THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:BMml041024

4 October 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: Nathan.MacDonald@lawcouncil.au

Dear Dr Popple,

Privacy and Other Legislation Amendment Bill 2024

Thank you for the opportunity to contribute to the Law Council's submission to the Senate Legal and Constitutional Affairs Legislation Committee's Inquiry into the Privacy and Other Legislation Amendment Bill 2024 (the Bill). The Law Society's Privacy and Data Law and Criminal Law Committees contributed to this submission.

General comments

Our submission is focused on how the proposed provisions in the Bill might practically operate, including potential unintended consequences. However, we note that this is a difficult task, without a clear understanding of the Government's legislative roadmap for further reforms arising from the Privacy Act Review Report.

Schedule 1—Privacy reforms

Children's Online Privacy Code (Part 4)

The Law Society supports the introduction of a Children's Online Privacy Code (COP Code). However, without further detail about the content, it is difficult to comment on whether it achieves the intended purpose.

Exclusion of health service providers

We query the rationale, under proposed section 26GC(5)(a), for a blanket exclusion for entities providing a health service, when the purpose of the COP Code is intended to clarify the principles-based requirements of the *Privacy Act 1988* (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.[1] In our view, the exclusion of entities providing a health service excludes many APP entities that should be covered by the COP Code. This exclusion is also much wider than

[1] See Proposal 16.5 in the *Privacy Act Review Report* 2022: https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au

T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

Law Council
OF AUSTRALIA
CONSTITUENT BODY

entities providing counselling services, as was agreed to in the Government Response to the Privacy Act Review (Government Response) in response to proposal 16.5.[2] The Explanatory Memorandum notes at paragraph 85 that there may be 'general health, fitness or wellbeing apps or services that may be covered by the COP Code', however it is likely that many such APP entities might try to establish that they are excluded for being 'entities … providing a health service' under proposed section 26GC(5)(a)(iii).

We also query the need for the blanket exclusion, noting that proposed subsections 26GC(5)(b) and (7) allow for the Office of the Australian Information Commissioner (OAIC) to specify within the COP Code itself which APP entities are and are not covered. The Explanatory Memorandum states at paragraph 88 that this may include the provider of a health service. The breadth of the exclusion, and the approach to health services under the COP Code should be further considered in our view.

Definition of 'child' – the need for consistency

The commentary in the Privacy Act Review Report (Review Report) states:[3]

> 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) (Online Safety Act), the UK Age Appropriate Design Code…

The commentary in the Government Response states:[4]

> Children are particularly vulnerable to online harms. Children increasingly rely on online platforms, social media, mobile applications and other internet connected devices in their everyday lives. While these services provide many benefits to children and young people, there is concern that children are increasingly being 'datafied', with thousands of data points being collected about them, including information about their activities, location, gender, interests, hobbies, moods, mental health and relationship status.

It is important to ensure consistency for individuals and businesses when introducing new definitions into the Act. Although the definition of 'child' is consistent with the *Online Safety Act 2021* (Cth), it is possible that defining a child as an individual who has not reached 18 years may lead to unintended consequences and inconsistencies with other health and privacy legislation, noting the generally accepted position in relation to a child's capacity to consent. This is summarised in the Government Response to proposal 16.2 of the Review Report:[5]

> …the Government agrees in-principle that the Privacy Act should codify the principle that valid consent must be given with capacity (proposal 16.2). It is crucial that there are exceptions for circumstances where a parent's or guardian's involvement in capacity decisions could be harmful to the child or otherwise contrary to their interests. The guidance provides sufficient flexibility by allowing entities to decide if an individual under the age of 18 has the 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.

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 being prepared by the eSafety Commissioner.

---

[2] Attorney-General's Department, *Government Response to the Privacy Act Review* (2023) 13.
[3] Attorney-General's Department, *Privacy Act Review Report* (2022) 147.
[4] *Government Response*, above 2, 13.
[5] Ibid.

Cross Border/Overseas data flows (Part 6)

In the Government Response, the Government agreed[6] with the proposals to consult on an additional requirement in subsection 5B(3) of the Act to demonstrate an 'Australian link' that is focused on personal information being connected with Australia,[7] and to introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).[8]

The Government Response also sets out the Government's agreement in principle that standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.[9]

In our view, the provisions of Part 6 of the Bill are welcome as they will clarify and simplify the cross-border requirements, and will assist APP entities to address the relevant requirements. We suggest consideration be given to making the required changes to APP 8.2(a) and the *Privacy Regulation 2013*, to expressly reference some of the mechanisms widely used by APP entities to address Article 46 of the European Union's *General Data Protection Regulation* (GDPR) and, in particular, safeguards, such as binding corporate rules and standard data protection clauses, adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).[10] Express references to such measures will help avoid 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 proposed regulations.

We also suggest that the Government should address the existing ambiguity in subsection 5B(3) of the Act. These issues were the subject of the Law Council's submission in November 2022, on the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022.*[11] The concerns expressed in that submission stand. In our view, the stated benefits of adding the clarifications under APP 8.2(a),[12] without addressing the current broad extraterritorial reach of the Act under APP 8.2(a), will create unintended consequence for the operation of APP 8.2(a). The existing overreach of subsection 5B(3) introduces unnecessary complexity and ambiguity 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.

