Law Council
OF AUSTRALIA

Government response to the Privacy Act Review Report

Attorney-General's Department

13 April 2023

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 2023 are:

- Mr Luke Murphy, President
- Mr Greg McIntyre SC, President-elect
- Ms Juliana Warner, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Ms Tania Wolff, 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 thanks the following Constituent Bodies for their contributions in the preparation of this submission:

- Queensland Law Society
- The Law Institute of Victoria
- The Law Society of New South Wales
- The Law Society of South Australia
- The Victorian Bar

The Law Council is also grateful for the substantial contributions of the Business Law Section's Privacy Law and Media and Communications Committees.

Executive Summary

1. The Law Council of Australia welcomes the review of the *Privacy Act 1988* (Cth) (the **Act**) and thanks the Attorney-General's **Department** for the opportunity to provide comment that will inform the Government Response to the Privacy Act Review **Report**, released on 16 February 2023.

2. The Law Council is supportive, at least in principle, of many of the proposals in the Report. However, it calls for and recommends that additional details be provided to give the proposals more certainty. To that end, the Law Council would welcome an opportunity to review an exposure draft bill with a view to providing further comment on legal issues raised. Where the Law Council has not expressed a view, the matter remains an open issue subject to further consultation and review as appropriate.

3. The approach to reform, a summary of key positions, and the Law Council's methodology are set out below.

Approach to reform

4. The Law Council's approach has been driven by the following considerations that the Law Council continues to support:

    - a principles-based, technology-neutral and flexible approach to regulation of privacy and information related rights;
    - interoperability and harmonisation where possible, including harmonisation with State-based regimes and international norms and standards; and
    - certainty of legal requirements ensuring that standards set are clear and the scope and content of obligations imposed on Australian Privacy Principle (**APP**) entities can be complied with in practice.

5. The Law Council notes that the Act applies on an economy-wide basis. Many of the proposals, if enacted, will require fundamental technological changes by APP entities to support implementation and change management, as well as extensive communications with consumers impacted by the changes. Sufficient time will be critical for this to occur successfully.

Summary of key positions

6. The Law Council's key positions are:

    - Legislative reform to Australia's privacy framework must be supported by appropriate regulatory guidance. Establishing an independent and objective source of guidance on matters pertaining to the application of the Act and for promoting a common understanding of privacy and data laws should be considered.
    - Adequate resourcing of the Office of the Australian Information Commissioner (**OAIC**) will be critical, noting the proposed expanded nature of the regime and additional powers and responsibilities granted to the OAIC under the Act, and impacts on individuals and regulated APP entities. The effectiveness of this resourcing would be further enhanced if directed, in part, to supporting continuous improvement programs among businesses of all sizes and in all sectors. This would be in recognition of the compliance burden that a substantially uplifted privacy regime entails.

- The definition of ‘personal information’ is a fundamental issue and should be addressed as matter of priority.
- Australia’s privacy framework must strike the right balance between protecting the privacy rights of individuals and the avoidance of compliance costs. In this respect:
  - the proposed removal of the small business exemption would be a reasonable step towards promoting consistency and uniformity in the application of privacy legislation, on the condition that it will not impose an unjustified burden on small businesses and that potential implementation challenges are addressed; and
  - the proposed modification of the employee records exemption would be appropriate, given that there is no clear distinction between the privacy risks faced by an individual whether in the course of the employment relationship or in other aspects of their personal life, provided that the drafting adequately addresses legitimate uses of data in the administration of the employment relationship.
- The protection of the privacy of individuals must be carefully approached in light of the Constitution’s implied freedom of political communication and the importance of the media in an open and democratic society. While the Law Council does not have a settled view on the proposed journalism exemption, it remains supportive of steps to clarify and provide certainty to the balancing of all parties’ concerns.
- There is in-principle support for the introduction of the fair and reasonable test subject to clarification as to how the test will be applied in practice. Substantial additional detail and formal guidance will be required.
- Consideration should be given to tight regulation of the collection, protection and security of biometric information, including strict regulation around the use of this data by law enforcement agencies.
- Further information and consideration will be required regarding the proposed right to object to the collection, use or disclosure of personal information. Proposals concerning individual rights, such as erasure and de-indexing, will require further consideration, noting the complexity of the issues involved and the potential for unintended ramifications, particularly without minimum technology standards currently being required of technology developers who operate in Australia.
- The proposals in relation to automated decision making (**ADM**) in the privacy context are supported. However, further consideration should be given to these matters more broadly.
- Any new definitions of ‘direct marketing’, ‘targeting’ and ‘trading’ require careful drafting to avoid creating further uncertainty, and to ensure clarity of interaction between different obligations and laws.
- The extraterritorial scope of the Act should be amended to introduce an additional requirement to demonstrate an ‘Australian link’, which would effectively clarify that foreign organisations will only be regulated to the extent that their handling of personal information has a connection to Australia.

- Introducing separate 'mid-tier' and 'low-level' civil penalties would add a significant level of complexity to the enforcement regime for the Act. While a 'mid-tier' civil penalty provision is supported in cases that involve conduct falling short of the 'serious' standard under section 13G of the Act, the Law Council is not supportive of the introduction of an infringement notice regime for 'minor administrative breaches' as proposed.
- The Law Council's consultations indicate that there is general support for the proposed direct right of action and statutory tort for serious invasions of privacy, noting that views across the legal profession differ, and that there are concerns from some sectors as to its necessity and potential for unintended consequences.
- There is a need to review key aspects of the notifiable data breach (**NDB**) scheme including NDB notifications that involve multiple APP entities; the interaction of information submitted as part of NDBs with the definition of 'serious' as it relates to serious interference with privacy under Section 13G; and the impacts of notifications on impacted individuals, particularly in cases where the same incident could give rise to notifications by multiple APP entities. In addition, any legislative response under the Act must be consistent with the Government's 2023-2030 Australian Cyber Security Strategy,[1] once finalised, which the Law Council notes the Department of Home Affairs is currently consulting on.

Methodology and structure

7. This submission is in two parts. Part 1 sets out the Law Council's key comments and positions on the following proposals and the accompanying consultation questions:

    - **3:** Objects of the Act
    - **4:** Personal information, de-identification and sensitive information
    - **6:** Small business exemption
    - **7:** Employee records exemption
    - **8:** Journalism exemption
    - **12:** Fair and reasonable personal information handling
    - **13:** Additional protections
    - **18:** Individual rights
    - **19:** Automated decision making
    - **20:** Direct marketing, targeting and trading
    - **23:** Overseas data flows
    - **25:** Enforcement
    - **26:** A direct right of action
    - **27:** Statutory tort for serious invasions of privacy
    - **28:** Notifiable data breaches scheme

8. Part 2 sets out additional comments in table form, referencing the proposals sequentially. Part 2 provides further rationale and observations, as well as identifying contrasting views received by the Law Council in the course of preparing this submission.

[1] Department of Home Affairs, 2023-2030 Australian Cyber Security Strategy (Web Page, 2023) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>.

Introductory comments

9. The Law Council commends the Department on the comprehensive nature of the Report and in particular the detailed references to previous submissions and inputs.

10. Unfortunately, the current consultation timeframe has meant there has been limited opportunity for the Law Council—including its Constituent Bodies and Committees—to engage at a detailed level with the Report and the 116 proposals in the Report, in addition to the 31 survey questions published on the Department's Consultation Hub. Accordingly, the Law Council has regrettably had insufficient opportunity to consider each of the proposals and questions in detail. In future, on subject matter and legal reform that is substantive and wide-reaching, it would be of great assistance if more time could be provided to ensure consultations and subsequent submissions are as meaningful as possible.

11. The Law Council looks forward to reviewing the Government Response and engaging across Government and with the Department as these significant reforms progress, noting that continued broad consultation and transparency in relation to the progress of the reforms will be critical.

