognise that the implications for an individual in the event of a privacy breach can be significant and permanent. The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) somewhat addressed public concerns about the actions and obligations related to high-profile data breaches in recent years in Australia, to the detriment of many affected individuals.[13]

10. Understandably, individuals are becoming increasingly concerned by the prospect of their personal information being misused, or used against them.[14] In addition, individuals are becoming increasingly cautious about new forms of technology, such as artificial intelligence and biometric analysis (such as facial recognition technology), due to the perception that there are inadequate mechanisms in place to protect their personal information that is collected and processed using these technologies.[15]

---

[10] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 3.
[11] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023).
[12] See Office of the Australian Information Commissioner ('OAIC)', *Australian Community Attitudes to Privacy Survey* (August 2023) 5-6.
[13] See Law Council of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (Submission to the Senate Legal and Constitutional Affairs Legislation Committee, 8 November 2022).
[14] OAIC, *Australian Community Attitudes to Privacy Survey* (August 2023) 14.
[15] Ibid 71-79.

11. We, therefore, have consistently expressed the view that the Privacy Act should be significantly enhanced to better equip individuals, organisations, and regulators to deal with emerging technologies, and new methods (and speed) of generating and sharing information. We also reiterate the importance of consistency and compatibility between Australia's existing privacy legislation and other related reforms, including with respect to recent discussions about the regulatory approaches to artificial intelligence in Australia.[16]

12. The Privacy Act Review Report, released by the Department in February 2023, similarly concluded that comprehensive reform is required to ensure that the Privacy Act is fit for purpose, and capable of addressing the heightened data risks of the digital age.[17] We engaged closely with the Department in its development of the Report by responding to a comprehensive Issues Paper and Discussion Paper.[18] In addition, we provided a detailed submission to the Department in April 2023 to inform the Government Response to the Report.[19] We commend that submission to the Committee for its consideration during this inquiry.

13. In our April 2023 submission to the Department, we stated:

> *The Law Council is supportive, at least in principle, of many of the proposals in the Report. However, it calls for and recommends that additional details be provided to give the proposals more certainty. To that end, the Law Council would welcome an opportunity to review an exposure draft bill with a view to providing further comment on legal issues raised.*[20]
>
> …
>
> *Further, given the high-level nature of the various proposals, it may be that there are further issues which are identified during the legislative process that the Law Council has not identified during this limited consultation process … Therefore, early and reasonable consultation with civil society, regulators and other interested parties and stakeholders on any exposure draft legislation will be critical.*[21]

[16] See, e.g., Law Council of Australia, *Introducing mandatory guardrails for AI in high-risk settings: Proposals Paper* (Submission to the Department of Industry, Science and Resources, 9 October 2024); *Inquiry into the opportunities and impacts of the uptake of artificial intelligence technologies in Australia* (Submission to the Senate Committee on Adopting Artificial Intelligence, 20 May 2024).
[17] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023).
[18] Law Council of Australia, *Review of the Privacy Act 1988 (Cth)—Issues Paper* (Submission to the Attorney-General's Department, 17 December 2020); *Privacy Act Review: Discussion Paper* (Submission to the Attorney-General's Department, 27 January 2022).
[19] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023).
[20] Ibid 6.
[21] Ibid 11.

14. Similarly, in our April 2024 submission to the Department in response to its consultation on civil remedies to address doxxing, we stated:

> *The Law Council reiterates its call for careful and considered consultation of any draft legislation introducing a statutory tort [for serious invasions of privacy] and other reforms designed to strengthen individual protection, to ensure that measures reflect community expectations and that the courts are empowered to weigh up the public interest in privacy against any other countervailing interests that may arise.*[22]

15. However, the Department did not provide us with an opportunity to review, or provide feedback on, an exposure draft of the Bill or any preliminary materials during its development. This is disappointing, given the legal profession's significant ongoing interest in these reforms, as evidenced by our detailed submissions to the Department in the course of the Privacy Act Review, and our subsequent offers to the Department to be consulted directly during its development of the Bill.

16. The truncated Committee inquiry timeframe is also disappointing, given the significance of the proposed reforms to Australia's approach to privacy and data law, and the fact that an exposure draft of the Bill was not subject to public consultation. Whilst the comprehensive Privacy Act Review Report was welcome after a long review process, the adaptation of many of its high-level proposals into the Bill necessitates close scrutiny to ensure that—as drafted, and in practice—these measures will achieve their policy intention and will not give rise to unintended consequences.

17. The Bill was referred to the Committee for inquiry on 19 September 2024, with a reporting date of 14 November 2024. This reporting date has resulted in a period of approximately three weeks for submissions to be provided. This timeframe has heavily impeded the ability of the Law Council, its Business Law Section, and its Constituent Bodies, to engage at a detailed level with the legislative and explanatory materials (184 pages in total).

18. In addition, several of our Constituent Bodies were unable to contribute to this submission, despite having a strong interest in these reforms. As a result, we have been unable to ascertain the views of the legal profession on a range of features in the Bill, nor have we had an opportunity to conduct a comprehensive analysis of the entirety of the proposals.

19. This truncated process is highly problematic from the perspective of broader public scrutiny of the making of Australia's laws, as part of a democratic process. This is a regrettable—and increasingly prevalent—consequence of the Parliamentary inquiry timeframes during this Parliament. This trend also undermines the Law Council's role as a membership-based peak organisation, in which we have an obligation to consult with our Constituent Bodies, Sections, and advisory committees on matters of policy.

20. Accordingly, to best assist the Committee to consider the Bill in its short inquiry period, this submission does not seek to repeat or re-prosecute, in detail, considerations raised in our earlier submissions to the Department in respect of the Privacy Act Review. Instead, our submission largely focuses on discrete drafting

[22] Law Council of Australia, *Doxxing and privacy reforms* (Submission to the Attorney-General's Department, 10 April 2024) 4.

suggestions and opportunities to minimise the risk of unintended consequences arising in relation to how various aspects of the Bill may operate in practice.

21. Nonetheless, even this is a challenging task, without a clear understanding of the Government's intentions about further tranches of reforms arising out of the 116 proposals in the Privacy Act Review Report. In his Second Reading Speech on the Bill on 12 September 2024, the Attorney-General stated that:

> *This bill is an important first step in the government's privacy reform agenda, but it will not be the last. Over the coming months, the Attorney-General's Department will develop the next tranche of privacy reform for targeted consultation, including draft provisions*.[23]

22. Whilst it is pleasing that the Government intends to continue this significant reform work, we call for a roadmap, or strategy, to publicly detail how these reforms will be progressed—similar to the materials that the Government issued in 2023 for the *Security of Critical Infrastructure Act 2018* (Cth).[24] The proactive provision of clear details (i.e., what proposals will be addressed in each tranche of reform) will promote much-needed certainty for the multitude of sectors that expect to be impacted by these significant changes.

