Law Council
OF AUSTRALIA

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Senate Legal and Constitutional Affairs Committee

8 November 2022

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.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, 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 90,000 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 2022 are:

- Mr Tass Liveris, President
- Mr Luke Murphy, President-elect
- Mr Greg McIntyre SC, Treasurer
- Ms Juliana Warner, Executive Member
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, 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.asn.au.

Acknowledgements

The Law Council is grateful for the contributions of the Law Institute of Victoria, the Law Society of New South Wales, the Law Society of South Australia, and the Queensland Law Society in the preparation of this submission, in addition to the contribution of its Business Law Section's Privacy Law Committee.

Executive Summary

1. The Law Council of Australia (**Law Council**) welcomes the opportunity to provide this submission to the Senate Legal and Constitutional Affairs Legislation Committee (**Committee**) on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth) (**Privacy Bill**).

2. The Law Council supports, in principle, many of the proposed amendments outlined in the Privacy Bill. The Law Council notes that, increasingly, individuals are required to provide personal and sensitive data in order to participate in Australia's digital economy and to access services. It also notes the importance of a privacy framework that primarily incentivises steps being taken to prevent data breaches, instead of reparations being made after a breach has occurred.

3. However, the Law Council is of the view that several measures in the Privacy Bill require additional justification, clarification, and refinement. Accordingly, the Law Council makes the following recommendations:

   - Paragraph 5B(3)(c) of the *Privacy Act 1988* (Cth) (**Privacy Act**) should be retained until judgment in the matter of *Facebook Inc v Australian Information Commissioner*[1] has been delivered and/or the review of the Privacy Act has been completed by the Attorney-General's Department.
   - Should paragraph 5B(3)(c) be removed, a balancing limitation should be added to confine the scope of the extraterritorial application of the Privacy Act, such as to 'personal information from a source in Australia'.
   - The amendments under the Privacy Bill should not apply to information obtained prior to their commencement unless further justification is provided.
   - Further justification should be provided for the significant proposed increases to penalties under the Privacy Act, noting that smaller entities, not just multinational corporations, may be subject to the regime.
   - Section 13G of the Privacy Act should be drafted with greater clarity about:
     - what may amount to a 'serious interference' in existing paragraph 13G(a);
     - the meaning of 'benefit' in proposed subsection 13G(3); and
     - the factors that a Court should take into account in assessing what penalty to levy.
   - Existing paragraph 13G(b) of the Privacy Act should be removed, or, at a minimum, the reference to a 'repeated' act or practice should be deleted.
   - The Office of the Australian Information Commissioner (**OAIC**) should be sufficiently resourced to perform and implement the proposed enforcement powers under the amended Privacy Act.
   - Proposed subsection 66(1AA) of the Privacy Act should carry a civil penalty, rather than a criminal penalty. If the criminal penalty is to be retained, consideration should be given to increasing the threshold of 'two or more contraventions'.

[1] [2022] HCATrans 157.

- New subsection 26WU(4) of the Privacy Act should be amended to require that the manner and timeframe specified by the Australian Information Commissioner (**Commissioner**) be reasonable or practicable in the circumstances.
- Subsection 33A(3) of the *Australian Information Commissioner Act 2010* (Cth) (**AIC Act**) should be amended so that the Commissioner must be satisfied on reasonable grounds that the receiving body has secure arrangements in place for protecting the information or documents.
- An additional threshold should be inserted into proposed subsection 33A(3) of the AIC Act about factors the Commissioner should consider before disclosing information, such as necessity, proportionality and relevance.
- Proposed section 33B of the AIC Act should include further limitations on the Commissioner's power to disclose information if satisfied it is in the public interest to do so, for example, including a presumption against disclosure where an investigation is not complete.

4. Finally, the Law Council notes the importance of consistency and compatibility between Australia's existing privacy legislation and anticipated reforms. It continues to welcome and engage with the holistic review of the Privacy Act, which is being concurrently conducted by the Attorney-General's Department. The Law Council considers that it will be important to maintain the momentum of this review to avoid uncertainty and unintended consequences created by the fragmented approach to reform, to which the Privacy Bill is contributing.

Introduction

5. The Law Council acknowledges that the Privacy Bill represents an initial step towards responding to increasing concerns regarding privacy, security, and data protection. These are matters that are naturally at the forefront of minds in the wake of recent cyber incidents involving theft of personal data, and it is understandable that there is a desire to respond in a timely manner. The Law Council also acknowledges that services and organisations that deal with sensitive and/or personal data should be transparent and accountable in order to promote confidence that this data is stored securely and used appropriately.

6. The Privacy Bill was referred to the Committee for inquiry on 28 October 2022. The Committee is due to report on or before 22 November 2022, and submissions were due on 7 November 2022. There have been only six business days for submissions to be prepared.

7. The proposed reforms outlined in the Privacy Bill address public concerns about the actions and obligations that have been subject to recent data breaches in Australia, to the detriment of many affected individuals. The Law Council recognises the need to make changes to the privacy regime as a matter of priority.

8. However, as a membership-based organisation, the Law Council has an obligation to consult with its Constituent Bodies, Sections, and expert committees on matters of policy. The limited consultation period has heavily constrained the Law Council's ability to engage at a detailed level with the legislative and explanatory materials. The Law Council's views on the contents of the reforms should therefore be considered preliminary. This is most unfortunate, given the significant proposals contained within the Privacy Bill. In the Law Council's view, 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.

9. The Privacy Act has now been in operation for over 30 years and the *Privacy Amendment (Private Sector) Act 2000* (Cth) was introduced some 20 years ago, extending privacy obligations to the private sector to provide a minimum set of privacy protections for individuals. More recently, in 2014 the changes from 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 Australian Privacy Principles. There have since been significant changes to the landscape in which these pieces of legislation operate. Critically, the current framework is contingent on individuals providing consent to their information being shared or stored. However, the Law Council is concerned that people generally do not understand how their data will be used or protected.

10. The Law Council has welcomed—and continues to engage with—the concurrent review of the Privacy Act, which is being undertaken the Attorney-General's Department,[2] and notes the importance of consistency and compatibility between Australia's existing privacy legislation and anticipated reforms. The Privacy Act, as updated, will need to cater to a broad range of data protection issues, ranging from topical, sizable incidents, currently the subject of multiple regulatory interventions, to the mostly silent and unnoticed day-to-day management of the personal information of millions of individuals undertaking routine transactions involving data in all sectors

[2] Attorney-General's Department, Review of the Privacy Act 1988 (Web Page, January 2022) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

of the economy. To this end, the Law Council is concerned that the introduction of the Privacy Bill, independently of the Privacy Act review, may unnecessarily increase the regulatory burden on affected entities, as well as complicate the ongoing review of the substantive provisions of the Privacy Act.