Australia's place in the global economy

12. Australia's regulatory approach to privacy and data law must be mindful of Australia's unique economic conditions and place in the global economy.

13. While the privacy and data law regimes adopted internationally, in jurisdictions such as the EU, United Kingdom (**UK**), and California may be instructive, the Act must, in the Law Council's view, account for Australia's specific economic requirements, and support technological growth and innovation to the greatest extent possible.

14. The Law Council also considers that the Act should be flexible enough to adapt to ongoing developments in international privacy and data law and ensure that Australia's regime remains in line with global standards.

Indigenous data sovereignty

15. The Law Society of New South Wales has noted that a priority reform identified in the National Agreement on Closing the Gap recognises the principle of Indigenous data sovereignty,[2] that is, the right of Aboriginal and Torres Strait Islander people to govern the collection, ownership and application of data as a cultural and economic asset.

[2] National Agreement on Closing the Gap (July 2020) <https://www.closingthegap.gov.au/sites/default/files/files/national-agreement-ctg.pdf> 13-15 (Priority Reform Four).

16. The Law Council acknowledges that it has been argued that:

> *Aboriginal and Torres Strait Islander peoples, families and communities, heavily overrepresented in social disadvantage–related data will also be overrepresented in the application of these new technologies, but in a data landscape, Indigenous peoples remain largely alienated from the use of data and its utilisation within the channels of policy power. Existing data infrastructure, and the emerging Open Data infrastructure, neither recognise Indigenous agency and worldviews nor consider Indigenous data needs.*[3]

17. The Closing the Gap priority reforms are a whole of government concern, and in the view of the Law Society of New South Wales, this requires proceeding with this reform in a way that is consistent with enlivening Indigenous data sovereignty principles. While the Law Council has not had an opportunity to consult with its Indigenous Legal Issues Committee on this matter in the time provided, it would be happy to do so.

Resourcing of the OAIC

18. The proposed reform and transition process will require time and resources to ensure that there is adequate opportunity for the preparation of detailed guidance, consultation on the various drafts, and socialisation with the community including, in some cases, other regulators or industry associations.

19. The ability to resource adequately the transition and the ongoing administration of the new regime will have a direct bearing on its efficacy. Adequate resourcing will be especially important, noting the proposed expanded nature of the regime and additional powers and responsibilities granted to the OAIC under the Act, and the impacts on individuals and regulated APP entities. Moreover, a review of the funding and enforcement models as noted in Proposal 25.7 will require a degree of independence and appropriate oversight.

Sources of guidance

20. In addition to corresponding resourcing, the Law Council is of the strong view that legislative reform to the privacy framework must be supported by appropriate regulatory guidance.

21. The OAIC must be resourced to support businesses in understanding their obligations and in complying with the Act. This should include resources to support entities coming under the expanded scope of the Act and guidance around the intended scope of 'trading in personal information'. The Report recognises that OAIC would need to be resourced to provide support to meet the needs and any challenges experienced by small businesses to adopt the privacy standards in the Act. This will be a significant undertaking and it is not yet clear what resources will be sufficient and/or of most assistance.

22. The private sector, including the legal profession, will play an important role in supporting businesses (particularly any small business clients) through any reforms. Consultation with such stakeholders early will therefore be essential.

[3] Maggie Walter et al., Indigenous Data Sovereignty in the Era of Big Data and Open Data, *Australian Journal of Social Issues* (June 2021) 143-56. Available at <https://doi.org/10.1002/ajs4.141>.

23. The Law Council further suggests that consideration be given to constituting a board or advisory panel, independent of (but not in place of) the OAIC, that would be responsible for providing independent and objective guidance on matters pertaining to the application of the Act and for promoting a common understanding of privacy and data laws. In the Law Council's view, such a body should be modelled on the European Data Protection Board and should have standing under the Act. Such a body could also be responsible for carrying out Privacy Impact Assessments (**PIAs**) on proposed legislation, both primary and subordinate.

24. Various aspects of the Report and the broader program of reform justify the constitution of an independent advisory board, noting in particular that:

- many of the proposals expressly refer to the need for further guidance;[4]
- the board could support the enhanced functions of the OAIC as a regulator with additional enforcement powers;
- it could potentially supplant the need to empower the Information Commissioner with the ability to develop an APP Code under Proposal 5.1, which various stakeholders noted may be somewhat controversial;[5]
- it could potentially assist in harmonising the various State, Territory and Commonwealth privacy and data law regimes;
- it is, in the Law Council's view, consistent with the revised objects of the Act proposed under Proposals 3.1 and 3.2;
- it could substantially improve certainty and consistency in the application of new and potentially far-reaching obligations under the Act, noting many proposals are expressed as principles requiring further guidance, such as the new requirements in relation to automated decision making[6] and the new obligations under the fair and reasonable test;[7] and
- the board could consider and develop industry-specific guidance, for example, specific to the media industry, which would assist to the extent that there are divergent views on the proposals in the Report.

Next steps

25. Following the publication of the Government Response to the Report, the Law Council recommends transparency to the greatest extent possible in relation to how the reforms will be progressed. In this respect, the proactive provision of clear details (i.e., which proposals will be addressed in each tranche of reform) will promote much-needed certainty for the multitude of sectors who expect to be impacted by these changes.

26. Further, given the high-level nature of the various proposals, it may be that there are further issues which are identified during the legislative process that the Law Council has not identified during this limited consultation process. The Law Council submits that the proposed reforms should be viewed within the context of the Australian privacy framework as a whole to ensure that policy objectives and community expectations are met by the law. Therefore, early and reasonable consultation with civil society, regulators and other interested parties and stakeholders on any exposure draft legislation will be critical.

[4] Attorney-General's Department, Privacy Act Review Report (2022), Proposals 4.1, 4.2, 10.2, 10.3, 11.2, 13.1, 13.3, 16.2, 17.1, 17.2, 19.2, 21.3, 21.5 and 24.
[5] Ibid 47-48 (Proposal 5.1).
[6] Ibid 188-193 (Proposal 19).
[7] Ibid 110-121 (Proposal 12).

Part 1: Feedback on key proposals and survey questions

Objects of the Act (3)

27. As a general principle, data protection regulation should enable a balance between the general public's interest in their personal information being retained appropriately along with its commercial interest in the data of businesses, subject to appropriate controls and restrictions. This approach will ensure that Australia is able to develop as a central hub for innovation and industry, as well as decrease regulatory barriers for small businesses.[8]

28. The Law Council has received competing views on amending the objects of the Act, as set out in Part 2. On balance, the Law Council supports Proposals 3.1 and 3.2 in principle, noting that Proposal 3.1 refers to personal information (a narrower, legally defined term), while Proposal 3.2 refers to privacy (a broad concept). Proposal 3.2 will therefore require additional clarity, given the structural consequences and noting the potential overlap with the proposed statutory tort for serious invasions of privacy,[9] and the functions of the courts in determining matters of public interest. Further, any explanatory materials accompanying subsequent bills should provide a rationale for the changes to the objects of the Act and the different outcome(s) the change is intended to bring about.

29. Acknowledging these differences in views, the Law Council recommends that consideration be given to retaining the current objects of the Act in section 2A, with the matters noted in Proposals 3.1 and 3.2 to be in addition to these objects, rather than replacing them. The Law Council especially notes that existing object 2A(b) addresses the important need to recognise that the protection of privacy of individuals is balanced with the interests of entities in carrying out their functions or activities.