23. Overall, while our views should be considered preliminary, and subject to potential change, we support the passage of the Bill, subject to the recommendations below, and any supplementary submissions that we make. The modernisation and strengthening of the Privacy Act are of critical importance. As such, we do not seek to impede the passage of this timely Bill.

Recommendation 1

- **The Government must release a roadmap to outline its specific intentions for further tranches of reform arising out of the Privacy Act Review Report, including indicative timeframes.**

[23] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 September 2024, 25 (Mark Dreyfus, Attorney-General).
[24] Department of Home Affairs, *Critical Infrastructure Resilience Strategy* (February 2023); *Critical Infrastructure Resilience Plan* (February 2023).

Schedule 1—Privacy reforms

Part 1—Objects of the Act

24. Item 1 of Schedule 1 to the Bill proposes to amend section 2A (Objects) of the Privacy Act by repealing existing paragraph 2A(a) ('to promote the protection of privacy of individuals') and replacing it with the following two paragraphs:

> *(a) to promote the protection of the privacy of individuals with respect to their personal information; and*
>
> *(aa) to recognise the public interest in protecting privacy;*

25. This change is consistent with Proposals 3.1 and 3.2 of the Privacy Act Review Report,[25] to which the Government agreed in its Response.[26]

26. Whilst we supported both proposals, in principle, in our 2023 submission to the Department, we raised the following matters for the Department's consideration in respect of Proposal 3.2:[27]

> *On one hand, there is potential benefit in clarifying upfront in section 2A that the Act is about the protection of personal information and recognising the public interest in protecting privacy.*
>
> *On the other hand, the Law Council acknowledges the concerns of some practitioners, including its Business Law Section's Media and Communications Committee, that Proposal 3.2 risks elevating the public interest in privacy above countervailing public interests, including the public interest in freedom of expression. Australia does not have the broad protections for the right to freedom of expression that is enshrined in the laws of the UK, USA, Canada and New Zealand, so this risk is very real.*[28]

27. We have received feedback that, as drafted, there is a risk that new paragraph 2A(aa) could be misconstrued, or may fail to be interpreted in accordance with Australia's obligations under Article 17 of the ICCPR.[29] Although the ICCPR is expressly referred to in the preamble to the Privacy Act, this risk remains, given the absence of an overarching federal Human Rights Act—which the Law Council has consistently advocated for[30]—that incorporates international human rights standards, including for the protection of privacy rights and the right to freedom of expression.

---

[25] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 18-21.
[26] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 5, 21.
[27] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 12, 42.
[28] Ibid 42.
[29] International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[30] See, e.g., Law Council of Australia, *Inquiry into Australia's Human Rights Framework* (Submission to the Parliamentary Joint Committee on Human Rights, 3 July 2023); *Federal Human Rights Charter* (Policy Position, November 2020).

28. Accordingly, proposed paragraph 2A(aa) should be amended to make clear that its scope is confined to 'the privacy of individuals', consistent with proposed paragraph 2A(a), as follows (suggested text underlined):

> *(aa) to recognise the public interest in protecting the privacy of individuals; and*

29. This change would assist in ensuring that matters arising under the Privacy Act are interpreted in line with Australia's obligations under the ICCPR to positively protect against arbitrary or unlawful interferences, or attacks against an individual's private life. This change would also more effectively reflect the changes in Schedule 2 to the Bill, in respect of the introduction of a statutory tort for serious invasions of privacy.

Recommendation 2

- **Amend proposed paragraph 2A(aa) (inserted by Item 1 of Schedule 1 to the Bill) to expressly refer to protecting the privacy of individuals, consistently with proposed paragraph 2A(a).**

Part 2—APP codes

30. Part 2 of Schedule 1 to the Bill seeks to enhance the Information Commissioner's code-making powers, consistently with Proposal 5.1 of the Privacy Act Review Report.[31]

31. In our 2023 submission to the Department, we did not support this proposal as it did not have sufficient clarity and, consequently, carried the potential for conflict and uncertainty.[32] Nonetheless, we acknowledge that the Government agreed to Proposal 5.1 in its Response to the Privacy Act Review Report.[33]

32. Accordingly, if Part 2 of Schedule 1 to the Bill is to remain, we suggest that the Information Commissioner should also be empowered to advise the Minister of the necessity for an APP code (or temporary code), and that the Minister be required to consider this request, prior to issuing a direction to the Information Commissioner to develop a code under proposed sections 26GA and 26GB.

33. This change would recognise the significant expertise of the Information Commissioner, including the Commissioner's knowledge of developments in the technological and privacy sphere. The individual who holds such a position is, therefore, well-placed to identify matters that need to be addressed by way of an APP code.

[31] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 47-48.
[32] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 47.
[33] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 15-16, 22.

Recommendation 3

- **Amend Part 2 of Schedule 1 to the Bill to empower the Information Commissioner to advise the Minister of the necessity for an APP code (or temporary code), and so that the Minister is required to consider this request prior to issuing a direction under proposed sections 26GA and 26GB of the Privacy Act.**

Part 4—Children's privacy

34. Part 4 of Schedule 1 to the Bill proposes to require the Information Commissioner to develop a Children's Online Privacy (**COP**) Code. According to the Bill's Explanatory Memorandum:

> *The COP Code would be an enforceable APP code that sets out how one or more of the APPs are to be applied or complied with in relation to the privacy of children.*[34]

35. We support the introduction of a COP Code, and we indicated such support in our April 2023 submission to the Department, in response to Proposal 16.5 of the Privacy Act Review Report.[35] We were pleased to note that the Government agreed to this proposal in its Response.[36]

36. We particularly welcome that the Bill provides that the Information Commissioner may consult with children, relevant organisations concerned with children's welfare, the eSafety Commissioner, and the National Children's Commissioner, in developing the COP Code.[37]

37. However, without further detail about the content of the COP Code, it is difficult to comment on whether Part 4 of Schedule 1 to the Bill will achieve its intended purpose and adequately protect children against arbitrary or unlawful interference with their privacy by an APP entity, in line with Article 16 of the Convention on the Rights of the Child.[38]

Exclusion of health service providers

38. Proposed subparagraph 26GC(5)(a)(iii) of the Privacy Act (inserted by Item 32 of Schedule 1 to the Bill) seeks to impose a blanket exclusion from complying with the COP Code for entities 'providing a health service'.

39. We query the rationale for this exclusion, given that the intention of the COP Code—as articulated in the Privacy Act Review Report—is to clarify the principles-based requirements of the Privacy Act in more prescriptive terms, and provide guidance on how the best interests of the child should be upheld in the design of online services.[39]

---

[34] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 25.
[35] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 59-60.
[36] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 13, 30.
[37] Privacy and Other Legislation Amendment Bill 2024 (Cth) Schedule 1, Part 4, Item 32 (new s 26GC(8) of the *Privacy Act 1988* (Cth)).
[38] *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).
[39] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 154-157.