11. Accordingly, the Law Council supports expediting the Privacy Act review and welcomes the Attorney-General's recent remarks that the Privacy Act review 'will be finished by the end of this year'.[3] In this respect, the Law Council also calls for a roadmap for the harmonisation of Australia's privacy and data laws as part of this review process, to ensure the development of a national privacy framework which is consistent, clear, and accessible.

12. Finally, the Law Council notes that, while the public focus of a data breach may be targeted towards an organisation, the impact and consequences are most acutely felt by the people whose data has been accessed, shared and compromised. The Law Council calls for an increased focus on options for improving remediation for affected persons, to ensure the framework supports victims of privacy breaches, and would be pleased to contribute to any consultations in relation to these matters. This is canvassed in the current review.

Substantive issues

Extraterritoriality

13. The Explanatory Memorandum provides that the Privacy Bill is intended to amend:

> *… the extraterritorial jurisdiction of the Privacy Act to ensure foreign organisations that carry on a business in Australia must meet the obligations under the Act, even if they do not collect or hold Australians' information directly from a source in Australia*.[4]

Item 10 of Schedule 1 to the Privacy Bill would give rise to this change by repealing existing paragraph 5B(3)(c).

14. The Law Council understands that the intended effect of this change is to ensure that businesses that operate in Australia are still captured by the Privacy Act, without the need to demonstrate that they collect personal information 'in Australia' per se. It notes the below extract from the Explanatory Memorandum:

> *Currently, foreign organisations must meet obligations under the Privacy Act if the entity has an Australian link. A foreign organisation will have an Australian link if the organisation or operator carries on business in Australia and collects or holds information from a source inside Australia. However, when a breach of the Privacy Act occurs, it may be difficult to establish that these foreign organisations collect or hold personal information from a source in Australia*.[5]

However, there is no balancing reform that would limit the effect of the Privacy Act to information that has *some connection* with Australia.

---

[3] The Hon Mark Dreyfus KC MP, 'National Press Club Q&A' (Speech, 12 October 2022) <https://www.markdreyfus.com/media/transcripts/national-press-club-q-a-12-october-2022-mark-dreyfus-kc-mp/>.
[4] Explanatory Memorandum, Privacy Bill 2.
[5] Ibid 12-13.

15. The Law Council is of the view that removing paragraph 5B(3)(c), without replacing it with any other provision, may have broader implications and consequences than is intended. Repealing this paragraph would likely not limit the extraterritorial application to personal information 'from a source in Australia'[6] as envisaged in the Explanatory Memorandum. Rather, this repeal could have the unintended effect of being applicable to all foreign organisations operating in Australia for all their privacy practices, including those that affect citizens of other nations who do not have any link to Australia, because the amendment would mean that the threshold to satisfy the 'Australian link' is that the foreign operation carries on business in Australia.

16. The Law Council submits that, should the Privacy Bill pass as drafted, a foreign organisation that carries on any business in Australia (such as a bank in the United Kingdom that has a branch in Australia) may be subject to all requirements of the Privacy Act, both in relation to Australian-sourced data that is collected in the United Kingdom, but also in relation to their activities in the United Kingdom affecting their customers there. Further, it is not only the Australian Privacy Principles that would be expressed to apply to such entity—the credit information provisions in Part IIIA of the Privacy Act likewise would expressly apply to those activities, which have no connection with Australia.

17. The Law Council notes that, under section 13D of the Privacy Act, acts or practices specifically required by a law of a foreign country will not be an interference with privacy when engaged in outside Australia and an external Territory. However, just as in Australia, there are many lawful and socially useful activities that are not compelled by law which could be captured under this section.

18. The Law Council considers that it will be important to understand the scope and impact of the proposed changes and consider the potential for conflicts of laws and unintended legal consequences for sectors that are already regulated, either under their applicable home data protection regimes or industry-specific regulations that authorise and regulate their sphere of operations in Australia. For example, in the banking sector, there are approximately 50 foreign banks which have been approved by the Australian Prudential Regulation Authority (**APRA**) to have an Australian branch.[7]

19. Given the importance of considering extraterritoriality and the approach under the General Data Protection Regulation (**GDPR**) as part of broader reforms, the Law Council does not support the proposed changes as presented in the Privacy Bill in relation to these matters.

The General Data Protection Regulation of the European Union

20. At present, paragraph 5B(3)(c) is the sole effective jurisdictional limit on the operation of the Privacy Act. Critically, the effect of every substantive section of the Privacy Act has its jurisdictional issues balanced because of this paragraph.

21. Accordingly, if paragraph 5B(3)(c) is to be removed by to Item 10 of Schedule 1 to the Privacy Bill, the Law Council suggests that it is necessary to include some balancing limitation so that the relevant personal information must have some link with Australia for the Privacy Act obligations to attach.

---

[6] Ibid 13.

[7] As listed at Australian Prudential Regulation Authority ('APRA'), Register of authorised deposit-taking institutions (Web Page, 3 November 2022) <https://www.apra.gov.au/register-of-authorised-deposit-taking-institutions>.

22. The Law Council understands that this is the approach adopted by the GDPR of the European Union (**EU**). For example, Article 3 of the GDPR distinguishes between the processing of personal data by organisations 'established' in the EU (regardless of where the processing takes place) and the processing of personal data by organisations not established in the EU. Article 3(2) is reproduced below (emphasis added):

> *This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> *a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
>
> *b. the monitoring of their behaviour as far as their behaviour takes place within the Union.*[8]

23. That is, the GDPR is expressed to apply within and outside the EU, but only in relation to data as to persons in the EU, and only when certain activities are involved (i.e. offering goods and services to data subjects in the EU, or monitoring their behaviour).

24. In the Law Council's view, there is a clear opportunity for the Australian privacy regime to align with the approach in the GDPR: for example, by confining the scope of the extraterritorial jurisdiction of the Privacy Act to 'personal information from a source in Australia', importing the wording used in the Explanatory Memorandum.[9]

Impacts of subsection 5B(3) if amended

25. Assuming the Privacy Act is amended in the manner currently proposed, the Law Council cannot see any reason why a Court would interpret the Privacy Act as having some implicit limitation to apply to Australian-sourced data only. This is because, as the Explanatory Memorandum makes clear,[10] the Privacy Bill seeks to remove the existing jurisdictional limitation and not replace it.

26. Further, a literal interpretation of subsection 5B(3), if amended as proposed by the Privacy Bill, would seemingly empower the OAIC to enforce and regulate personal information completely unrelated to Australia, such as the personal information of citizens of other countries who do not have ties to Australia, or whose personal information is collected outside of Australia. It would not be an answer to this concern to speculate that the OAIC might selectively choose not to enforce the Privacy Act, once amended, in respect of information that has no connection with Australia.