30. The Law Council has previously suggested to the Department that the objects clause could also include:

    - an object of promoting fair and responsible handling by APP entities of personal information about individuals, through implementation of reliable and effective data governance, and appropriate monitoring, oversight and review processes and practices; and
    - an object of providing enforceable rights for individuals to seek redress for an interference with their privacy, in addition to any complaints process.[10]

31. Finally, the Business Law Section's Media and Communications Committee recommends consideration be given to the addition of a new object in section 2A to recognise that the protection of privacy of individuals is balanced with public interest in freedom of expression and the ability to impart and receive information freely in a democratic society, making clear the need for balance when considering such significant human rights. Similar provisions are in the EU General Data Protection Regulation (**GDPR**) and the *Data Protection Act 2018* (UK).

---

[8] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 6.
[9] Attorney-General's Department, Privacy Act Review Report (2022), 280-287 (Proposal 27.1).
[10] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 6-7.

Personal information, de-identification and sensitive information (4)

Amending the definition of 'personal information'

32. The question of certainty of the definition of 'personal information' is a fundamental issue in the reform process which, in the Law Council's view, should be addressed as a matter of priority. This definition is a cornerstone of Australia's privacy regime by defining what information is protected—and therefore what is regulated—under the Act and the regulatory framework administered by the OAIC.

33. The Law Council has previously welcomed the proposal that any new definition of 'personal information' should replace the word 'about' with 'relates to'.[11] It notes that Proposal 4.1 aligns with the Consumer Data Right and the GDPR, and its Constituent Bodies and Business Law Section's Privacy Law Committee have welcomed the inclusion of this proposal in the Report.

34. However, the Law Council is also aware of concerns, including from its Business Law Section's Media and Communications Committee, that this amendment will significantly expand the scope of the information falling within the definition of 'personal information'. This could result in:

- trivial or innocuous information being afforded the benefits of the protections in the Act, which could add to confusion and uncertainty;
- flow-on impacts in relation to individual rights, particularly the right of access and erasure; and
- requiring APP entities to be able to provide access to, or delete, specific technical information (i.e., telecommunications technical network information), which will be a large compliance burden for organisations with limited privacy benefits (noting this information is usually only held for limited periods) and will impact the ability of telecommunications providers to undertake network assurance and provide services to the benefit of all users.

Law Council view

35. The current law reform process provides an opportunity to address, as a matter of priority, ambiguities in the definition of 'personal information', and produce a clear definition that will deliver much-required certainty as to the scope and substance of the regime. Such certainty is critical to individuals who will have the benefit of protection under the Act and equally critical for APP entities that have responsibilities under the Act. Further, without a clear definition, many of the proposals in the Report will lack precise meaning in scope and application and may consequently fail to adequately address the risks that they seek to respond to.

36. On balance, the Law Council supports Proposal 4.1 in principle, and also notes that Proposal 4.2 will assist in providing certainty to APP entities by including in the Act a non-exhaustive list of information which may be personal information, in addition to more specific examples in the explanatory materials and OAIC guidance. As raised above, noting the materiality of the issues, an independent source of guidance should be considered.

[11] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 7.

37. Finally, a clear definition of what is personal information, and what obligations are attached when protecting it, will deliver better privacy outcomes, better legal outcomes and better regulatory outcomes without the need for any additional provisions, such as the proposals to regulate de-identified information. The Law Council submits that the approach to reform needs to be holistic.

38. To that end, the Law Council's earlier recommendation regarding an independent status of an opinion-giving body under the Act would assist with the delivery of certainty required of the definition. It would do so in a way that is transparent, does not jettison a principles-based approach and allows for interoperability and reference to international guidance or standards as appropriate.

De-identified information

39. Proposals 4.5 and 4.6 seek to regulate de-identified information and define it by a negative reference to 'personal information'. However, as the purpose of the Act is to regulate personal information as defined, it would be more appropriate to concentrate attention on the clarity of the definition of 'personal information', rather than traverse into areas of what is *not* personal information and is therefore outside the scope of the Act. Further, if the definition of 'personal information' is adequately addressed, as noted above, there would be no need to define 'de-identified information'.

40. The Law Council therefore does not support amending the definition of 'de-identified' per Proposal 4.5. While it may be appropriate to address process-related issues, the proposed attempt to regulate de-identified data and the de-identification process stems from a lack of clarity as to the current scope of 'personal information'.

41. The Law Council instead suggests that consideration be given to defining 'pseudonymisation' as per Article 4.5 of the GDPR:

> *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*.

42. Further, the Law Council does not support Proposal 4.6, which extends the protections of APP 11.1, APP 8 and the Report's targeting proposals, to de-identified information. In addition to terms within the proposal not being well understood (e.g., 'in such a way as to undermine the effectiveness of the de-identification'), it is of the view that this proposal will have multiple unintended adverse consequences, including:

- confusing the stakeholders who have long been trained to identify and protect personal information (as opposed to what is *not*);
- requiring a level of prescription that is at odds with the fact that the Act is based on compliance with principles, not prescription; and
- overlapping with other regimes that regulate information, such as the Australian Prudential Regulation Authority (**APRA**) CPS 234 and the operative definition in that standard: 'Information asset' is defined as 'information and information technology, including software, hardware and data (both soft and hard copy)' (emphasis added).[12]

[12] Australian Prudential Regulation Authority ('APRA'), Prudential Standard CPS 234: Information Security (July 2019), <https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf> Para 12(c).

Malicious re-identification of de-identified information

Should there be a criminal offence for re-identifying de-identified information? What exceptions should apply?

43. When de-identified information is maliciously re-identified, the risk to individuals and the community is significant. However, the Government ought to be cautious of criminalising behaviour without specific, targeted and extensive consultation on the potential impact and consequences of criminalisation.

44. The Law Council has received mixed views on this question which underscores the need for further discrete consultation. In the consultation time available, the Law Council has been unable to obtain the views of its National Criminal Law Committee. The Law Council therefore supports further consultation on the introduction of a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions, pursuant to Proposal 4.7. It welcomes the opportunity to participate in further consultations on this matter.

45. While reserving its position on whether there should be a criminal offence in such circumstances, the Law Council has made some preliminary comments on this matter in Part 2.

Geolocation tracking data

46. The Law Council supports, in principle, Proposal 4.10 which seeks to recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. It also supports, in principle, the proposed definition of 'geolocation tracking data'.

47. While the Law Council supports broadening the categories of data for which consent is required to be obtained, this proposal will require more clarity, as tracking is an ongoing activity (like surveillance) and geolocation data is a type of information. The question of geolocation is sensitive, in the same way as information relating to health or political opinion. This will go to the clarity as to what is 'personal information', as noted above.

Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?

48. While consideration should be given to expanding the requirement for consent to other metrics of personal information which are tracked over time (i.e., health data, heart rate and sleeping schedule information), the Law Council does not have a settled view on this question.

49. However, the Law Council has received broader feedback cautioning against introducing a framework which utilises consent as a key feature in authorising the handling of tracking data. Although consent is a necessary aspect of privacy regulation, an overreliance on consent is unduly burdensome on consumers, and may not result in improved privacy outcomes, given the complicated and technical nature of information handling practices. Furthermore, embedding standing consent language in most standard terms and conditions may make the requirement illusory in conferring protection.

50. The Law Council is wary of models that rely on consent as a key feature in authorising the handling of personal information under the Act, as too often, individuals are not adequately informed as to how their data will be used and any consent to such data use is therefore vitiated. It is therefore concerned that an increase in consent notifications may contribute to 'consent fatigue', whereby users become overwhelmed and cynical as a result of repeated consent notifications.