40. The exclusion of entities providing a health service will exclude many APP entities that should be covered by the COP Code, given that 'health service' is broadly defined in section 6FB of the Privacy Act (and includes physical and psychological health). This exclusion is also much wider than entities providing 'preventative or counselling services',[40] as was agreed to in the Government Response to Proposal 16.5,[41] and would potentially exclude many digital providers whose tools are targeted at children.

41. The Explanatory Memorandum to the Bill provides that 'more general health, fitness or wellbeing apps or services may be covered by the COP Code'.[42] Nonetheless, it is likely that many such APP entities may attempt to establish that they are excluded from the COP Code as being 'entities … providing a health service' under proposed subparagraph 26GC(5)(a)(iii).

42. In addition, we query the necessity of a blanket exclusion, noting that proposed subsections 26GC(5)(b) and (7) allow for the OAIC to specify within the COP Code itself which APP entities are, and are not, covered.[43] Of note, the Explanatory Memorandum to the Bill states that the COP Code may specify that 'a provider of a health service is bound by the COP Code'.[44]

Recommendation 4

- **The breadth of the exclusion of health service providers under Item 32 of Schedule 1 to the Bill, with respect to the COP Code, should be narrowed to exclude counselling services only, not health services more generally.**

Definition of 'child'

43. Item 30 of Schedule 1 to the Bill proposes to define 'child' under subsection 6(1) of the Privacy Act as 'an individual who has not reached 18 years'. This insertion is consistent with Proposal 16.1 of the Privacy Act Review Report.[45] The commentary in the Privacy Act Review Report states:

> *Defining a child as an individual under 18 years of age will allow for the development of child-specific privacy protections in the Act. This position would also be consistent with the* Online Safety Act 2021 *(Cth), the UK Age Appropriate Design Code and Ireland's* Data Protection Act.[46]

44. In its Response, the Government agreed to this proposal, and acknowledged that children are particularly vulnerable to online harms.[47]

45. However, it is important to ensure consistency for individuals and businesses when introducing new definitions into the Privacy Act. Whilst the proposed definition of 'child' is consistent with that in the *Online Safety Act 2021* (Cth), it is possible that defining a child as an individual who has not reached 18 years, as proposed in the Bill, may lead to unintended consequences. Specifically, Item 30 of Schedule 1, as

[40] Ibid 157.
[41] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 13, 30.
[42] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 42.
[43] Ibid.
[44] Ibid.
[45] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 147.
[46] Ibid.
[47] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 13, 29.

drafted, will apply to all matters under the Privacy Act and, by doing so, will erode many of the existing privacy-enhancing practices that respect the agency of young people under 18 years.

46. The proposed definition of 'child' may also result in inconsistencies with existing approaches in the health and privacy spheres, especially given that the Bill does not propose to define 'consent' or 'capacity' in respect of children. We note the generally accepted position regarding a child's capacity to consent, as summarised in the Government Response to Proposal 16.2 (emphasis added):

> *… the Government agrees in-principle that the Privacy Act should codify the principle that valid consent must be given with capacity … The guidance provides sufficient flexibility by allowing entities to decide if an individual under the age of 18 has capacity to consent on a case-by-case basis. If that is not practical, as a general rule, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.*[48]

47. We reiterate the importance of consistency for individuals and businesses when introducing the COP Code, and the need to have regard to the current industry codes that are being prepared by the eSafety Commissioner.[49] It is also critically important that entities are assisted to understand how to assess an individual's capacity to provide consent.

48. To address the concerns raised above, and to overcome any uncertainty as to the intention of Item 30 of Schedule 1 of the Bill, the proposed definition of 'child' should be limited to the use of that term in the COP Code only.

Recommendation 5

- **The proposed definition of 'child' (inserted by Item 30 of Schedule 1 to the Bill) should be limited to the use of that term in the COP Code only, not in the Privacy Act more broadly.**

Part 5—Security, retention and destruction

49. Part 5 of Schedule 1 to the Bill seeks to clarify the steps that entities are required to take to keep personal information secure.[50]

50. Item 34 of Schedule 1 to the Bill inserts APP 11.3 into Schedule 1 of Privacy Act, to clarify that 'reasonable steps', for the purposes of APPs 11.1 and 11.2, includes technical and organisational measures. According to the Bill's Explanatory Memorandum:

> *Examples of technical measures include protecting personal information through physical measures, and software and hardware—for example through securing access to premises, encrypting data, anti-virus software and strong passwords.*
>
> *Examples of organisational measures include steps, processes and actions an entity should put in place—for example, training employees*

[48] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 13.
[49] See eSafety Commissioner, *Industry codes and standards* (Web Page, 2024).
[50] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 7.

on data protection, and developing standard operating procedures and policies for securing personal information.[51]

51. This insertion is consistent with Proposal 21.1 of the Privacy Act Review Report,[52] to which the Government agreed to in its Response.[53] We support this change, and consider that it will provide further guidance and clarification to APP entities.

Part 6—Overseas data flows

52. Part 6 of Schedule 1 to the Bill seeks to provide greater certainty about when personal information can be disclosed overseas, and increase mechanisms to facilitate the free flow of information across national borders, while ensuring that the privacy of individuals is respected.[54]

53. We welcome these proposed amendments and consider that they will clarify and simplify the cross-border requirements and assist APP entities to address the relevant requirements. In particular, we support legislative clarity about exceptions under the Bill, covering circumstances where an entity reasonably believes the recipient of the information is subject to a law or binding scheme that is substantially similar to the APPs.[55]

54. To complement these amendments, we support the OAIC providing guidance for APP entities as to those overseas countries that have sufficient privacy or data protection laws for the purpose of the exception in APP 8.2(a).

55. In addition, the Bill is a missed opportunity to make other necessary changes to the Privacy Act and APPs in respect of overseas data flows.

56. In its Response to the Privacy Act Review Report, the Government agreed that:

- further consultation should be undertaken on the extraterritorial provisions of the Privacy Act to determine if an additional requirement in subsection 5B(3) that personal information is connected to Australia is necessary to narrow the current scope (Proposal 23.1);[56] and
- a mechanism should be introduced to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a) (Proposal 23.2).[57]

57. The Government also agreed in principle to Proposal 23.3 that standard contractual clauses for transferring personal information to countries that are not prescribed should be developed and made available to businesses.[58]

58. We supported each of these proposals in our April 2023 submission to the Department, and continue to do so.[59]

---

[51] Ibid 43.
[52] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 221.
[53] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 8, 33.
[54] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 7.
[55] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 1, item 36 (new s 100(1A) of the *Privacy Act 1988* (Cth)).
[56] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 16, 34.
[57] Ibid.
[58] Ibid.
[59] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 33-36, 75.

Extraterritoriality

59. We suggest that the Government should address the existing ambiguity in subsection 5B(3) of the Privacy Act within the Bill as a priority, given that Items 36 to 39 of Schedule 1 to the Bill propose to make changes to the APPs with respect to overseas data flows.