27. The Law Council considers it to be highly likely that a foreign entity that has properly implemented its privacy obligations in its own jurisdiction, and is providing satisfactory protection for its customers, might nevertheless be failing to comply with some element of the Australian Privacy Principles or Part IIIA of the Privacy Act and,

---

[8] European Union, General Data Protection Regulation (GDPR) 2022, <https://gdpr.eu/article-3-requirements-of-handling-personal-data-of-subjects-in-the-union/#:~:text=General%20Data%20Protection%20Regulation%20%28GDPR%29%20Art.%203%20GDPR,processing%20takes%20place%20in%20the%20Union%20or%20not> Art 3.

[9] Explanatory Memorandum, Privacy Bill 13.

[10] Ibid 12-13.

as a result, committing repeated 'interferences with privacy' that would expose it to the civil penalty provisions in section 13G of the Privacy Act.

28. The Law Council submits that expansions to the territorial scope of the Privacy Act are matters that go to its substantive content and detail, and must be considered as part of the current review of the Privacy Act. Further, although it is not a bar to enacting legislative change now, the Law Council notes that the effect of existing subsection 5(3) of the Privacy Act is a significant issue in a current appeal before the High Court of Australia in *Facebook Inc v Australian Information Commissioner* (***Facebook***).[11] The Law Council understands that written submissions will be lodged in that appeal in December 2022.[12]

29. Accordingly, if it is considered impracticable to expeditiously develop an appropriate jurisdictional limit to replace paragraph 5B(3)(c) during this inquiry, the Law Council submits that it may be more feasible to develop a suitable alternative limitation once the judgment in the *Facebook* matter has been delivered and/or the Privacy Act review has been finalised.

Recommendations

- **Paragraph 5B(3)(c) of the Privacy Act should be retained until a judgment in the *Facebook* matter has been delivered and/or the review of the Privacy Act has been completed by the Attorney-General's Department.**
- **Should paragraph 5B(3)(c) be removed, a balancing limitation should be added to confine the scope of the extraterritorial application of the Privacy Act, such as to 'personal information from a source in Australia'.**

Application of amendments

30. Item 45 of Schedule 1 to the Privacy Bill sets out the arrangements for the application of the amendments. The Law Council supports Item 45(3), which specifies that the increased penalties under section 13G of the Privacy Act do not apply in relation to an act done or practice engaged in before the commencement of this item.

31. However, the Law Council notes, with some concern, the retrospective nature of several of the Privacy Bill's provisions, including:

- the Commissioner's ability to disclose information or documents under proposed sections 33A and 33B that were obtained prior to the commencement of these amendments; and
- the Australian Communications and Media Authority's (**ACMA**'s) ability to disclose authorised information under subsection 59D(1) of the *Australian Communications and Media Authority Act 2005* (Cth) that was obtained prior to the commencement of these amendments.

32. While there may be practical considerations that necessitate the retrospective nature of these proposed provisions, the Law Council does not consider these considerations have been adequately explained or justified in the Explanatory

[11] [2022] HCATrans 157.
[12] High Court of Australia, Case S137/2022: *Facebook Inc v Australian Information Commissioner* (Web Page, 2022) <https://www.hcourt.gov.au/cases/case_s137-2022>.

Memorandum. Similarly, the Law Council does not consider the regulatory impacts of these retrospective provisions—which will inevitably affect existing matters and previous submissions made under mandatory reporting schemes—have been adequately disclosed.

33. Accordingly, the Law Council does not support the application of the amendments to information obtained prior to their commencement, in the absence of significant further detail regarding the regulatory impact of these provisions on existing privacy matters.

Recommendation

- **The amendments under the Privacy Bill should not apply to information obtained prior to their commencement unless further justification is provided.**

Guidance to inform legislative development

34. In its Discussion Paper as part of the Privacy Act review, the Attorney-General's Department proposed developing 'a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations'.[13]

35. Legal and business advisers need workable tools to navigate this increasingly complex field. As such, the Law Council supports the development of such resources which emphasise the importance of clarity and consistency in the creation of privacy legislation, including in relation to measures as contained in the Privacy Bill.

Penalties

36. The Law Council supports, in principle, increased penalties for non-compliance with obligations under the Privacy Act. It notes the importance of a privacy framework that primarily incentivises steps being taken to address potential privacy risks and prevent data breaches, instead of reparations being made after a breach has occurred. However, it is of the view that some refinements and further consideration is necessary before the penalties take effect, as outlined below.

Civil penalties under section 13G of the Privacy Act

Quantum

37. Item 14 of Schedule 1 to the Privacy Bill proposes to increase the existing maximum civil penalties under section 13G of the Privacy Act for serious or repeated interferences with privacy:

- for a person other than a body corporate, to $2.5 million; and
- for a body corporate, the maximum penalty will increase to an amount not exceeding the greater of:
  - $50 million;

[13] Attorney-General's Department, Privacy Act Review (Discussion Paper, October 2021) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf> 211.

- three times the value of the benefit obtained; or
- if the court cannot determine the value of the benefit, 30 per cent of their adjusted turnover during the breach turnover period for the contravention.

38. Item 14 also provides that the 'breach turnover period' for a contravention means the longer of:

- the period of 12 months ending at the end of the month in which the contravention ceased, or proceedings in relation to the contravention were instituted (whichever is earlier); or
- the period starting at the beginning of the month in which the contravention occurred or began occurring and ending at the same time as the period determined in the above paragraph.

39. The Law Council notes that the current penalty under section 13G of the Privacy Act is 2,000 penalty units. On the current penalty rate value, this is $2.22 million for bodies corporate and $444,000 for other entities regulated by the Privacy Act.[14]

40. The Explanatory Memorandum to the Privacy Bill provides:

> *These penalties fall short of community expectations, particularly if it is large multinational organisations being penalised, and given the potential financial and emotional harm of serious or repeated breaches.*[15]

41. The Law Council is of the view that an increase in penalties will assist in ensuring that appropriate attention is given to best practice corporate compliance in the privacy area, and notes that the relatively low penalties for privacy breaches at present do not always compel businesses to prioritise security of data. For example, at an international level, ensuring that non-compliance is no longer a cost-effective option has played a significant role in encouraging best practice in the European Union and the United Kingdom under the GDPR. By increasing the cost of non-compliance, the Law Council considers this could promote alignment with both community and regulatory expectations in favour of greater ownership and accountability around privacy and data protection.