51. Accordingly, in addition to enhanced consent requirements, greater emphasis could be placed on organisational accountability in the collection and handling of sensitive information, including geolocation and other data. In this context, the Law Council notes that the proposed 'fair and reasonable' test may provide more robust consumer protections than a purely consent-based model.[13]

Small business exemption (6)

52. As technology has evolved, so has the way that businesses of all kinds store personal information. The effect has been that many larger small businesses now use much the same practices and technology to manage personal information as larger enterprises. This means that the risks surrounding the storage of employee records by larger small businesses have merged into the same risks that exist for storage of personal information collected for business reasons.[14]

53. However, stakeholders have noted that the same cannot be said for the majority of the smallest/micro businesses, who lack the technology infrastructure and business practices to effectively manage such personal data to the same degree as larger businesses, particularly in light of the role smaller businesses can play in the supply chains of larger businesses.[15] It is important that Australia's privacy framework strikes the right balance between protecting the privacy rights of individuals and the avoidance of compliance costs. Regulation should therefore be proportionate to the risk involved and capable of being effectively enforced.

54. The Law Council agrees that consideration of the removal of the small business exemption from the Act should be subject to the implementation of the measures in Proposal 6.1 to facilitate small business compliance, namely after:

- an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act;
- appropriate support is developed in consultation with small business;
- consultation with small business to determine the most appropriate way for small business to meet their obligations proportionate to the risk (for example, through a code); and
- small businesses are in a position to comply with these obligations.

[13] Attorney-General's Department, Privacy Act Review Report (2022), 110-116 (Proposal 12.1).
[14] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 9.
[15] Ibid.

55. Subject to the above considerations, and satisfaction that the removal of the exemption will not impose an unjustified burden on small businesses, the Law Council considers the removal to be a reasonable step towards promoting consistency and uniformity in the application of privacy legislation, in accordance with the long-standing views of the OAIC.[16]

56. The Law Council acknowledges that there is a risk that removing the small business exemption may have a chilling effect on innovation, particularly for start-ups and new businesses. Accordingly, consideration ought to be given to empowering the Information Commissioner to make limited exemptions or temporary relief from the Act, either for specific periods of time, or from particular requirements of the Act if, in practice, compliance with specific obligations proves unduly burdensome for certain classes of small business, provided there is a long-term commitment and compliance initiatives directed to all-business compliance.

If you are a small business operator, what support from government would be helpful for you to understand and comply with new privacy obligations?

57. The Law Council welcomes the approach set out in Proposal 6.1, which reflects the need for impact analysis, stakeholder consultation and comprehensive assistance being made to small businesses prior to removing the exemption. In the shorter term, the measures in Proposal 6.2 appear to be appropriate and are supported in principle, although they may be ultimately unnecessary if addressed through the processes in Proposal 6.1.

58. In considering the forms of government assistance that may be appropriate to assist with compliance, the Law Council supports the development of information and training resources tailored to the needs of various small businesses. It suggests that guidance models may be obtained from recent initiatives implemented by the UK Information Commissioner's Office[17] and New Zealand Office of the Privacy Commissioner.[18]

59. Consideration should be given to developing the following forms of government support:

- Template privacy policies, notices and consent forms (which can be modified based on different risk factors) to be made available at the time of registering an Australian Business Number (**ABN**) and/or business name.
- All existing ABN holders should also be notified of their new obligations under the Act and be provided with template documentation.
- A default or basic privacy policy could also be included in the legislation, (perhaps like replaceable rules) to help overcome the risk that compliance material not suited to this jurisdiction, or substandard material, will be used by businesses for cost reasons.
- Tailored advice and education provided by the OAIC (or the proposed independent advisory board referred to above under 'General comments').

[16] Australian Law Reform Commission ('ALRC'), For Your Information: Australian Privacy Law and Practice (Report 108, Volume 2, August 2008) <https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf> 1155 [33.41].
[17] Information Commissioner's Office, SME web hub – advice for all small organisations (Web Page, 2022) <https://ico.org.uk/for-organisations/sme-web-hub/>.
[18] Office of the Privacy Commissioner (NZ), Privacy Statement Generator (Web Page, 2013) <https://www.privacy.org.nz/tools/privacy-statement-generator/>.

- Free online training and information seminars with respect to privacy and data management, as well as cyber security training and assistance.
- A small business hotline and/or live chat service.

60. It has been suggested that the complexity of the existing scheme derives from the fact that the APPs were designed mostly for larger businesses. A concise, plain English document, code or charter for small business, instead of—or to supplement—the APPs may better support implementation.

Implementation considerations

61. The Law Council's Constituent Bodies have identified areas in which the Report has not fully contemplated the scope of potential issues and nuances in the implementation of Proposal 6.1.

62. For example, whilst the Report considers in detail the situation of a small business as a data processer, a further challenge for small business will be how to manage NDBs and related obligations as *controllers*, especially where the breach has occurred at the processor level.

63. It is rightly recognised in the Report that the use of third-party online platforms, in addition to 'software as a service', by small business has increased both the risk and consequences of data breaches. This software encourages (or even demands) the collection of large amounts of personal information from customers that in many cases is not strictly necessary. The Law Council notes that in practice, it is rarely feasible for small business to tailor these systems to capture less information, even if they wanted to do so. It also recognises that challenges may arise when using 'software as a service', in respect of who owns the stored data.

64. Under the proposed reforms, small business may therefore be left with a situation where software vendors will be permitted to pass much of the risk arising from overcollection of data (or a data breach) to its users, as those vendors will only be processors. The Law Council queries whether or not this achieves or promotes greater privacy protection.

Issues specific to the legal profession

65. An estimated 82 per cent of law practices in Australia were sole practitioners in 2020,[19] and an even greater number would be small businesses within the existing small business definition ($3 million turnover).

66. Therefore, apart from those who may already be covered by an exception to the current small business exemption (e.g., personal injuries law practices holding medical information), privacy compliance will be a significant issue and will add to overhead costs. This is likely to be reflected in access to justice issues including higher fees, particularly in regional, rural and remote areas.

[19] Urbis, 2020 National Profile of Solicitors (Report for the Law Society of New South Wales, July 2021) <https://www.lawsociety.com.au/sites/default/files/202107/2020%20National%20Profile%20of%20Solicitors%20-%20Final%20-%201%20July%202021.pdf> 3.

67. The Law Council recognises that some of the proposed reforms may be problematic for smaller firms to manage without appropriate exemptions. For example, to comply with the proposed right of erasure,[20] there will need to be processes in place to allow client files to be held without redaction. It may also be complex for these firms to establish whether personal information within a client file belongs to, or ought to be the responsibility of, the firm for the purposes of the Act.

68. The Law Council accordingly reiterates its suggestion that consideration ought to be given to empowering the Information Commissioner to make limited exemptions from the Act, if, in practice, compliance with specific obligations proves unduly burdensome for certain classes of small business.

Employee records exemption (7)

69. The Law Council has previously expressed the view that employers ought to be subject to the same privacy obligations as APP entities and should not benefit from the exemptions under the Act in relation to the storage of employee data.[21] Further, the existing employee records exemption is, of itself, not comprehensive and remains difficult to apply as a matter of practice.[22]

70. The Law Council notes that employee records frequently contain highly sensitive information, such as health data, criminal records and financial information, and there is no clear distinction between the privacy risks faced by an individual whose personal information is being handled by an employer, as opposed to any given business with which they have interacted.

71. The Law Council therefore supports Proposal 7.1—which seeks to modify the exception to enhance protection of private sector records—in principle, noting that, given its broad implications for employers, the timing and implementation of this change will need to be considered in detail.

How should employers provide enhanced transparency to employees about the purposes for which their personal and sensitive information is collected, used and disclosed?

72. The Law Council strongly supports enhanced transparency by employers in relation to the collection, use and disclosure of employees' data.