60. We canvassed our concerns with this ambiguity in our November 2022 submission to this Committee during its inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,[60] and in our April 2023 submission to the Department, as follows:[61]

> *…there are many foreign corporations that carry on business in Australia that are headquartered outside Australia and carry on business in many other jurisdictions. Foreign banks and airlines are obvious examples. As currently drafted, section 5B(3) [of the Privacy Act] purports to apply the provisions of the Act to the conduct of these entities in respect of conduct that has no connection with Australia.*
>
> *The Law Council queries why, as a matter of policy and international comity, Australian law should seek to regulate the conduct of a European airline in respect of its handling of passenger data for flights between destinations that do not include an airport in Australia, or the conduct of an American bank in respect of its purely domestic American banking business, simply because that airline or that bank happens to carry on business in Australia.*
>
> *The Law Council is therefore of the strong view that for Australian law to apply to the extraterritorial conduct of such an entity, there should be a rational nexus between the conduct and Australia.*[62]

These concerns remain.

61. Adding clarifications after APP 8.2(a) (as proposed by Part 6 of Schedule 1 to the Bill), without addressing the current broad extraterritorial reach of the Act, under APP 8.2(a), will create unintended consequences for the operation of this paragraph.

62. The existing overreach of subsection 5B(3) of the Privacy Act introduces unnecessary ambiguity and complexity to the proposed cross-border provisions—provisions that, by their nature, aim to simplify compliance for APP entities, and to protect the rights of individuals whose personal information is the subject of the transfer. A limitation, therefore, should be added to subsection 5B(3) that confines the scope of the extraterritorial application of the Privacy Act, such as to 'personal information from a source in Australia'.

63. We acknowledge that the Government has agreed to consult on this matter,[63] pursuant to Proposal 23.1 of the Privacy Act Review Report. As such, if the Government is not minded to address the current overreach of subsection 5B(3) of

---

[60] See Law Council of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (Submission to the Senate Legal and Constitutional Affairs Legislation Committee, 8 November 2022) 8-11.
[61] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 33-36, 75.
[62] Ibid 33-34.
[63] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 16, 34.

the Privacy Act in this Bill in accordance with our suggestion above, then we suggest that the necessary consultations take place as a matter of priority.

Recommendation 6

- **Part 6 of Schedule 1 to the Bill should be amended to add a limitation to existing subsection 5B(3) of the Privacy Act that confines the scope of the extraterritorial application of the Privacy Act, such as to 'personal information from a source in Australia'.**

Express references to mechanisms and safeguards

64. As drafted, Part 6 of Schedule 1 to the Bill does not expressly harmonise with existing cross-border mechanisms widely used by many APP entities to address the requirements of the EU GDPR and APP 8.

65. Accordingly, we suggest that the Bill should amend APP 8.2(a)—and the Privacy Regulation should also be amended—so as to expressly reference some of the mechanisms that are widely used by APP entities to address Article 46 of the EU GDPR ('transfers subject to appropriate safeguards'). Reference should particularly be made to safeguards, such as Standard Contractual Clauses, adopted by the European Commission in accordance with the examination procedure referred in Article 93(2) of the EU GDPR.[64]

66. Express references to these mechanisms will help to avoid the unintended consequences of potentially conflicting measures being described, or adopted, by APP entities, especially if some countries may be added, or subsequently removed, by the regulations that are proposed by Part 6 of Schedule 1 to the Bill.

Recommendation 7

- **APP 8.2(a) and the Privacy Regulation should be amended so as to reference some of the mechanisms that are widely used by APP entities to address Article 46 of the EU GDPR, such as Standard Contractual Clauses, as approved by the European Commission.**

Part 8—Penalties for interference with privacy

67. Part 8 of Schedule 1 to the Bill proposes to introduce various new enforcement powers, including:

    - a new civil penalty for all interferences with privacy (up to 2000 penalty units);[65] and
    - the power for the Information Commissioner to issue infringement notices for breaches of the APPs and non-compliant data breach statements (up to 200 penalty units).[66]

68. These amendments are broadly consistent with Proposals 25.1 and 25.2 of the Privacy Act Review Report,[67] to which the Government agreed in its Response.[68]

---

[64] *General Data Protection Regulation* (EU) 2016/679 Art 46(2).
[65] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 1, item 56 (new s 13H of the *Privacy Act 1988* (Cth)).
[66] Ibid Sch 1, item 56 (new s 13K of the *Privacy Act 1988* (Cth)).
[67] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 253-258.
[68] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 20, 35.

In our April 2023 submission, we indicated that we supported Proposal 25.1 in part, noting that these changes would add a significant level of complexity to the enforcement regime in the Privacy Act.[69] We supported Proposal 25.2, but observed that there will be a need to consider how this amendment will be applied, also noting the role of the OAIC.[70]

69. We are generally supportive of the various proposed enforcement mechanisms in Part 8 of Schedule 1 to the Bill. We caution, however, that the proposed mechanisms may not be appropriate if the Privacy Act is eventually extended to smaller organisations, noting that the Government agreed, in principle, to the removal of the small business exemption in its Response to the Privacy Act Review Report.[71]

70. Our fundamental concern, currently, is whether each of the penalties is sufficiently clear and proportionate to the offence, and that like matters or contraventions are addressed in a like manner. In this respect, we query whether the principles-based obligations listed in proposed section 13K of the Privacy Act (inserted by Item 56 of Schedule 1 to the Bill) are sufficiently prescriptive to enable certainty in compliance by entities.

71. The challenge with proposed section 13K is that many of the matters that would give rise to the contravention are expressed as matters of principle under the APPs, and steps that require 'reasonable' (as opposed to absolute) steps to address compliance. These are typically not prescriptive or binary matters that lend themselves to a simple determination of liability.

72. Many of the key determinations of OAIC findings in respect of breaches of policy or notice provisions have been the subject of considerable investigations examining very different practices or contraventions. For example:

- in the Clearview AI Determination,[72] the OAIC investigated the practices of collection and use involving facial recognition technology, and the underlying business model of the APP entity. The OAIC investigation found, amongst other things, that Clearview breached APPs 3.3, 3.4, 3.5 and 5;
- a similarly detailed review was required in the 7-Eleven Determination.[73] The convenience store group was found to have interfered with customers' privacy by collecting sensitive biometric information that was not reasonably necessary for its functions, and without adequate notice or consent; and
- in other matters, the determinations require an investigation into conceptually very different matters, such as:
  - the speed of the data breach response and other more procedural matters;
  - whether the respondent took 'reasonable steps' to complete the assessment of the incident within 30 days; and/or

[69] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 36-37, 76.
[70] Ibid 37.
[71] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 6, 23.
[72] OAIC, Commissioner initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr54 (14 October 2021).
[73] OAIC, Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr50 (29 September 2021).