42. However, the Law Council is concerned by the extent of the penalty increases proposed, and suggests some refinements to ensure that there is sufficient certainty for entities that are subject to the Privacy Act and that will therefore be subject to these significant penalties, should the Privacy Bill be passed. While the Law Council acknowledges the importance of privacy, security, and data protection—as highlighted by the recent cyberattacks on Optus and Medibank, among others—the proposed increase appears excessive. This is particularly because the regulated community will include smaller organisations (that are not otherwise within the scope of the small business exemption;[16] that are prescribed through the *Privacy Regulation 2013* (Cth);[17] or that have opted-in to the Privacy Act).[18] At this point, the

[14] Explanatory Memorandum, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth) ('Privacy Bill') 6.
[15] Ibid 6.
[16] *Privacy Act 1988* (Cth) ('Privacy Act') ss 6D, 6E.
[17] *Privacy Regulation 2013* (Cth) s 7.
[18] *Privacy Act 1988* (Cth) ('Privacy Act') s 6EA; the Office of the Australian Information Commissioner ('OAIC') maintains a register of small business operators that have opted-in to the Privacy Act. As at 7 November

Law Council does not agree with the statement in the Explanatory Memorandum that:

> *… the level of civil penalties which apply under section 13G are a fair and proportionate response to the behaviours the penalties are intended to deter and penalise*.[19]

43. The Law Council submits that the proposed increases to the penalty regime under the Privacy Act have not been adequately justified in the Privacy Bill's Explanatory Memorandum, and queries in what circumstances the maximum penalty will be applied.

Alignment with other regimes

44. The Law Council acknowledges the recommendations of the Australian Competition and Consumer Commission (**ACCC**) in its 2019 *Digital Platforms Inquiry Final Report* that the maximum penalties in the Privacy Act be increased to mirror penalties of the Australian Consumer Law (**Consumer Law**).[20] The Law Council has agreed, in the course of several subsequent consultations, that such alignment could serve to elevate the status of privacy law, and act as a significant deterrent against severe and/or repeated offences against the Privacy Act.[21]

45. However, the Law Council notes that, at the time of the ACCC's recommendation, the maximum financial penalties available under section 151 of the Consumer Law had been increased under the *Treasury Laws Amendment (2018 Measures No. 3) Act 2018* (Cth) to be:

- for a person other than a body corporate, a fine of not more than $500,000;[22] and
- for a body corporate, a fine of not more than the greater of the following:
  - $10 million;[23]
  - three times the value of the benefit obtained;[24] or
  - if the court cannot determine the value of the benefit, 10 per cent of their annual turnover during the 12-month period ending at the end of the month in which the body corporate committed, or began committing, the offence.[25]

2022, the register contained the names of 697 businesses. See OAIC, Privacy opt-in register (Web Page, September 2021 <https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register?result_11193_result_page=1>.

[19] Explanatory Memorandum, Privacy Bill 6.

[20] ACCC, Digital Platforms Inquiry (Final Report, June 2019) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report> 35 [Recommendation 16(f)].

[21] See Law Council of Australia, Privacy Act Review: Discussion Paper (Submission to the Attorney-General's Department, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 19; Law Council of Australia, Review of the Privacy Act 1988 (Cth) – Issues Paper (Submission to the Attorney-General's Department, 17 December 2020) <https://www.lawcouncil.asn.au/publicassets/762d595e-dd59-eb11-9438-005056be13b5/3942%20-%20Review%20of%20the%20Privacy%20Act%20%20Issues%20Paper.pdf> 23; Law Council of Australia, Digital Platforms Inquiry – Preliminary Report (Submission to the ACCC, 15 February 2019) 10.

[22] *Competition and Consumer Act 2010* (Cth) sch 2 ('Australian Consumer Law') s 151(6).

[23] Ibid para 151(5)(a).

[24] Ibid para 151(5)(b).

[25] Ibid para 151(5)(c)

46. The exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (**Online Privacy Bill**), released by the Attorney-General's Department in October 2021, sought to replicate these existing penalties in section 13G of the Privacy Act, with the ACCC's recommendation in its 2019 report used as the primary justification for this proposed alignment.[26]

47. The Privacy Bill's Explanatory Memorandum similarly points to the ACCC's recommendation as justification for increasing the penalties in section 13G of the Privacy Bill:

> *These changes are consistent with the proposed maximum penalties under the Australian Consumer Law (ACL) in the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022. The Australian Competition and Consumer Commission's Digital Platforms Inquiry July 2019 report recommended that the maximum penalties of the Privacy Act should be increased to mirror the penalties for breaches of the ACL as the lack of effective deterrence has enabled problematic data practices.*[27]

48. However, unlike in the exposure draft of the Online Privacy Bill, the penalties under the Consumer Law that the Privacy Bill seeks to 'mirror' are new and untested—they have been subject to limited consultation, and their practical ramifications are currently unknown.

49. As the Explanatory Memorandum says, the penalties under the Consumer Law, upon which the Privacy Bill relies, are provided in the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022 (**Competition Bill**). An exposure draft of the Competition Bill was subject to a short consultation period in August 2022, in which 18 submissions were received.[28] The Competition Bill was introduced in the House of Representatives on 28 September 2022 and passed both Houses on 27 October 2022.

50. As part of this consultation process, it is relevant to note that the Law Council's Business Law Section submitted that the proposed increases to maximum penalties to the Consumer Law under Part 4 of the Competition Bill were not necessary or warranted, and may have disproportionate effects and other unintended consequences.[29] Concerns raised by the Business Law Section in its submission included that:

- the current pecuniary penalty regime adequately serves to deter corporations and individuals from contravening the *Competition and Consumer Act 2010* (Cth) (**Competition Act**), including the provisions of the Consumer Law;[30]
- the Competition Bill does not bring Australia into line with other international jurisdictions, despite this being its stated intention;[31]

---

[26] Attorney-General's Department, Online Privacy Bill Exposure Draft (Web Page, 2021) <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>.
[27] Explanatory Memorandum, Privacy Bill 6.
[28] Treasury, Treasury Laws Amendment (Competition and Consumer Reforms No. 1) Bill 2022: More competition, better prices (Web Page, September 2022) <https://treasury.gov.au/consultation/c2022-308266>.
[29] Law Council of Australia (Business Law Section), Treasury Laws Amendment (Competition and Consumer Reforms No. 1) Bill 2022 (Submission to the Treasury 26 August 2022) <https://www.lawcouncil.asn.au/resources/submissions/treasury-laws-amendment-competition-and-consumer-reforms-no-1-bill-2022> 1.
[30] Ibid 3.
[31] Ibid 9-10.