73. In considering how notice might adequately be given by employers in accordance with Proposal 7.1(a), the Law Council notes that some guidance may be gleaned from the *California Privacy Rights Act of 2020*, under which employers are required to provide a privacy notice to employees and job applicants before (or at the time) personal information is collected, specifying:

- the categories of sensitive personal information collected;
- whether that information will be sold or shared;
- the length of time the employer intends to retain each category of personal information; and

[20] Attorney-General's Department, Privacy Act Review Report (2022), 174-176 (Proposal 18.3).
[21] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 9-10.
[22] Ibid 10.

- the categories of all third parties that the employer discloses to or allows to collect the employee's personal information.

74. The Law Council holds concerns in relation to Proposal 7.1(d), which outlines the aim of notifying employees and the Information Commissioner of any data breach involving employees' personal information which is likely to result in serious harm. This aspect of the proposal:

    - creates too high a hurdle to be overcome in order to protect the right to privacy of employees, both in terms of the level of the harm and the probability of its occurrence, as breaches of privacy ought not require harm to be demonstrated in order for the right to be afforded protection; and
    - leaves it to the employer engaged in the breach to determine whether circumstances require them to report.

75. The Law Council notes that the Report raises the possibility of a 'tripartite process'[23] to develop privacy codes of practice for employee records. In the experience of members of its Business Law Section's Privacy Law Committee, the application of privacy laws to workplace issues suggests that the most complex and sensitive cases involve circumstances in which employees have made a workers' compensation claim and/or there is an internal grievance procedure. Both of these scenarios often involve the collection of sensitive information and disclosure to third parties such as independent investigators, claims assessors and health practitioners.[24]

76. The Law Council accordingly considers that the exceptions that apply to the collection, use and disclosure of information of this kind must be broad enough to apply to practices that are not uncommon in the workplace environment. This could be achieved by way of:

    - detailed consideration of the exceptions in the Act; or
    - a code of practice that varies those exceptions in a way that is appropriate for the processing of sensitive personal information in the workplace.

77. The Law Council also suggests that further consideration should be given to enhancing transparency in the use of workplace surveillance technology to collect personal and sensitive employee information. The rapid development in the sophistication and prevalence of workplace surveillance technology poses significant regulatory challenges.[25]

[23] Attorney-General's Department, Privacy Act Review Report (2022), 71 (Proposal 7.1).
[24] See, e.g., *'VI' and CSIRO (Privacy)* [2020] AICmr 44 (19 August 2020); *AF v Minister for Health; Minister for Health v AF* [2012] NSWADT 210 (16 October 2012); and *AF v Roads and Maritime Services (No 2)* [2012] NSWADT 210 (16 October 2012).
[25] See, e.g., Parliament of NSW, Final Report – Workplace surveillance and automation (Report No 2, November 2022) <https://www.parliament.nsw.gov.au/lcdocs/inquiries/2591/Report%20No.%202%20-%20Future%20of%20work%20and%20workers%20in%20New%20South%20Wales.pdf>.

If privacy protections for employees were introduced into workplace relations laws, what role should the privacy regulator have in relation to privacy complaints, enforcement of privacy obligations and development of privacy codes in the employment context?

78. The Law Council considers that the OAIC is the appropriate agency to oversee and administer the privacy rights of employees with respect to the records held by employers. This approach would promote the greatest level of consistency and uniformity in the application of privacy principles and regulations. This could be undertaken together with appropriate input from workplace relations and safety regulators.

79. However, if the OAIC were to absorb this additional role, the Law Council reiterates the need for corresponding resourcing so that it can sufficiently discharge its functions.

Journalism exemption (9)

80. The Law Council appreciates that the protection of the privacy of individuals must be balanced with the Constitution's implied freedom of political communication and the importance of a robust media and journalism sector in an open and democratic society. It remains supportive of steps to clarify and provide certainty to the balancing of the implied freedom of political communication, public interest journalism and legitimate expectations of privacy of individuals.[26]

81. While the Law Council has not had the opportunity to arrive at a settled view on these proposals on behalf of the Australian legal profession, it acknowledges that its Business Law Section's Media and Communications Committee does not support them. These concerns are articulated further in Part 2, arguing that the retention of the journalism exemption, unamended, is consistent with the implied freedom of political communication and provides a necessary pre-requisite for the provision of public interest journalism.

82. The Law Council notes that in 1992, the High Court of Australia established that there is a right to freedom of political communication implied in the Constitution,[27] although the 1997 High Court case of *Lange v Australian Broadcasting Corporation*[28]served to place some limitations upon how far this implied right extends. Accordingly, once a burden on political communication is identified, the relevant test is:

    - whether the law has a legitimate purpose consistent with the constitutional system of representative government; and
    - if so, whether the law is reasonably appropriate and adapted to the achievement of that purpose.

    The Law Council suggests that any new reforms in this area have careful regard to this test.

[26] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 10.
[27] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1; *Australian Capital Television v Commonwealth* (1992) 177 CLR 6.
[28] 189 CLR 520.

Fair and reasonable personal information handling (12)

83. Proposals 12.1 to 12.3 introduce a test of 'fair and reasonable' which will require APP entities to demonstrate that their collection, use and disclosure of personal information is 'fair and reasonable'.

84. The Law Council supports, in principle, a test that seeks to harmonise and create an overarching principle or standard. However, it has concerns as to how the proposed 'fair and reasonable' test is to be formulated and is to be applied in practice, if enacted without substantial additional detail and formal guidance. In this respect, its Business Law Section's Media and Communications Committee suggests consideration be given to including an additional 'lawfulness limb' to help anchor the concepts of 'fair and reasonable' and to ensure more effective compliance by businesses.

85. Notions of reasonableness can be applied to various data and information rights and lends itself to a balancing exercise, as noted above. However, the question of how it complements and operates *together* with fairness is far from clear. This lack of clarity, and the fact that the test, if implemented, will be a positive obligation on *all* APP entities in *all* cases of collection, use and disclosure of personal information, may lead to uncertainty and misunderstandings as to how well-established and understood uses of personal information are to be treated under the new test.

86. The Law Council notes that the test is objective, and the application of the test would be addressed as part of a PIA process. While the Law Council welcomes the expanded role of PIAs in Proposal 13, the lack of clarity as to scope of the obligation will not be remedied alone by a PIA.

87. The Law Council accordingly recommends that new guidance is prepared that addresses the concept of fairness and reasonableness as it operates in the context of information rights. Guidance should expressly address, among other matters, the need to ensure that the test does not inadvertently have a retrospective application on personal information already collected, used, and disclosed for a broad variety of known purposes.

88. As certainty is a prerequisite for a test of this kind to be effective, further consideration should be given to:

    - decoupling the test by, for instance, including a concept of fairness as one of several considerations of what would be a reasonable or an unreasonable collection, use, and disclosure of personal information (this could be included in the considerations currently listed in Proposal 12.2);
    - connecting the requirement for fairness and reasonableness to the objects of the Act as noted in Proposals 3.1 and 3.2;
    - referencing unfairness in the updated objects of the Act and supporting the concept with further guidance on how the concept of fairness or unfairness applies to privacy and information related rights;
    - articulating the consequences of not meeting the test (in whole or in part), for example, what will be the subject of a civil penalty sanction, other enforcement means or what will render a given consent or contract invalid;
    - including 'safe harbour' provisions which deem specified practices to be fair and reasonable in particular circumstances;
    - specifying what role or status, if any, some of the guidance and standards have; and

- clarifying what aspects of the test are to be regulated by which regime, for example, that matters of fairness or unfairness are to be assessed by reference to concepts and precedents developed under consumer protection laws.

89. The Law Council reiterates the need for a holistic approach and that guidance will be required to properly support a new obligation of fairness and reasonableness. In this respect, the Law Council emphasises the benefits of opinions and guidance issued under an independent, formal structure and framework under the Act.

Additional protections (13)

90. The Law Council supports Proposals 13.1 to 13.4 in principle and emphasises the importance of good guidance to assist APP entities with their obligations.