- whether the statement provided to the Information Commissioner was provided 'as soon as practicable'.[74]

73. It may be informative for the Committee to compare the proposed power for the OAIC to issue infringement notices under Part 8 of Schedule 1 to the Bill with the powers available to other regulators, such as the Australian Securities and Investments Commission (**ASIC**)[75] and the Australian Competition and Consumer Commission (**ACCC**).[76]

74. ASIC's power to issue an infringement notice appears to be circumscribed by the consideration that it is more likely to issue an infringement notice as an alternative to court-based action, if:

- the alleged misconduct is relatively minor or less serious, and does not indicate a broader pattern of misconduct by the entity or within an industry;
- ASIC is not required to make a complex assessment of facts to evaluate whether the alleged misconduct contravened the law; and
- an infringement notice would be a proportionate enforcement response, considering the nature and size of the entity and the need for general and specific deterrence.[77]

75. Likewise, the ACCC's guidance indicates that the ACCC will only consider issuing an infringement notice where it is likely to seek a court-based resolution, should the recipient of the notice choose not to pay.[78] Before issuing an infringement notice, the ACCC will have turned its mind to the prospect of non-compliance, and be prepared to proceed to court as a likely alternative.[79]

76. In light of the wider regulatory landscape, we suggest that greater clarity is required as to what type of privacy contraventions will lead to:

- what degree of harm—if any—to the individual; and
- what types of enforcement mechanisms.

This clarity will, in turn, inform the type of regulatory response or intervention by the regulator. This will be pertinent to all APP entities, but especially to those in heavily regulated industries (i.e., the critical infrastructure sectors and health and financial services firms), where data-related contraventions may lead to multiple regulatory obligations and interventions.

77. Further consideration should be given to how effective infringement notices will be as an enforcement tool, considering the principles-based obligations in the Privacy Act. These obligations are notably less prescriptive than the requirements under the *Australian Securities and Investments Commission Act 2001* (Cth) and the Australian Consumer Law, as found in Schedule 2 to the *Competition and Consumer Act 2010* (Cth), for which infringement notices may be issued with more certainty, in the event of contravention.

---

[74] See, e.g., Pacific Lutheran College (Privacy) [2023] AICmr98 (24 October 2023).
[75] *Australian Securities and Investments Commission Act 2001* (Cth) ss 12CB, 12GX, 12GXA.
[76] *Competition and Consumer Act 2010* (Cth) Sch 2 ('Australian Consumer Law').
[77] Australian Securities and Investments Commission ('ASIC'), *Infringement notices: Your rights* (Information Sheet 275, March 2023).
[78] Australian Competition and Consumer Commission ('ACCC'), *Infringement notices* (Guidelines, July 2020) 3.
[79] Ibid.

78. We also caution that infringement notices may be issued without entities (particularly small and medium enterprises that are not exempt small businesses under the Privacy Act) fully understanding how they should comply with sections 26WK and 26WL of the Privacy Act. There is a risk that, over time, this may disincentivise—rather than promote—open and consultative communications with the OAIC.

79. To assist in addressing these concerns, consideration should be given to:

(a) amending proposed section 13K to require, in the first instance, an OAIC notice that clearly sets out what is needed to remedy the issue; and

(b) reviewing sections 26WK and 26WL of the Privacy Act to ascertain whether these provisions (or, at a minimum, the OAIC's data breach statement template form for the purpose of section 26WK) are adequately facilitating a workable and comprehensible compliance framework.

Recommendation 8

- **Given the principles-based obligations in the Privacy Act, further clarity is needed as to the list of factors that will give rise to infringement notices as an enforcement tool under Part 8 of Schedule 1 to the Bill.**

Recommendation 9

- **Proposed section 13K (inserted by Part 8 of Schedule 1 to the Bill) should be amended to require, in the first instance, an OAIC notice that clearly outlines what is required to remedy the issue.**

Recommendation 10

- **Sections 26WK and 26WL of the Privacy Act should be updated to address and align with the proposed provisions in Part 8 of Schedule 1 to the Bill to ensure that, together, they are facilitating a workable, consistent, and comprehensive compliance framework.**

Part 15—Automated decisions and privacy policies

80. Part 15 of Schedule 1 to the Bill seeks to enhance transparency about automated decisions that significantly affect the interests of an individual,[80] consistent with Proposals 19.1 and 19.2 of the Privacy Act Review Report.[81]

81. We have consistently emphasised the need for public and private entities to build public trust and confidence in automated decision-making processes, by ensuring that these processes are transparent, and that clear criteria exist about the factors considered, especially where the personal information of individuals is used.[82]

82. Accordingly, we were supportive of the three proposals in the Privacy Act Review Report relating to automated decision-making (Proposals 19.1 to 19.3). Pleasingly,

[80] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 7.
[81] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 190-191.
[82] See, e.g., Law Council of Australia, *Safe and Responsible AI in Australia* (Submission to the Department of Industry, Science and Resources, 17 August 2023) 24-28; *Positioning Australia as a leader in digital economy regulation—Automated decision making and AI regulation* (Submission to the Department of Prime Minister and Cabinet).

the Government was similarly supportive of each of these proposals in its Response.[83]

83. However, we query whether the provisions, as currently drafted, are fit for purpose. Key terms in Part 15 of Schedule 1 to the Bill are ambiguous and require clarity to be effective. For instance, we are concerned that the Bill fails to provide certainty as to the meaning of 'automated decisions' and imposes an unnecessarily high bar with the proposed requirement for the computer program to 'make, or do a thing that is substantially and directly related to making, a decision' (emphasis added).[84]

84. The Explanatory Memorandum to the Bill says the following about the meaning of 'computer program':

> *The term 'computer program' in APP 1.7(a) is intended to take its ordinary meaning and encompass a broad range of matters, including pre-programmed rule-based processes, artificial intelligence and machine learning processes to make a computer execute a task.*[85]

85. Further, the terminology used in Article 22 of the EU GDPR makes reference to (emphasis added):

> *… decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,*[86]

This is a very different test to what is proposed under the Bill, raising potential issues as to harmonisation and interoperability between the Privacy Act and the EU GDPR. Alignment to existing frameworks is required to address the need for consistent practices and harmonisation with existing regimes that already regulate this field of activity and type of technology. This need for clarity is further reinforced by the fact that non-compliant disclosures will be the subject of new civil penalty provisions under the Bill.

86. We also make the following general observations. The amendments to the Privacy Act in Part 15 of Schedule 1 to the Bill:

- appear to have been drafted in contemplation of automated decision-making processes in the public sector context, and bear less relevance to the private sector; and
- stop short of introducing a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made, in line with Proposal 19.3 of the Privacy Act Review Report (to which the Government agreed in its Response).[87]

[83] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 11, 32.
[84] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 1, pt 15, item 88 (new cl 1.7(a) of Schedule 1 to the *Privacy Act 1988* (Cth)).
[85] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77.
[86] European Union, *General Data Protection Regulation* (EU) 2016/679 Art 22(1).
[87] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 11, 32.