- the Explanatory Memorandum does not appear to provide a sufficient rationale for the proposed increase in the percentage of turnover from 10 per cent to 30 per cent or the 'breach turnover period' for which the percentage of turnover is to be applied;[32]
- Australia already has the highest consumer law penalty regime in the world,[33] and increased penalties are likely to have the harshest and most unintended consequences for smaller businesses;[34]
- significant penalties may suppress respondents' willingness to defend claims brought by the ACCC due to the risks of an aberrant finding under such a large penalty regime, and may result in more contested penalty hearings;[35]
- the proposed penalty increases would have the effect of imposing maximum penalties that are excessive in comparison to contravention of other serious corporate or white-collar civil and criminal offences, such as industrial manslaughter;[36]
- the proposed increase in penalties may have a chilling effect on business activity and investment in Australia, as businesses may not be prepared to consider innovative activities, which may be legal, or carry a very low risk of contravention, but which are nevertheless untested;[37]
- the costs of doing business may increase, as further compliance training and resources will need to be deployed to ensure sales and marketing teams, commercial teams, senior leadership teams and boards are educated about the increased penalties and risks to their business;[38] and
- an increase in the base penalty from $10 million to $50 million is likely to significantly and disproportionately adversely impact small businesses against which the ACCC commences legal proceedings.[39]

51. While the above arguments did not deter the passage of the changes to the Competition Act, the Law Council's concerns with the new Consumer Law penalty regime persist. Consequently, the Law Council is further troubled by the extent to which the Explanatory Memorandum to the Privacy Bill relies on the new penalty regime under the Consumer Law as the primary justification for the proposed changes to section 13G of the Privacy Act.

52. The Law Council emphasises that violations in relation to consumer protection and privacy both warrant high penalties. However, it considers that alignment with the penalty regime under the Consumer Law should not, of itself, justify the significant proposed changes to penalties in the Privacy Act, especially when there is a lack of certainty about what the 'benefit' in proposed section 13G is, and what conduct constitutes a 'serious' or 'repeated' interference with privacy, as outlined below.

---

[32] Ibid 9.
[33] Rod Sims, 'Continuing the ACL journey' (Ruby Hutchison Memorial Lecture, Online, 15 March 2022) <https://www.accc.gov.au/speech/continuing-the-acl-journey>.
[34] [34] Law Council of Australia, Treasury Laws Amendment (Competition and Consumer Reforms No. 1) Bill 2022 (Submission to the Treasury 26 August 2022) <https://www.lawcouncil.asn.au/publicassets/9218249f-d828-ed11-9460-005056be13b5/2022%2008%2026%20-%20S%20-%20Treasury%20Laws%20Amendment%20%20Competition%20and%20Consumer%20Reforms%20No%20%201%20%20Bill%202022.pdf> 10.
[35] Ibid.
[36] Ibid 11.
[37] Ibid 12.
[38] Ibid.
[39] Ibid.

Meaning of 'benefit'

53. As the Consumer Law and privacy regimes are distinct, the Law Council considers that questions relating to terminology and concepts will arise if sections from the Competition Act are merely replicated in the Privacy Bill without regard to the nuances of the privacy regime and the types of harms it seeks to address.

54. For instance, while a breach of the Consumer Law by a corporation may, evidently, produce a quantifiable, commercial benefit, the potential 'benefit' to a corporation resulting from serious or repeated data mismanagement is, in the Law Council's view, significantly less clear. As such, the Law Council questions the effectiveness of proposed paragraph 13G(3)(b) as a deterrent for corporations from engaging in problematic data practices.

55. In light of the above, the reference to 'benefit', as proposed to be inserted into section 13G of the Privacy Act, will likely need additional discussion and clarity, as it is currently unclear how one would determine the benefit obtained from a breach of the Privacy Act. The Law Council cautions that penalty and benefit calculations may, once formalised, be utilised as loss quantification frameworks in civil claims and class actions.

56. The Law Council accordingly suggests that consideration be given to reframing section 13G to reflect the harm caused by serious privacy infringements, rather than the value of the benefit obtained by the breaching entity.

'Serious' or 'repeated' conduct

57. If passed in its current form, the Privacy Bill will substantially increase the size of the penalties for entities subject to the Privacy Act, prior to any substantive reforms being made to its content, pending the results of its review. The Law Council is concerned that this fragmentation in the privacy reform process may expose entities to an increase in their respective compliance burden without a corresponding uplift in certainty of the standards that they are required to meet.

58. Section 13G of the Privacy Act deals with serious and repeated interferences with privacy. While an 'interference with privacy' is defined in section 13 of the Privacy Act, the terms of 'serious interference' and 'repeated interference' as used in section 13G are not defined, and unlike other sections of the Privacy Act, are not supported by a non-exhaustive list of factors that would give rise to such a contravention.[40]

59. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protections) Bill 2012 (Cth), which introduced the terms 'serious' and 'repeated' into section 13G of the Privacy Act, provided that 'the ordinary meaning of these words will apply'.[41] This means that matters to be considered under this section are addressed by regulatory guidance and applicable guides on regulatory enforcement. The OAIC has published guidance in this regard, providing factors and conduct which it would take into account when deciding to seek a civil penalty under section 13G of the Privacy Act.[42] In this regard, the Law Council suggests that, in addition to existing guidance,[43] it would be beneficial for the OAIC to publish

[40] See, for example section 26WG.
[41] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 226.
[42] OAIC, Chapter 6: Civil penalties – serious or repeated interference with privacy and other penalty provisions (Web Page, June 2020) <https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties>.
[43] Ibid.

practical examples or case studies which could shed light on the intended interpretation of these terms.

60. However, while such guidance material is helpful to providing a degree of clarity, these key threshold terms have not had the benefit of substantive interpretation through case law. Since the introduction of section 13G, there has only been one instance where it has been relied upon in civil penalty proceedings which commenced in 2020.[44] These are substantive legal questions that will be considered in more detail as part of the current review of the Privacy Act, however in the absence of such consideration, concerns remain with such a substantial increase to penalties in the event of a contravention.

61. In the Law Council's view, the penalties in the Privacy Act, if increased to mirror the increased penalties for breaches of the Consumer Law, should be drafted with greater clarity and include factors that should be taken into account in assessing what penalty to levy. This is particularly the case given that:

- use of data is usually systematised and automated (so that an inadvertently incorrect setting can lead to contravening conduct happening hundreds or thousands of times per day);
- interferences with privacy that are a result of proven shortcomings in standards of security or information handling practices may be the subject of other detailed obligations; and
- the regulated community may include small entities, such as individual medical practices, as well as multinational corporations.

62. Further, assuming the Privacy Bill passes in its current form and steps are taken to enforce the penalties as increased, the lack of clarity about the precise meaning of these types of interferences, and the current gaps in the notice and consent regime under the concurrent Privacy Act, will make enforcement difficult and potentially ineffective.

63. While the Law Council acknowledges that increased penalties will have a role in raising awareness and compliance with privacy and data obligations, it continues to support a holistic, consistent approach to privacy and data law reform. The Law Council considers that it will be important to maintain the momentum on the pending review of the content of the substantive provisions of the Privacy Act, to avoid uncertainty and unintended consequences created by the fragmented approach to reform.