Penalties (Part 8)

We are generally supportive of the variety of proposed enforcement tools. Our chief concern 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. Focusing on the civil penalty provision for which infringement notices can be applied under the proposed section 13K, we query whether principles-based obligations are sufficiently prescriptive to enable certainty in compliance.

We note that the challenge or mischief in this case is that many of the matters that would give rise to the contravention are expressed as matters of principle, and steps that require

---

[6] *Government Response*, above 2, 34.
[7] See Proposal 23.1 in the Review Report.
[8] See Proposal 23.2 in the Review Report.
[9] See Proposal 23.3 in the Review Report.
[10] *General Data Protection Regulation* (EU) 2016/679 Art 46(2).
[11] Law Council of Australia, submission to the Senate Legal and Constitutional Affairs Legislation Committee on the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth)*, 8 November 2022, 8-10.
[12] See Proposal 23.2 in the Review Report.

'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. Many of the key determinations of OAIC findings in respect of breaches of policy or notice provisions were the subject of considerable investigations looking at very different practices or contraventions. For example, in the Clearview Determination,[13] 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 APP 3.3, APP 3.4, APP 3.5, and APP 5. A similarly detailed review was required in the 7-Eleven Determination.[14] 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. In many other matters the determinations require an investigation into conceptually very different matters, such as the speed of data breach response, or more procedural matters, and whether the respondent took 'reasonable steps' to complete promptly or whether the statement provided to the Commissioner was provided 'as soon as practicable'.[15]

It may be informative to compare the proposed power for the OAIC to issue infringement notices with other regulators. ASIC is a regulator that issues infringement notices pursuant to section 12GX of the *Australian Securities and Investment Commission Act 2001 (ASIC Act)*. Notably, the provisions subject to an infringement notice listed under section 12GXA are more prescriptive than principles-based obligations, such as section 12CB of the *ASIC Act 2001*. Similarly, the nature of infringement notice provisions for which the Australian Competition and Consumer Commission (ACCC) may issue an infringement notice are likewise prescriptive in the enabling legislation, such as section 18 of the *Australian Consumer Law*.

ASIC's power to issue an infringement notice also 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:[16]

- 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
- 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.

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. 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.[17]

---

[13] Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr54 (14 October 2021): https://www.oaic.gov.au/__data/assets/pdf_file/0016/11284/Commissioner-initiated-investigation-into-Clearview-AI,-Inc.-Privacy-2021-AICmr-54-14-October-2021.pdf.

[14] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd(Privacy) [2021] AICmr 50 (29 September 2021): https://www.oaic.gov.au/__data/assets/pdf_file/0021/10686/Commissioner-initiated-investigation-into-Eleven-Stores-Pty-Ltd-Privacy.pdf.

[15] Pacific Lutheran College (Privacy) [2023] AICmr 98 (24 October 2023): https://classic.austlii.edu.au/au/cases/cth/AICmr/2023/98.html.

[16] ASIC, 'Infringement notices: Your rights', https://asic.gov.au/about-asic/asic-investigations-and-enforcement/infringement-notices/infringement-notices-your-rights/

[17] ACCC, Infringement notices: Guidelines on the use of infringement notices by the Australian Competition and Consumer Commission (2020), 3: https://www.accc.gov.au/system/files/Infringement%20notices%20-%20Guidelines%20on%20the%20use%20of%20infringement%20notices%20-%20July%202020.pdf

In light of the wider regulatory landscape, we suggest greater clarity is required as to what type of privacy contraventions lead to what degree of harm, if any, to the individual, and to what types of enforcement, which in turn will 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, such as the critical infrastructure sectors, or health or financial services firms, where data related contraventions may lead to multiple regulatory obligations and interventions.

We suggest further consideration be given to how effective infringement notices will be as an enforcement tool, in light of the principles-based obligations in the Act, which are notably less prescriptive than the requirements under the *ASIC Act 2001* or the *Australian Consumer Law*, for which infringement notices may be issued with more certainty in the event of contravention.

Automated decision-making (Part 15)

We appreciate that Part 15 is intended to bring about a level of transparency to automated decisions. However, we believe the provisions, as currently drafted, fail to provide certainty to the definition of a 'decision', and appear to impose a high and narrow bar with the requirement under proposed clause 1.7(a) of Schedule 1 for the computer program to 'make or do a thing that is *substantially and directly related to* making a decision'.

As a general observation, in our view the provisions seem to be drafted in contemplation of automated decision-making processes in the public sector context, and bear less relevance to automated decision-making in the private sector.

Meaning of 'automated decisions'

While in the case of a public sector entity this may be a single decision, as set out under legislation or regulation, 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 a number of decisions that follow a series of 'decision trees', some which might include the use of computer programs in deciding which branch of the decision tree is taken next. This may be a complex process and involve sensitive commercial-in-confidence information that is not appropriate for disclosure in a privacy policy.

It is difficult to know if the provision is intended to capture this, and, if it is, how a private sector entity would apply the test. We suggest the provision might achieve clearer implementation and a better outcome if its application is limited to public sector agencies.