Recommendation 11

- **The terminology in Part 15 of Schedule 1 to the Bill should be aligned with Article 22 of the EU GDPR, which regulates 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.**

Meaning of 'automated decisions'

87. Item 88 of Schedule 1 inserts APPs 1.7 to 1.9 to require entities to include additional information relating to automated decisions in an entity's privacy policy, where:

    - the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision; and
    - the decision could reasonably be expected to significantly affect the rights or interests of an individual; and
    - personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision.[88]

88. We acknowledge that, in the case of a public sector entity, an automated decision may be a single decision, as set out pursuant to legislation or a regulation.

89. However, in the case of private sector entities, the provision of goods or services, and/or the terms on which they are provided may be the result of several decisions that follow a series of 'decision trees'—some of which may include the use of computer programs in deciding what branch of the decision tree is taken next. This may be a complex process, potentially involving sensitive commercial-in-confidence information, that is not appropriate for disclosure in that entity's privacy policy.

90. It is difficult to ascertain whether Item 88 is drafted to capture these circumstances. If it is, it is not clear how a private sector entity would apply the test in proposed APP 1.7. The Committee should seek clarification from the Department on this matter.

91. If the decision could reasonably be expected to 'significantly affect the rights or interests of an individual',[89] decisions in the finance, insurance, and health sectors would likely all be captured. Likewise, many industries use computer programs to filter groups in terms of products and pricing. This practice can have significant consequences for individuals, although we cannot envisage the requirement for disclosure in a privacy policy providing substantive benefit in some circumstances.

92. By contrast, one of the biggest users of computer programs in making decisions is consumer credit, which is regulated under Part IIIA of the Privacy Act, and to which the APPs do not apply.

93. We are concerned that entrusting APP entities with the discretion to make their own determination as to what may constitute an automated decision may result in some entities forming erroneous views and not including information in their privacy policies that should be included.

[88] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 1, pt 15, item 88 (new cl 1.7 of Schedule 1 to the *Privacy Act 1988* (Cth)).
[89] Ibid (new cl 1.7(b) of Schedule 1 to the *Privacy Act 1988* (Cth)).

94. We recognise that Part 15 of Schedule 1 is not proposed to come into force until two years after the Bill passes the Parliament and receives Royal Assent.[90] Nonetheless, it is likely that any organisation that regards itself as being captured by the requirement in new APP 1.7 will provide generic disclosure in its privacy policy (e.g., 'any information you provide in the application process may be used by a computer program to assist with processing your application'). Such a statement will simultaneously fulfil the new obligation, but will provide no substantive information to meet the commendable objective of providing meaningful information to individuals.

95. Consideration should also be given to amending Part 15 of Schedule 1 to the Bill so that it includes a list of factors that must be considered by APP entities, prior to determining whether an automated decision may reasonably be expected to significantly affect the rights or interests of an individual.

96. Moreover, as foreshadowed in the Government Response, significant guidance must be provided by the OAIC to assist entities to meaningfully comply with their new obligation.[91]

97. Further, there is no provision in the Bill that provides for a right for individuals to request meaningful information about how substantially automated decisions with 'legal or similarly significant effect'[92] are made, consistent with Proposal 19.3 of the Privacy Act Review Report,[93] to which the Government agreed in its Response.[94] Part 15 of Schedule 1 to the Bill should be amended to include this right.

98. Without the introduction of this right, it is unclear how—in practice—individuals may understand how automated decisions are made through disclosure in a privacy policy alone, as this is likely to be a generic and broad statement. Further, as organisations are being given substantial time to prepare to comply with the obligations proposed in the Bill about automated decision-making, they should also be in a position to provide meaningful information to individuals, in line with Proposal 19.3.

Recommendation 12

- **It should be clarified whether Item 88 of Schedule 1 to the Bill, relating to automated decision making, is intended to apply to private sector entities and, if so, how private entities would apply the test in proposed APP 1.7 in circumstances where a series of decisions are made, some of which may include the use of computer programs and commercial-in-confidence information.**

Recommendation 13

- **Part 15 of Schedule 1 to the Bill should be amended to include a list of factors that must be considered by APP entities, prior to determining whether an automated decision may reasonably be expected to affect the rights or interests of an individual.**

[90] Ibid cl 2.
[91] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 11.
[92] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 192-193.
[93] Ibid.
[94] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 11, 32.

Recommendation 14

- **Part 15 of Schedule 1 to the Bill should be amended to provide for a right for individuals to request meaningful information about how substantially automated decisions with 'legal or similarly significant effect' are made, consistent with Proposal 19.3 of the Privacy Act Review Report.**

Recommendation 15

- **Should Part 15 of Schedule 1 to the Bill pass, significant guidance must be developed by the OAIC to assist entities to understand—and meaningfully comply with—their disclosure obligations.**

Meaning of 'substantially and directly related to making a decision'

99. Several of the proposed provisions in Part 15 of Schedule 1 of the Bill use the phrase 'substantially and directly related to making' a/the decision.[95] Yet, to satisfy both 'substantially' and 'directly' is a high and narrow test. Further, it is difficult to apply such a test if the definition of a 'decision' is not clear. As outlined above, where a decision was ultimately made at the end of multiple filters or 'branches' of a decision tree, it will be difficult for entities to know what is required to be disclosed in a privacy policy under proposed APP 1.7.

100. Whilst the test is narrow, the meaning of 'decision' appears to be simultaneously broadened by proposed APP 1.9 by providing that:

- making a decision includes refusing or failing to make a decision; and
- a decision may affect the rights or interests of an individual, whether adversely or beneficially.[96]

Consequently, it is unclear from the Bill whether the meaning of 'decision' is intended to follow that of the EU GDPR, or that under Australian administrative law.

101. There are many ways in which personal information can be used in automated processes. For example, there is the process of filtering, or pre-screening, information to achieve a more manageable dataset that a human can make a decision on. In these circumstances, an individual could argue that, because they were 'screened out' before reaching the human decision-maker, the computer program has done something that is 'substantially and directly related' to the making of the final decision, and that their rights were affected because their information never progressed to the human decision-maker.

102. Without knowledge of what reforms may be proposed in a subsequent bill, it is difficult to ascertain whether unintended consequences may flow from this amendment. To assist us in this regard, we reiterate Recommendation 1 of our submission, that the Government must release a legislative roadmap to outline its intentions in respect of further tranches of reforms arising out of the Privacy Act Review Report.

[95] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 1, pt 15, item 88 (new cl 1.7(a) and (c) and 1.8(c) of Schedule 1 to the *Privacy Act 1988* (Cth)).
[96] Ibid (new cl 1.9(a) and (c) of Schedule 1 to the *Privacy Act 1988* (Cth)).

103. In the interim, we suggest that these provisions be redrafted, to ensure that their practical application is workable. As drafted, the phrase 'substantially and directly related to making a decision' could have application beyond what is intended.