Privacy Impact Assessments

91. Proposal 13.1 recommends that APP entities undertake PIAs for activities with high privacy risks and to produce them to the OAIC upon request. However, what this proposal does not make clear is that the OAIC may request production of PIAs in the context of a data breach, whether that data breach was notifiable or not, having regard to section 26WU of the Act.

92. It is possible that an APP entity may be unwittingly exposing itself to an action by the OAIC based on the information contained, or not contained, in the PIA. In some instances, the PIA may have been drafted prior to the NDB scheme being introduced, or otherwise prior to an amendment that may follow from Proposal 13.1, without regard to the potential that the OAIC may require production of that PIA and the consequential action the OAIC may initiate against that APP entity.

93. Accordingly, the Law Council recommends that the production of any PIA to the OAIC should only extend to those PIAs undertaken subsequent to the implementation of Proposal 13.1, if implemented.

Biometric information

What additional requirements should apply to mitigate privacy risks relating to the development and use of facial recognition technology and other biometric information?

94. The Law Council recognises that the collection of biometric information, including facial recognition, without prior notice and without consent represents a serious risk to the right to privacy. Consideration should therefore be given to tight regulation of the collection and protection of this information, including strict regulation around the use of this data by law enforcement agencies.

95. The Law Council notes that unique risks may be involved where there are secondary uses of sensitive biometric data, collected with or without consent. For example, where biometric data has been input algorithmically into a secondary AI system, merely erasing an individual's data at the point of capture may be insufficient to remedy the relevant privacy risks.

96. In relation to additional requirements that should apply to mitigate privacy risks, the Law Council has received the following suggestions from its Constituent Bodies:

- Further consideration should be given to adopting an enhanced risk assessment process for the use of facial recognition technology (including iris, ear and other facial-feature measuring or recognition technology) in line with the model law proposed by the Human Technology Institute of the University of Technology Sydney.[29]
- There is merit in a risk-based approach to regulating the use of facial recognition technology, in which the relevant legal requirements are calibrated to the assessed level of risk, under mandatory Facial Recognition Impact Assessments.
- In relation to the capture and use of facial recognition technology and biometric data more broadly, it is essential to adopt a technology-neutral, risk-based approach to regulation.
- It is crucial to be mindful of the potential downstream privacy risks caused by the amalgamation of data, and interrelatedness of various technologies, particularly in the context of AI.

97. The model used in the Australian Capital Territory (**ACT**) may also be of assistance, in which section 14 of the *Information Privacy Act 2014* (ACT) defines facial recognition technology and biometrics as 'sensitive information'. Further, this legislation:

- prescribes specific safeguards around sensitive information while still acknowledging legitimate expectations;
- includes practical Privacy Principles for departments and others to adhere to; and
- includes an accessible complaints process.

Individual rights (18)

Objection

98. The Law Council supports, in principle, the right to object to the collection, use or disclosure of personal information, pursuant to Proposal 18.2, although some of its Constituent Bodies have observed that this proposed right is somewhat limited in its utility and application.

99. For instance, while an individual is entitled to a written response to their objection from the relevant entity, there is no requirement for the entity to take remedial action resulting from receipt of a valid objection. For organisations, the increased burden of compliance may incentivise them to simply provide generic, proforma responses, with little subsequent recourse for the individual.

100. While the Report notes that this right would be 'modelled on the corresponding right in the GDPR',[30] the Law Council notes that the right to object in the GDPR is also underpinned by the lawfulness of processing requirements under Article 6.

[29] Human Technology Institute, Facial Recognition Technology: Towards a Model Law (Report, September 2022) <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>.
[30] Attorney-General's Department, Privacy Act Review Report (2022), 172.

101. In any event, the Law Council suggests consideration should be given to specifying a reasonable timeframe for the delivery of written responses by entities under Proposal 18.2. A dispute resolution mechanism, following objection, could also be considered.

Erasure

102. The right to erasure at Proposal 18.3 and its corresponding implementation fundamentally requires striking an appropriate balance between an individual's right to control their personal information and other rights (and obligations) to retain and or share or access information.[31]

103. Further, the Law Council reiterates its previous submissions that any right to erasure requires careful consideration and detailed consultation with a broad cross-section of stakeholders, not least because there may be numerous unintended consequences,[32] particularly for the media, who will likely be inundated by erasure applications (i.e., from persons who have been acquitted of a crime which was reported on), which may result in critical archives of newspapers of record being impacted.

104. The Law Council has previously received limited support for a right to erasure amongst its membership, and this was indicated in its January 2022 submission to the Department in response to the Discussion Paper.[33] While some broader support for the right to erasure was indicated during the Law Council's most recent consultation process in March 2023, the Law Council considers that Proposal 18.3 has not been explained adequately in the Report.

105. It will accordingly be important for the Department to articulate exactly what is meant by Proposal 18.3 and whether it is any more than an extension of APP 11.3, requiring destruction or de-identification of information which is no longer necessary, or whether what is contemplated is a broader right to erasure, subject to a limited set of exceptions.

106. The Law Council therefore reserves its view on this proposal until further information is provided, but notes that any exceptions to the right should be strictly limited and proportionate, whether in the employment context or elsewhere. Information should be maintained securely and only retained to the extent strictly necessary to carry out functions and activities to which the information subject has expressly agreed and only for so long as that consent is extant.

De-indexing

107. The Law Council has received mixed views on the right to de-index search results containing certain personal information pursuant to Proposal 18.5.

108. Some of the Law Council's Constituent Bodies have indicated in-principle support for this proposal. However, its Business Law Section's Media and Communications Committee has raised concerns regarding potential adverse practical implications for the media and digital platforms. These potential consequences, should this proposal be implemented, are outlined in Part 2, with reference to experiences in the EU and UK.

---

[31] Monique Magalhaes, Why the GDPR's Right to Erasure may sometimes be wrong, TechGenix (Online, 2018) <https://techgenix.com/right-to-erasure/>.
[32] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 16.
[33] Ibid.

109. The Law Council reserves its position on Proposal 18.5 and recommends that, because the issues are complex and warrant further consideration, this proposal be deferred to a later tranche of reforms to the Act.

Exceptions

Are further exceptions required for any of the proposed rights?

110. The Law Council considers that, if implemented, any exceptions to the proposed rights to access and explanation, objection, erasure, correction and de-indexing should be strictly limited to those which are specified in law, necessary and proportionate. However, it has concerns regarding the exceptions in Proposal 18.6 being cast in very broad terms, where some level of proportionality-based scrutiny is not applied, such as:

- being for 'law enforcement purposes' in Proposal 18.6(a); and
- '(where compliance is) inconsistent with another law or contract with the individual' in Proposal 18.6(b).

111. The Law Council considers there should be strict regulation and limitations on the disclosure and use of private and personal data by law enforcement agencies. Given breaches of privacy by law enforcement agencies can pose significant risks to people's rights and potentially lives (such as in domestic violence situations), a blanket exemption for such agencies should not be encouraged. The Law Council is therefore of the view that the determination as to the precise (or category of) exceptions which could be contemplated must be carefully considered.

112. In determining where it may be a necessity to limit rights, the established proportionality test that is a feature of international human rights law may prove to be a useful example to draw upon in the Act. Such a test is already well understood in jurisdictions with existing Human Rights legislation such as Queensland,[34] Victoria[35] and the ACT,[36] and is currently employed by the Parliamentary Joint Committee on Human Rights.[37]

113. Some Constituent Bodies have suggested to the Law Council that there should be a very limited approach taken in terms of legislating exemptions to the individual rights contemplated by this reform and, on balance, preferred the adoption of a proportionality approach to be used in order to determine when exceptions apply. Conversely, the Business Law Section's Media and Communications Committee has suggested that additional exceptions to the rights of access and erasure would help provide a more proportionate balance between the burden on regulated entities and the perceived privacy benefits. These suggestions are outlined further in Part 2.