If the decision could reasonably be expected to significantly affect the rights and interests of an individual (proposed clause 1.7(b) of Schedule 1), decisions in the areas of finance, insurance and health would likely all be captured. It is also relevant that one of the biggest users of computer programs in making decisions is consumer credit, which is regulated under Part IIIA of the Act and to which the Australian Privacy Principles do not apply.

While the provisions do not come into force for two years, unless there is significant guidance (as foreshadowed in the Government Response), it is likely that any organisation which regards itself as being captured by the requirement will provide generic disclosure, such as 'any information you provide in the application process may be used by a computer program to assist with processing your application', which simultaneously fulfils the obligation but provides no substantive information to meet the objective of provision of useful information to individuals.[18] Likewise, many industries use computer programs to filter groups in terms of

[18] See Proposal 19.3 in the Review Report.

products and pricing, which can have significant consequences for individuals, but we cannot envisage the requirement for disclosure in a privacy policy providing substantive benefit.

Further, there does not appear to be a provision that provides for a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. This is proposal 19.3 in the Review Report, which was agreed to by the Government.[19] Without this right, it is unclear to us how individuals might understand how automated decisions are made through disclosure in a privacy policy alone, which is likely to be a broad, generic statement.

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

Generally, to satisfy both 'substantially' and 'directly' is a high and narrow test. It is difficult to apply this test if the definition of a decision itself 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 can be difficult for entities to know what is required to be disclosed in a privacy policy under the proposed clause 1.7 of Schedule 1.

While the test is narrow, the meaning of 'decision' appears to be simultaneously made broader by proposed clause 1.9 of Schedule 1, which provides that making a decision includes refusing or failing to make a decision, and may affect the rights or interests of an individual, whether adversely or beneficially. It is unclear whether the definition of decision is intended to follow that of the GDPR, or that under Australian administrative law.

There are many ways in which personal information is used in automated processes. For example, there is the process of filtering or pre-screening information to achieve a more manageable set of information that a human can make a decision on. A person could argue that because they were 'screened out' before getting to the human decisionmaker, the computer program has done something that is substantially and directly related to the final decision, and that their rights were affected because their information never progressed to the human decisionmaker.

Without knowledge of what might proposed in a second tranche of reforms, it is difficult for us to comment on unintended consequences. We suggest the Government release a legislative roadmap, similar to the roadmap that issued for the *Security of Critical Infrastructure Act 2018*.

Schedule 2—Serious invasions of privacy

The proposed provisions in Schedule 2 to introduce a statutory tort for serious invasion of privacy are, in our view, broadly consistent with the Australian Law Reform Commission's 2014 Report, *Serious Invasions of Privacy in the Digital Era*, led by Professor Barbara McDonald (2014 Report).

The proposed clause 7(2) of Schedule 2 provides that the invasion of privacy is actionable without proof of damage. We note that Recommendation 8-2 of the 2014 Report recommended that 'The plaintiff should not be required to prove actual damage to have an action under the new tort'.[20] However, we suggest that not requiring proof of damage may become a point of litigation, especially considering examples in other jurisdictions. To avoid possible litigation in the future, we suggest that this statutory tort should be considered together with the direct cause of action and that clarity be provided on the relationship between the two.

[19] *Government Response*, above 2, 32.
[20] Australian Law Reform Commission, Summary Report: *Serious Invasions of Privacy in the Digital Era* (2014): https://www.alrc.gov.au/wp-content/uploads/2019/08/summary_report_whole_pdf_.pdf

We also suggest that consideration should be given to how the tort will operate with existing exceptions under the Act, such as the exceptions for employee records and small businesses.

Schedule 3—Doxxing offences

The Law Society agrees that conduct that falls squarely within the practice of doxxing should be proscribed. However, we note that such a proscription must be drafted with care. We are concerned that, as currently drafted, the proposed offences are so broad that they may unintentionally criminalise many forms of conduct which they were not intended to cover. For example, a person who writes or publishes an online article critical of a group, as per proposed section 474.17D, which includes the names of people who are members of that group, may be committing an offence under that section. By way of example, there was a *Four Corners* story about disabled athletes who were said to be exaggerating their disabilities in order to compete in the Paralympics. That story included the names and images of certain athletes who were said to be conducting themselves in this way. Under the proposed legislation, that story may constitute a criminal offence if the test that a reasonable person would regard the reporting as being menacing or harassing towards the individual is met. Similarly, we query whether the proposed sections would capture women who post on their social media accounts allegations that a particular man, or men, sexually assaulted them.

There is a divergence of views within our membership in respect of what the appropriate mental element should be. Some of our members consider mere recklessness enough, whereas others consider that the threshold ought to be higher, such as actual intent. We suggest that the inclusion of a 'reasonable excuse' defence would be an appropriate mechanism to ensure that the proposed provisions are appropriately circumscribed.

If you have any questions in relation to this submission, please contact Mimi Lee, Policy Lawyer, by phone (02) 9926 0174 or by email to mimi.lee@lawsociety.com.au.

Yours sincerely,

Brett McGrath
President