Recommendation 16

- **The provisions in Part 15 of Schedule 1 to the Bill that refer to 'substantially and directly related to making a decision' should be redrafted to ensure that they do not apply beyond what is intended.**

Schedule 2—Serious invasions of privacy

104. Schedule 2 to the Bill proposes to establish a cause of action in tort for serious invasions of privacy, broadly consistent with Proposal 27.1 of the Privacy Act Review Report,[97] to which the Government agreed, in-principle, in its Response.[98]

105. Under the Bill, individuals would have a cause of action under this statutory tort if they suffer an invasion of their privacy, either by an intrusion into their seclusion, or by misuse of information, when:

- a person in their position would have had a reasonable expectation of privacy in all the circumstances; and
- the invasion of privacy was intentional or reckless; and
- the invasion of privacy was serious.[99]

106. In our April 2023 submission to the Department, we acknowledged that there are diverse views within the legal profession on the introduction of a statutory tort for serious invasions of privacy.[100] Of note, our Business Law Section's (**BLS**) Media and Communications Committee did not support Proposal 27.1, instead favouring increased resourcing being provided to the OAIC to assist in enforcement.[101]

107. On balance, and having regard to developing international jurisprudence in this area,[102] we provided in-principle support for the introduction of a statutory tort in our April 2023 submission, in the form recommended by the Australian Law Reform Commission (**ALRC**),[103] and on the condition that there are sufficiently high thresholds in place to ensure actions are limited to serious invasions of privacy.[104]

108. In our submission to the Department, we further remarked that:

> *It is expected that reasonable minds across the legal profession will differ in respect of any introduction of a new cause of action which would expand tort law in Australia, as would be the case should this proposal*

---

[97] Attorney-General's Department, *Privacy Act Review Report 2022* (February 2023) 281-287.
[98] Commonwealth of Australia, *Government Response: Privacy Act Review Report* (September 2023) 19, 36.
[99] Privacy and Other Legislation Amendment Bill 2024 (Cth) Sch 2, item 10 (new cl 7(1) of Schedule 2 to the *Privacy Act 1988* (Cth)).
[100] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 39.
[101] Ibid 79.
[102] See, eg, *Lloyd v Google* [2021] UKSC 50.
[103] Australian Law Reform Commission ('ALRC'), *Serious Invasions of Privacy In the Digital Era* (Report 123, June 2014).
[104] Law Council of Australia, *Government response to the Privacy Act Review Report* (Submission to the Attorney-General's Department, 13 April 2023) 39.

be adopted. It is therefore essential that certainty and clarity in respect of the scope of any such cause of action be provided.[105]

… given the need for further detailed consultation on the model and scope of the tort, which will be very important to get right, the Law Council considers that the introduction of a statutory tort for serious invasions of privacy may be most appropriately progressed through a subsequent tranche of reforms to Australia's privacy regime, as opposed to being included in any first tranche.[106]

109. We reiterated these positions in our April 2024 submission to the Department on doxxing.[107]

110. We continue to support, in principle, the introduction of a statutory tort for serious invasions of privacy in the form recommended by the ALRC. However, there are several drafting and practical matters in respect of various clauses in Schedule 2 to the Bill that we wish to raise for the Committee's scrutiny and consideration, set out below.

Clause 1—Objects of this Schedule

111. We have received feedback that the proposed objects of the Schedule in clause 1, specifically paragraphs (c), (d), and (e), are vague and quite repetitive. As drafted, these objects leave scope for misinterpretation and/or the risk of non-application.

112. For example, the scope of object (e) ('implement Australia's international obligations in relation to privacy') is very broad. Although reference is made in the Bill's Explanatory Memorandum to Article 17 of the ICCPR,[108] the ICCPR should be directly referenced within the text of Schedule 2 to the Bill, as follows (suggested text underlined):

> *(e) implement Australia's international obligations in relation to privacy, <u>including obligations under the International Covenant on Civil and Political Rights</u>.*

Clause 7—Cause of action

113. We have also received feedback from our BLS Media and Communications Committee that:

- subclause 7(1) should be drafted so that the establishment of the tort is expressly subject to the establishment of the public interest element at subclause 7(3); and
- the scope of proposed subclause 7(6)(b) and (c) is unduly broad and could give rise to interlocutory applications (for example, applications for preliminary discovery) to uncover the motive of a journalist's source. Such interlocutory applications are likely to stifle legitimate free speech and have a chilling effect on journalism.

---

[105] Ibid 38.
[106] Ibid 40.
[107] Law Council of Australia, *Doxxing and privacy reforms* (Submission to the Attorney-General's Department, 10 April 2024) 2-4.
[108] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 82.

114. If exempt practices and organisations under the Privacy Act are to be exempt from claims under the statutory tort, then a new paragraph (e) should be inserted in proposed subclause 7(1) to provide as follows (or similar):

> *(e) and the defendant, and the practice or practices in question, are not otherwise exempt from the operation of this Act.*

Clause 8—Defences

115. We have received feedback from our BLS Media and Communications Committee that the defence of public interest, found in section 29A of the *Defamation Act 2005* (NSW), and its equivalent in other states and territories, should be added to the list of 'related defences' at subclause 8(3). In addition, the list of 'related defences' should be expressly specified to be a non-exclusive list.

Clause 9—Interim injunctions

116. Careful consideration must be given to the interim injunction procedure at clause 9 to ensure that procedures cannot be used to circumvent the strict requirements for obtaining a suppression or non-publication order (for example: the regime in Part VAA of the *Federal Court Act 1975* (Cth)).

Clause 11—Damages

117. Careful consideration must be given to the types of damages awards available to claimants, including giving consideration to making those types of damages consistent with those available to claimants in defamation actions.

Clause 15—Exemption for journalists

118. Clause 15 of Schedule 2 provides as follows:

> *This Schedule does not apply to an invasion of privacy by any of the following to the extent that the invasion of privacy involves the collection, preparation for publication or publication of journalistic material:*
>
> *(a) a journalist;*
>
> *(b) an employer of a journalist;*
>
> *(c) a person assisting a journalist who is employed or engaged by the journalist's employer;*
>
> *(d) a person assisting a journalist in the person's professional capacity.*

119. We query the appropriateness of the exemptions from liability for journalists in clause 15, including that the exemption does not appear to have specific regard to organisations that are involved in the publishing process, to the extent that they are not the employing entity of the journalist.

120. In particular, we have received feedback that:

- whilst, in some cases, a publisher will be deemed 'an employer of a journalist', in other cases, publishers of material may not readily fall into the exempt categories provided under proposed subclause 15(1). For instance, the

proposed exemption fails to recognise that publishers often source material from self-employed journalists or other content providers;

- the exemption for journalists will not cover many journalists' sources, with the effect being that tortious action could be taken against a source instead of a journalist as a means of bypassing the exemption. This omission has the potential to render the journalism exemption nugatory in some circumstances and, as expressed by the BLS Media and Communications Committee, will mean that the tort will have a chilling effect on legitimate free speech;
- the definition of 'journalistic material' in proposed subclause 15(3) with reference to 'news, current affairs or a documentary' is unduly narrow in scope, despite the evolving nature of information transmission methods and delivery, and the broad range of topics they may touch upon—thereby risking journalistic freedom to pursue matters of genuine public interest; and
- the definition of 'journalistic material' is also unduly narrow insofar as it will not cover many other legitimate forms of free speech (for example, works including biographies or memoirs) or other media content that otherwise offers a valuable contribution to cultural and public life (for example, comedy, satire and other entertainment).