[34] *Human Rights Act 2019* (QLD).
[35] *Charter of Human Rights and Responsibilities Act 2006* (Vic).
[36] *Human Rights Act 2004* (ACT).
[37] Parliamentary Joint Committee on Human Rights, Guide to Human Rights (June 2015) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources> 8.

Automated decision-making (19)

114. In relation to ADM, the Law Council supports the recommendations in Proposals 19.1 and 19.2 that:

- privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights; and
- high-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act and supplemented by OAIC Guidance (19.2).

115. In addition, the Law Council supports, in principle, Proposal 19.3 which recommends that a right be introduced for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

116. Beyond these proposals that relate to ADM in the privacy context, the Law Council acknowledges that further consideration should be given to regulation of ADM in the public and private sectors more broadly and recognises the concurrent work in this respect by the Digital Technology Taskforce of the Department of Prime Minister and Cabinet, which the Law Council contributed to in June 2022.[38]

What types of decisions are likely to have a legal or similarly significant effect on an individual's rights?

117. The Law Council supports the broad conception of a 'legal or similarly significant effect' on an individual's rights in considering the widespread use of ADM by government and the private sector, as provided in Proposals 19.1 to 19.3. Nonetheless, as the Report recommends broader work to regulate AI and ADM, the Law Council considers that it would be appropriate to defer these proposals to a later tranche of reforms.

118. Any decisions affecting the essential needs of individuals or access to basic goods, services and utilities (including the pricing of goods and services), as well as government services, should, in the Law Council's view, be construed as 'significant'. ADM may be deployed at multiple levels of the supply chain, and automated decisions by any relevant intermediaries could have significant effects on the rights of individuals.

119. Beyond the proposals in the Report which specifically relate to the interaction of ADM and Australia's privacy regime, the Law Council considers it important that ADM processes which directly affect individual rights and liberties have some level of human oversight, and provide the ability for humans to intervene, as well as provide the opportunity for review of the decision by a human.

[38] See Law Council of Australia, Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper (Submission, 3 June 2022) <https://www.lawcouncil.asn.au/publicassets/06c499e1-5be5-ec11-9452-005056be13b5/2022%2006%2003%20-%20S%20%20Automated%20Decision%20Making%20and%20AI%20Regulaiton%20Issues%20with%20attachments.pdf>.

120. More broadly, where decisions could have a significant or severe effect on the liberties and freedoms of individuals, the Law Council considers that the use of ADM processes may be inappropriate, including in circumstances of modern warfare, end of life decisions for humans and the justice system.[39]

    - Tools of autonomous military warfare, such as drones, purport to make decisions more quickly and with greater accuracy, yet are informed by human programmers and coding. This gives the impression of autonomy, through complex machine learning capabilities that limit the ability for humans to intercede or control decisions, while removing the liability for harm caused as a result of autonomous weapons from human programmers.
    - Decisions which require empathy and insight into the human experience, such as end of life decisions, should not be made using ADM processes. The intersection of medicine, ethics and ADM creates risks for increased discrimination, and the violation of individual privacy and self-determination in a medical context.
    - ADM processes in the justice system of Australian courtrooms could have adverse outcomes and is not supported, particularly where such use would impact on judicial discretion. The Law Council is concerned that ADM processes, which rely on factors derived from historical data to predict future outcomes, would potentially compromise due process and entitlement to a judgment predicated on the overall circumstances of the case.

121. Scrutiny should also be applied in circumstances where ADM processes are used to ensure that it is clear when conclusions reached amount to 'decisions' under the relevant legislation. This would encourage greater public confidence in government agencies and protect people experiencing vulnerability within the community. Examples of conclusions that did not amount to 'decisions', or were wrongfully reached by a government agency, include the automated determination in *Pintarich v Deputy Commissioner of Taxation*[40] and the 'Robodebt' scheme. These examples illustrate a need for improved regulation and oversight of ADM particularly in the delivery of government services and assistance.

122. The Law Council notes that many individuals seeking decisions by social security or migration bodies may be vulnerable, such as low-income earners, elderly individuals or people from culturally and linguistically diverse communities. These groups seeking access to health or insurance information with limited technological literacy are more likely to be adversely impacted by negative automated decisions, particularly where the review process is inaccessible or also requires the use of technology.

123. The Law Council reiterates the point made in its previous submission to the Department that any relevant decisions should be considered in a form that would allow it to be focused on the technology of the day and to be updated regularly. Specifically, while the Act aims to be technology-agnostic, ADM is one area where the law needs to be able to 'keep up' with developments and guide APP entities (many of whom are not aware of ADM) in dealing with the legal impacts of the use of ADM, meaning that flexibility and adaptability are particularly important features of any legislative framework addressing those matters.[41]

---

[39] Ibid 49-50.
[40] [2018] FCAFC 79.
[41] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 16-17.

Should there be exceptions to a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made?

124. The Law Council considers that the right of individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made, pursuant to Proposal 19.3, is necessary to ensure that individuals can exercise their rights to privacy. Any exceptions to the ability to request such information should therefore be subject to the principles of legality, necessity and proportionality.

125. The Law Council recognises that individuals may not be aware that a decision is being made through an automated process, what factors are being considered by the automated process, who the ultimate decision maker is, and whether any correspondence they receive amounts to a 'decision' at all. However, the Law Council notes that there is likely to be significant ambiguity in what is meant by 'meaningful information' as it relates to complex algorithms, as provided in Proposal 19.3.

126. While disclosure and transparency in response to these questions will be required as ADM processes become more prevalent in both public and private entities, the Law Council acknowledges that it may not be feasible—or even possible—to explain the inner workings of many automated systems at all, or at least not in a way that meaningfully assists individuals to understand how decisions have been made. This not only means that the right to request meaningful information is somewhat hollow, but providing individuals with an explanation that does not in fact assist understanding may further diminish trust in the decision-making process.[42] Nevertheless, all ADM must be amenable to judicial scrutiny in the event that affected individuals seek to challenge the outcome. Courts are sufficiently equipped to impose confidentiality regimes in appropriate cases.

127. Further consideration is also required in respect of how the proposed changes would intersect with doctrines of 'commercial in confidence' and/or trade secrets. These doctrines often protect information about the design and processes of automated systems, including when those systems are built by private industry under government contract. Presumably removing the exemption, and consequently giving individuals a right to this information, would abrogate these doctrines. The Law Council considers that while this may be an appropriate balance to strike from a rights perspective, commercial entities may argue that such a policy setting may hinder the development of automated systems.

[42] See Julian Fell et al., How to wrench open the black box of algorithms that decide our fate, ABC News (Online, 12 December 2022) <https://www.abc.net.au/news/2022-12-12/robodebt-algorithms-black-box-explainer/101215902>.

Direct marketing, targeting and trading (20)

Direct marketing

What would be the impact of the proposals in relation to *direct marketing* on individuals, businesses and government?

Definitions and clarity of interaction between laws

128. The Law Council recognises that the way in which personal information is handled for marketing purposes, and the privacy risks associated with direct marketing, have changed dramatically since the APPs were introduced in 2014.

129. The Law Council is broadly supportive of defining the concept of 'direct marketing', pursuant to Proposal 20.1(a). As this term is not currently defined in the Act, this has created some uncertainty for organisations over the activities to which APP 7 (which addresses direct marketing) is intended to apply.

130. However, the Law Council considers that any new definitions require careful drafting to avoid creating further uncertainty and to ensure clarity of interaction between different obligations and laws, as elaborated on in Part 2. An overarching principle of regulation in this area should therefore be to ensure certainty both for organisations and for individuals.