64. As part of its engagement with the Online Privacy Bill,[45] the Law Council submitted that, at a minimum, careful consideration needs to be given to revising the requirements of section 13G of the Privacy Act by:

- adding a note to address what may amount to a 'serious interference' in existing paragraph 13G(a) and clarifying that the provision applies to the privacy of one or more individuals; and
- removing existing paragraph 13G(b), or as a minimum, deleting the reference to a 'repeated' act or practice. This would address the fact that strictly speaking, many contraventions of the Privacy Act are potentially repeated, in that the digital environment operates in real time and relies on systems and

[44] *Australian Information Commission v Facebook Inc* [2020] FCA 531.
[45] Law Council of Australia, Online Privacy Bill Exposure Draft (Submission to the Attorney-General's Department, 14 December 2021), <https://www.lawcouncil.asn.au/resources/submissions/online-privacy-bill-exposure-draft> 14-15.

processes that are, by their nature, repeatable (for example, providing inadequate notice to users of a platform in contravention of Australian Privacy Principle 5).[46]

The Law Council considers that these suggestions remain particularly relevant in respect of the Privacy Bill.

Recommendations

- **Further justification should be provided for the significant proposed increases to penalties under the Privacy Act, noting that smaller entities, not just multinational corporations, may be subject to the regime.**
- **Proposed section 13G of the Privacy Act should be drafted with greater clarity about:**
  - **what may amount to a 'serious interference' in existing paragraph 13G(a);**
  - **the meaning of 'benefit' in proposed subsection 13G(3); and**
  - **the factors that a Court should take into account in assessing what penalty to levy.**
- **Existing paragraph 13G(b) should be removed, or, at a minimum, the reference to a 'repeated' act or practice should be deleted.**

Application to entities that provide services to regulated agencies and organisations

65. The Law Council notes that the increased penalty regime will affect not only Privacy Act entities, but also entities that provide services to regulated agencies and organisations. The increased penalties, coupled with the provisions that seek to strengthen the Notifiable Data Breach (**NDB**) scheme in Part IIIC of the Privacy Act, will have a significant impact on affected entities in the conduct of their businesses and on their potential risk exposure in the event of a breach.

66. It is therefore critical that legislative reform with respect to privacy and cybersecurity is supported by appropriate regulator guidance and enforcement, to promote corporate compliance and to avoid compliance costs which may not necessarily enhance privacy risk management.

Resourcing of the Office of the Australian Information Commissioner

67. The Law Council also submits that, based upon previous regulator inaction in the privacy field, any such increase in penalties under the Privacy Act should be accompanied by a commensurate increase to the resources of the OAIC.

68. The OAIC must be sufficiently resourced to perform and implement the proposed enhanced enforcement powers, while also discharging its other key statutory functions and activities, including providing information to the public, organisations, and agencies about their rights and obligations under the Privacy Act.

69. In this regard, the Law Council welcomes the $17.0 million of new funding allocated over two years from 2022–23 to support the OAIC in undertaking its privacy and

[46] Privacy Act sch 1 ('Australian Privacy Principles') s 5.

regulatory functions, as announced in the 2022–23 Federal Budget in October. However, the Law Council notes with concern that, following this period, a steep decline is forecast in the total expenses incurred by the OAIC in relation to these functions—$30.4 million in 2022–23, $27.4 million in 2023–24, and $16.3 million in 2024–25.

Recommendation

- **The OAIC should be sufficiently resourced to perform and implement the proposed enforcement powers under the Privacy Act.**

Criminal penalties under section 66 of the Privacy Act

Replacement of subsection 66(1)

70. At present, subsection 66(1) of the Privacy Act provides that a person shall not refuse or fail to give information; or to answer a question or produce a document or record, when so required under the Privacy Act. For an individual, the current penalty is imprisonment for 12 months or 20 penalty units (or both),[47] and for a body corporate, the current penalty is 100 penalty units.[48]

71. Item 38 of Schedule 1 to the Privacy Bill seeks to repeal existing subsection 66(1) and replace it with a 'basic contravention' carrying a civil penalty of 60 penalty units where a person is required to give information, answer a question or produce a document or record under the Privacy Act and refuses or fails to do so. The proposed penalty is 60 penalty units for a person, which the Law Council notes is 300 penalty units for a body corporate.[49]

72. The Explanatory Memorandum provides that:

> *The purpose of converting subsection 66(1) from a criminal offence to a civil penalty provision is to allow the Commissioner to issue a civil penalty or an infringement notice for minor instances of non-compliance without having to resort to the prosecution of a criminal offence. Infringement notices will provide the Commissioner with a timely, cost-efficient enforcement outcome in relation to minor contraventions of section 66.*[50]

73. The Law Council has previously expressed support for an infringement notice regime, similar to the scheme already available to the ACCC and ACMA. Accordingly, it supports the conversion of subsection 66(1) to a civil penalty provision which will provide an alternative to litigation of a civil matter and enable the Commissioner to resolve privacy complaints and investigations more efficiently.

New subsection 66(1AA)

74. Item 39 of Schedule 1 to the Privacy Bill inserts new subsection 66(1AA) in the Privacy Act which addresses 'multiple contraventions', which provides that a person will commit an offence if:

- the person is a corporation; and

[47] Privacy Act para 66(1)(a).
[48] Ibid para 66(1)(b).
[49] Applying the multiplier in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 82(5).
[50] Explanatory Memorandum, Privacy Bill 22.

- the person has engaged in conduct that constitutes a system of conduct or a pattern of behaviour; and
- the system of conduct or pattern of behaviour results in two or more contraventions of subsection 66(1) of the Privacy Act.

75. This new offence will carry a penalty of 300 penalty units, which matches the civil penalty units for a basic contravention under subsection 66(1) by a body corporate.

76. The Explanatory Memorandum provides that the purpose of this new subsection is:

> *…to enable the OAIC to refer matters to the Commonwealth Director of Public Prosecutions involving more serious, systemic conduct*.[51]

77. The Law Council queries whether it is necessary to criminalise the conduct of a corporation refusing or failing to answer a question or produce a document, especially if the breach occurs twice. While it acknowledges the argument in the Explanatory Memorandum that 'conduct regarded as criminal carries a greater stigma',[52] the Law Council considers that criminalisation in such circumstances seems severe. If this proposed subsection is to be retained, consideration should be given to increasing the contravention threshold above two breaches in order to more appropriately reflect 'serious, systemic conduct' which warrants the imposition of a criminal offence.

Recommendation

- **Proposed subsection 66(1AA) of the Privacy Act should carry a civil penalty, rather than a criminal penalty. If the criminal penalty is to be retained, consideration should be given to increasing the threshold of 'two or more contraventions'.**

Increased powers of regulators

78. The Law Council supports, in principle, the increased powers of regulators proposed in the Privacy Bill. However, it is of the view that some refinements are necessary, as outlined below.