121. Harmonisation with existing regimes, such as the Australian Consumer Law, and the defences that are relevant to defamation proceedings, provide a useful basis for the much-needed consistency and harmonisation with respect to exemptions under the Bill. For example, the journalist exemption in clause 15 should be expanded to include organisations that are involved in the publication process.

Recommendation

122. The matters identified above demonstrate that Schedule 2 to the Bill must be redrafted to ensure that the parameters of the statutory tort are sufficiently clear and precise, and, by extension, fit-for-purpose.

Recommendation 17

- **Schedule 2 to the Bill should be redrafted to:**
  - **expressly reference the ICCPR in paragraph 1(e);**
  - **provide guidance on the meaning of 'consent' for the purpose of a defence;**
  - **clarify the interaction between matters that are currently exempt from the Privacy Act by virtue of sections 7B and 7C; and**
  - **expand the journalist exemption in clause 15 to include organisations that are involved in the publication process.**

Schedule 3—Doxxing offences

123. Schedule 3 to the Bill proposes to amend the *Criminal Code Act 1995* (Cth) to introduce new offences targeting the release of personal data using a carriage service in a manner that would be menacing or harassing—a practice that is colloquially known as 'doxxing' (or 'doxing').[109]

124. Proposed subsection 474.17C(1) of the Criminal Code—inserted by Item 1 of Schedule 3 to the Bill—provides that a person commits an offence if:

> *(a) the person uses a carriage service to make available, publish or otherwise distribute information; and*
>
> *(b) the information is personal data of one or more individuals; and*
>
> *(c) the person engages in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those individuals.*
>
> *Note: Publishing the name, image and telephone number of an individual on a website and encouraging others to repeatedly contact the individual with violent or threatening messages is an example of conduct (commonly referred to as doxxing) that is covered by this subsection.*

125. The Bill proposes that this offence will carry a penalty of imprisonment for six years.

126. Further, proposed subsection 474.17D(1) of the Criminal Code provides that a person commits an offence if:

> *(a) the person uses a carriage service to make available, publish or otherwise distribute information; and*
>
> *(b) the information is personal data of one or more members of a group; and*
>
> *(c) the person engages in the conduct in whole or in part because of the person's belief that the group is distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin; and*
>
> *(d) the person engages in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those members.*
>
> *Note: Publishing the names, images and residential addresses of members of a private online religious discussion group across multiple websites and encouraging others to attend those addresses and block entryways, or otherwise harass the members of that group, is an example of conduct (commonly referred to as doxxing) that is covered by this subsection.*

127. The Bill proposes that this offence will carry a penalty of imprisonment for seven years.

[109] 'Doxxing' is an abbreviation for 'dropping documents': eSafety Commissioner, *Doxing* (Web Page, 2024).

128. The term 'doxxing' is very broad—the eSafety Commissioner defines it as 'the intentional online exposure of an individual's identity, private information or personal details without their consent'.[110]

129. Whilst the term is not mentioned in the Privacy Act Review Report, we acknowledge that the issue of doxxing has received significant media attention in 2024.[111] We also appreciate that, as identified by the eSafety Commissioner, doxxing can leave targets vulnerable to—and fearful of—public embarrassment, discrimination, stalking, identity theft, financial fraud, and damage to their personal and professional reputation.[112] We outlined these considerations in more detail in our April 2024 submission to the Department.[113]

130. We also acknowledge that there are instances in which doxxing behaviour is legitimate and should not be circumscribed. For example, doxxing can be part of public interest journalism where it involves the unveiling of private information that exposes contradictory, unethical, or illegal behaviour by public officials or business people.[114]

131. In respect of Schedule 3 to the Bill, we are concerned that there is potential for the proposed offences to be misused. We have received feedback that proposed offences are so broad that they may unintentionally criminalise many forms of conduct that they were not intended to cover, or that they may be used strategically to stifle legitimate public debate.

132. For instance, a person who writes or publishes an online article that is critical of a group (as per proposed section 474.17D of the Criminal Code), that includes the names of people who are members of that group, may be committing an offence under that section. By way of illustration, in April 2023, there was an ABC *Four Corners* report about Paralympic athletes who were deliberately overstating their disabilities.[115] The report included the names and images of certain athletes who were alleged to be engaging in this conduct. Under the Bill, that story may constitute a criminal offence (if the test is met that a reasonable person would regard the reporting as being menacing or harassing towards them). Additionally, we query whether the proposed offences would capture instances where an individual has posted allegations on their social media account that a person (or persons) sexually assaulted them.

133. The Bill also should provide further guidance on what constitutes 'menacing' or 'harassing' behaviour. As drafted, there is no clear definition of what behaviour constitutes 'harassing'—the term most likely applicable to doxxing.

134. Moreover, the concept of 'personal data' is defined very broadly in proposed subsections 474.14C(2) and 474.14D(2) to mean information about the individual or group members that allows them to be 'identified, contacted or located'. There also appears to be no clear differentiation between penalties for certain types of

---

[110] Ibid.
[111] See, e.g., Josh Taylor, *Publication of Jewish creatives WhatsApp group led to death threats, MP says*, The Guardian (Online, 9 February 2024); David Crowe, *'Doxxing' laws to be brought forward after Jewish WhatsApp leak*, The Sydney Morning Herald (Online, 12 February 2024); Lisa Visentin, *Doxxers on notice they will face jail time under new laws*, The Sydney Morning Herald (Online, 18 February 2024).
[112] Australian Government, eSafety Commissioner, *Doxing* (Web Page, March 2024).
[113] Law Council of Australia, *Doxxing and privacy reforms* (Submission to the Attorney-General's Department, 10 April 2024).
[114] eSafety Commissioner, *Doxing trends and challenges – position statement* (Position Statement, 23 January 2022) 2.
[115] Australian Broadcasting Corporation, *Four Corners: Broken rules and dreams at the Paralympics* (Video Report, 3 April 2023).

'personal data' being released. For instance, leaking sensitive information (e.g., private medical, legal, or financial records) may warrant a harsher punishment under the Bill, compared to publishing an individual's name and social media handle.

135. Certainty about these matters is crucial, particularly noting the significant penalties of six and seven years' imprisonment for the offences in proposed sections 474.14C and 474.14D, respectively.

136. Finally, further education is needed to inform the community about the harms associated with doxxing. Emphasis should be placed on the importance of limiting public disclosure of personal information online, not only the information of individuals but also the information of groups of individuals.

Recommendation 18

- **Schedule 3 to the Bill should be redrafted to address the concerns raised in this submission about:**
  - **the doxxing offences being drafted too broadly;**
  - **the need for guidance on what constitutes 'menacing' or 'harassing' behaviour; and**
  - **the lack of differentiation between penalties for the release of certain types of 'personal data'.**