Information gathering powers

79. Item 18 of Schedule 1 to the Privacy Bill seeks to add new section 26WU at the end of Part IIIC of the Privacy Act, which provides the Commissioner with information gathering powers in relation to actual or suspected eligible data breaches. The Explanatory Memorandum states:

> *This is necessary to ensure the Commissioner has comprehensive knowledge of the information compromised in an actual or suspected eligible data breach in order to assess the particular risk of harm to individuals. For example, additional information may assist the Commissioner in determining whether to issue a notification under section 26WR to direct an entity to notify the Commissioner and affected individuals about an eligible data breach*.[53]

[51] Ibid.
[52] Ibid.
[53] Ibid 15.

80. While the Law Council supports, in principle, enabling the Commissioner to conduct comprehensive and expeditious investigations relating to eligible data breaches, the broad powers proposed under section 26WU both to obtain and retain information, raise several practical and procedural issues.

81. Proposed subsection 26WU(4) outlines the procedural requirements for a written notice given by the Commissioner to provide information, produce a document or answer a question under subsection 26WU(3). While the Commissioner is required to state the manner and time in which information is to be provided, the Law Council suggests consideration be given to amending the subsection such that the manner and timeframe specified by the Commissioner must be reasonable or practicable in the circumstances.

82. In the Law Council's view, this qualification is necessary to counterbalance the significant powers granted to the Commissioner under proposed section 26WU, noting that under subsection 26WU(6), the sole mechanism available to entities to oppose the disclosure of information under section 26WU is to obtain a certificate from the Attorney-General under section 70 of the Privacy Act.

83. The Law Council also notes, in any event, that the increased enforcement powers proposed under section 26WU are contingent upon a significant increase in funding and resourcing for the OAIC in order to take practical effect.

Recommendation

- **New subsection 26WU(4) of the Privacy Act should be amended to require that the manner and timeframe specified by the Commissioner be reasonable or practicable in the circumstances.**

Information sharing powers

84. Item 20 of Schedule 1 to the Privacy Bill seeks to enhance the Commissioner's ability to share information by inserting the following sections at the end of Division 3 of Part IV of the AIC Act:

- section 33A—the Commissioner may share information with other authorities; and
- section 33B—Commissioner may disclose certain information if it is in the public interest.

Sharing information with authorities

85. The Privacy Bill inserts new section 33A into the AIC Act, which empowers the Commissioner to share information (including personal information) or documents with a 'receiving body' for the purpose of the Commissioner or the receiving body exercising powers or performing functions or duties. The following bodies will be covered under this proposed provision:

- an enforcement body;[54]

[54] An 'enforcement body' is defined in subsection 6(1) of the *Privacy Act 1988* (Cth) ('Privacy Act'), and includes, among other entities, the Australian Federal Police and state and territory police forces; state and territory crime and/or anti-corruption commissions; the Australian Crime Commission; the Office of the Director of Public Prosecutions and similar state and territory prosecutorial bodies; the Australian Securities and Investments Commission; and the Australian Prudential Regulation Authority,

- an alternative complaint body;[55]
- a State or Territory authority,[56] or an authority of the government of a foreign country, that has functions to protect the privacy of individuals (whether or not the authority has other functions).

86. The Explanatory Memorandum provides that the purpose of new section 33A is to:

> *… ensure the Commissioner is able to transfer a complaint to a receiving body, and also share information for the purposes of the Commissioner or the receiving body exercising their powers, or performing their functions and duties. This may occur when, for example, the Commissioner is holding information that relates to both an investigation under the Privacy Act, and under the receiving body's framework*.[57]

87. The Law Council notes this is a broad power and constitutes an authorisation by law for the Commissioner's use or disclosure of information for a secondary purpose for the purposes of Australian Privacy Principle 6.2(b).[58] Beyond the restriction that the information or documents must have been acquired by the Commissioner in the course of exercising powers, or performing functions or duties, under the Privacy Act, the only other condition imposed with respect to the Commissioner's decision to share this information, per proposed paragraph 33A(3)(b), is that:

> *…the Commissioner is satisfied on reasonable grounds that the receiving body has satisfactory arrangements in place for protecting the information or documents*.

88. While the Law Council recognises the need for the Commissioner to transfer a complaint where appropriate, it is concerned that these conditions impose an inappropriately low threshold for the sharing of information under new section 33A. Given the Commissioner's broad discretion under this section, the Law Council suggests consideration be given to amending subsection 33A(3), to the effect that the Commissioner must be satisfied on reasonable grounds that the receiving body has 'secure' arrangements in place for protecting the information or documents. Such as requirement would, in the Law Council's view, provide a more appropriate safeguard for the receipt and storage of sensitive privacy information.

89. Proposed subsection 33A(3) also does not require the Commissioner to consider factors such as necessity, proportionality and relevance with respect to the disclosure of information. The Law Council accordingly submits that an additional threshold be inserted in subsection 33A(3) with regards to factors the Commissioner should consider before disclosing information.

90. Notwithstanding the limitations set out in proposed subsections 33A(3)-(5), there is also, in the Law Council's view, a significant risk that the information sharing regime proposed under section 33A may act as a deterrent for entities that would otherwise

[55] An 'alternative complaint body' is defined in subsection 50(1) of the Privacy Act, and includes, among other entities, the Australian Human Rights Commissioner; the National Data Commissioner; the Ombudsman; the Australian Public Service Commissioner; the Inspector-General of Intelligence and Security; and a recognised external dispute resolution scheme.
[56] A 'State or Territory' authority is defined in subsection 6C(3) of the Privacy Act, and includes, among others, a State or Territory Minister; a Department of a State or Territory; a State or Territory court and tribunal; and a person holding or performing the duties of an appointment made (otherwise than under a law of a State or Territory) by a Governor of a State, the Australian Capital Territory Executive, the Administrator of the Northern Territory, or a State or Territory Minister.
[57] Explanatory Memorandum, Privacy Bill 16.
[58] Privacy Act sch 1 ('Australian Privacy Principles') s 6.

pursue early and voluntary engagement with the regulator. As noted in the OAIC's *Privacy Regulatory Action Policy*:

> *The OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches.*[59]

91. In 2020–21, voluntary notifications comprised approximately 15 per cent of the notifications received by OAIC under the NDB scheme.[60] The sharing of information by the Commissioner with other bodies, including 'enforcement bodies' under proposed paragraph 33A(2)(a), has the potential to undermine the voluntary aspects of OAIC's regulatory approach, which may be necessary to mitigate or resolve privacy issues at an early stage.

92. The risk of disincentivising voluntary reporting might be compounded by the indefinite, and potentially expansive list of bodies authorised to receive information under proposed subsection 33A(2) of the AIC Act. Alternative complaint bodies, for example, as defined by subsection 50(1) of the Privacy Act, include any external dispute resolution schemes which may recognised by the OAIC on an ongoing basis. The Law Council suggests consideration be given to amending this provision to provide an exhaustive list of relevant bodies authorised to receive information under the Privacy Act. Such provision could be modelled on section 155AAA of the Competition Act.

Recommendations

- **Subsection 33A(3) of the *Australian Information Commissioner Act 2010* (Cth) should be amended so that the Commissioner must be satisfied on reasonable grounds that the receiving body has secure arrangements in place for protecting the information or documents.**
- **An additional threshold should be inserted into proposed subsection 33A(3) about factors the Commissioner should consider before disclosing information, such as necessity, proportionality and relevance.**

Disclosure of information by the Commissioner

93. Item 20 of Schedule 1 to the Privacy Bill also inserts new subsection 33B(1) into the AIC Act, which provides that the Commissioner may disclose information acquired in the course of exercising powers or performing functions or duties under the AIC Act if the Commissioner is satisfied that it is in the public interest to do so.

94. According to the Explanatory Memorandum, the purpose of subsection 33B(1) is:

> *…to empower the Commissioner to disclose or publish information relating to privacy and personal information, for example information about an ongoing investigation on the OAIC's website. This will ensure Australians are informed about privacy issues and to reassure the community that the OAIC is discharging its duties.*[61]

[59] OAIC, Privacy regulatory action policy (Web Page, May 2018) <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy>.
[60] OAIC, Annual Report 2020-21 (Report, 21 October 2021) <https://www.oaic.gov.au/about-us/our-corporate-information/annual-reports/oaic-annual-reports/annual-report-2020-21>.
[61] Explanatory Memorandum, Privacy Bill 17.

95. New subsection 33B(2) provides that the Commissioner must have regard to the following factors in determining that a disclosure is in the public interest:

- the rights and interests of any complainant or respondent;
- whether the disclosure will, or is likely to, prejudice any investigation the Commissioner is undertaking;
- whether the disclosure will, or is likely to, disclose the personal information of any person;
- whether the disclosure will, or is likely to, disclose any confidential commercial information;
- whether the Commissioner reasonably believes that the disclosure would be likely to prejudice one or more enforcement related activities conducted by or on behalf of an enforcement body.

The Commissioner may also have regard to any other matter the Commissioner considers relevant.

96. The Law Council notes that similar to proposed section 33A, this power constitutes an authorisation by law for the Commissioner's use or disclosure of information for a secondary purpose for the purposes of Australian Privacy Principle 6.2(b).[62]

97. While the Law Council supports the mandatory considerations for the Commissioner when deciding whether a disclosure is in the public interest, it is of the view that this power is too broad and should be tightened, as it currently enables the OAIC to publicly disclose information acquired during an information, including before an investigation is complete. While there may be circumstances where disclosure of this nature is warranted, this should be the exception rather than the rule. Proposed section 33B should include further limitations on this power to ensure it is not exercised by the Commissioner as a matter of routine.

98. As currently drafted, the Law Council considers that the Commissioner's power in new section 33B of the AIC Act may discourage entities from disclosing to the OAIC, knowing this may make the investigation process more complex and difficult, and could result in details of the investigation being prematurely publicised.

Recommendation

- **Proposed section 33B of the AIC Act should include further limitations on the Commissioner's power to disclose information if satisfied it is in the public interest to do so, for example, including a presumption against disclosure where an investigation is not complete.**

New assessment powers under the Notifiable Data Breach scheme

99. Item 21 of Schedule 1 to the Privacy Bill seeks to insert a new paragraph into subsection 33C(1), which lists matters the Commissioner may conduct an assessment of. Proposed paragraph (ca) provides that the Commissioner may conduct an assessment of the ability of an entity subject to Part IIIC (notification of eligible data breaches) of the Privacy Act to comply with that Part, including the extent to which the entity has processes and procedures in place to:

[62] Privacy Act sch 1 ('Australian Privacy Principles') s 6.

- assess suspected eligible data breaches; and
- provide notice of eligible data breaches to the Commissioner and to individuals at risk from such breaches.

100. The Law Council understands that the Privacy Bill accordingly seems to empower the OAIC to conduct an assessment of an entity's compliance with the Privacy Act's NDB scheme to 'ensure entities are meeting the scheme's reporting and notification requirements'.[63]

101. The Law Council supports this measure. While Australia has seen a welcome increase in the notification of data breaches since the introduction of the NDB scheme,[64] its notification rate remains lower than many European nations who are subject to the notification under the GDPR.[65] The Law Council has previously received anecdotal reports that there is under-reporting of data breaches.

102. A such, there seems to be little doubt that the legislative self-assessment provisions in Part IIIC of the Privacy Act, as to what constitutes a data breach which 'would be likely to result in serious harm',[66] are failing in promoting appropriate public notification and transparency, as well as in encouraging the consequent corporate compliance efforts required to prevent data breaches in the first place.

103. In order to further strengthen the NDB scheme, the Law Council submits that the following matters require further consideration as part of the Privacy Act review:

- uncertainty regarding the threshold of the 'serious harm' test;[67]
- uncertainty as to the entities which have primary notification responsibilities under the scheme;[68] and
- the need for greater legislative guidance about how the scheme interacts with domestic and international laws, for example, where a data breach scenario impacts individuals across multiple State and Territory and/or international jurisdictions.[69]

104. The Law Council notes that in its Discussion Paper as part of the Privacy Act review, the Attorney-General's Department similarly outlined calls for 'additional OAIC guidance and education' and consideration of reform to improve the effectiveness of the NDB scheme.[70] These issues are particularly important in the context of the new compliance and infringement powers proposed under the Privacy Bill and highlight the need for legislative clarity to support entities and affected individuals.

---

[63] Explanatory Memorandum, Privacy Bill 5.
[64] OAIC, Notifiable Data Breaches Report: July-December 2021 (Web Page, 22 February 2022) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021>.
[65] DLA Piper, GDPR Data Breach Survey: January 2021 (Web Page, 19 January 2021) <https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/>.
[66] Privacy Act s 26WE(2).
[67] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission to the Attorney-General's Department, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 22.
[68] Law Council of Australia, Feedback on Notifiable Data Breaches Scheme Draft Resources (Letter to OAIC, 11 July 2017) < https://www.lawcouncil.asn.au/publicassets/622f88aa-5368-e711-93fb-005056be13b5/3310%20-%20Feedback%20on%20Notifiable%20Data%20Breaches%20Scheme%20Draft%20Resources.pdf>.
[69] Ibid.
[70] Attorney-General's Department, Privacy Act Review (Discussion Paper, October 2021) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf> 201.