Unqualified right to opt-out

131. The Law Council broadly supports Proposal 20.2 which recommends introducing an unqualified right for individuals to opt-out of their personal information being used or disclosed for direct marketing purposes.[43]

132. However, the Law Council considers that, in practice, there may be a limited difference between the proposed 'unqualified right' and the existing requirement for organisations to provide a simple means by which the individual may easily request not to receive direct marketing communications from that organisation. Proposal 20.2 also appears to be similar to the existing requirement to provide an unsubscribe facility under the Spam Act.[44]

[43] Ibid 211-214.
[44] *Spam Act 2003* (Cth) s 18. Note that subsection 18(3) allows a sender and recipient to a commercial electronic message that is not a 'designated' message to agree that opt-out language need not be included in every such message. In practice, many organisations rely on this provision in a way that is consistent with consumer expectations. For example, if an organisation conducts two or more separate businesses under different brands, it is common for a consumer to agree that the sender need only offer an opt-out for messages relating to one of the brands. There are many examples of businesses that operate a 'multi-brand' strategy when consumers may receive differently branded products or services supplied by the same legal entity, such as Telstra/Belong, CBA/BankWest, Westpac/St George Bank/Bank of Melbourne, Woolworths/Big W, Medibank/ahm. As submitted above, any reform of the direct marketing provisions of the Privacy Act ought to be harmonised with the Spam Act and evaluate the impact of changes on business practices that have evolved to comply with existing provisions of the Spam Act.
[44] Attorney-General's Department, Privacy Act Review Report (2022), 211-214.

133. The Law Council therefore suggests that the Department clarify whether this proposal is intended to impose new process steps for organisations, as this will be important for the purposes of any regulatory impact assessment. In particular, the Department should clarify whether the proposed 'unqualified right to opt out' is intended to:

- be included within each item of direct marketing, as is currently the case in the particular circumstances dealt with under APP 7.3; or
- operate as a standalone process (e.g., by way of an opt-out request accessed via a website, or a request made to an email address).

Interaction with Proposal 20.3

134. In addition, the Law Council submits that clarity will be required in relation to how the 'unqualified right to opt-out' in relation to direct marketing will interact with the similarly proposed 'unqualified right to opt-out' of receiving targeted advertising in Proposal 20.3.

135. The Report indicates that these are intended to operate as separate, but overlapping opt-out mechanisms.[45] Therefore, if an individual elects to opt out of targeted advertising but not direct marketing, an organisation will be able to continue to use personal information to communicate generic marketing, but not targeted advertising, to that individual. On the other hand, if an individual opts out of direct marketing from an organisation, this would—in most circumstances—automatically function as an opt-out from targeted advertising received directly from that organisation.

136. Subject to the Law Council's views on the scope of the proposed regulation of 'targeting' below, it recommends that the drafting of any unqualified right to opt-out must make the interaction between Proposals 20.2 and 20.3 clear. In addition, this should be clarified through OAIC guidance.

Targeting

What would be the impact of the proposals in relation to *targeting* on individuals, businesses and government?

Expansion of the scope of the Privacy Act

137. Proposal 20.1(b) seeks to expand the scope of the Act beyond regulating personal information to introduce new requirements for 'targeting' which uses not just personal information, but also de-identified and unidentified information relating to an individual.

138. The Law Council acknowledges the potential for certain targeted advertising practices to impact consumers. However, the Act is fundamentally focused on the regulation of personal information. The Law Council accordingly submits that the expansion of the Act to regulate behaviours and outcomes which do not relate to, or make use of, personal information would be inconsistent with its current objects.

139. Importantly, this would also distinguish Australia's approach to that adopted in other jurisdictions such as the UK, where its GDPR only regulates targeting to the extent that it involves personal data. Instead, other specific laws and regulations (e.g., the EU ePrivacy Directive) govern targeting based on certain types of electronic data.

[45] Ibid.

140. The Law Council is of the view that regulation of targeting should, for the purposes of the Act, be limited to where *personal information* is collected, used or disclosed for targeting, rather than including de-identified and unidentified information.

Definition of 'targeting'

141. In addition to the threshold issue of the expansion of the scope of the Act outlined above, the Law Council submits that the proposed broad definition of 'targeting' represents a significant expansion of the law, and potentially captures a range of legitimate business activities beyond targeted advertising or marketing, including profiling. 'Profiling' is defined in Article 5 of the GDPR as:

> *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

142. The recent decision of the Federal Court of Australia in *Australian Energy Regulator v Origin Energy Electricity Ltd*[46] highlights the value and necessity of accurately profiling a relevant customer base, particularly in dealings involving vulnerable groups. In that case, Origin Energy's automated processes for dealing with customers experiencing hardship and payment difficulties resulted in it breaching its own hardship policies and the retail rules by:

- unilaterally establishing new customer payment plans if the customer's previous plan had been cancelled for non-payment, while failing to consider a customer's capacity to pay;
- increasing a customer's payment amounts following a review of the customer's usage, while failing to consider the customers' capacity to pay; and
- cancelling customer payment plans where it was unable to discuss with the customer a review of their payment plan, including in circumstances where customers were continuing to make payments under the existing plans.[47]

143. Given this, the Law Council considers several of the activities in the proposed definition of 'targeting' should not be included. This is because they are examples of activities which can, in many circumstances, be treated as either primary or reasonably expected secondary purposes for collection. Examples of acts which should not be captured by the definition of 'targeting' are:

- tailoring an existing product or service to meet an individual's specific requirements (e.g., segmenting customers by reference to attributes, such as age, in order to provide those customers with relevant or inclusive and accessible products or services);
- 'personalised' advertising on social media and other platforms, and embedded in 'free' apps;
- tailoring information about an existing product or service also in a manner designed to meet an individual's specific requirements; and
- providing options to access recommended (non-marketing) content on websites where an individual is logged into their account and the

[46] [2022] FCA 80.
[47] Australian Energy Regulator, Origin penalised $17 million for customer hardship breaches (Media Release, 29 June 2022) <https://www.aer.gov.au/news-release/origin-penalised-17-million-for-customer-hardship-breaches>.

recommended content is based on the individual's personal information, for example their browsing history on that website.

144. The Law Council submits that these are standard, and expected, parts of business activity and do not need to be made subject to new requirements.

145. If a new concept of targeting is to be introduced, the Law Council is of the view that it should be defined to apply only to the collection, use or disclosure of personal information *for advertisements* communicated to an individual. This is particularly important given that Proposal 20.8 seeks to prohibit targeting based on sensitive information. Indeed, the Law Council has several concerns about how Proposal 20.8, would work in practice, as outlined in Part 2.

Impact on the legal profession

146. For the Australian legal profession, the primary impact of these proposals would likely be with respect to the tightening of the consent and opt-out requirements, restrictions on targeted online advertising and the increased level of transparency as to any targeted practices.

147. It is assumed that law practices are otherwise already complying with their obligations under APP 7 and not (generally) trading in personal information or targeting children. However, existing State and Territory advertising restrictions, including in respect of 'claims farming' and personal injury advertising, should also be considered in this context.

Overseas data flows (23)

Question 27: Should the extraterritorial scope of the Act be amended to introduce an additional requirement to demonstrate an 'Australian link' that is focused on personal information being connected with Australia?

148. The Law Council considers that the extraterritorial scope of the Act should be amended to introduce an additional requirement to demonstrate an 'Australian link' and supports Proposal 23.1 which recommends further consultation. This would effectively clarify that foreign organisations will only be regulated to the extent that their handling of personal information has a connection to Australia.

Consequences of the current extraterritorial scope

149. In November 2022, the Law Council provided a submission to the Senate Legal and Constitutional Affairs Committee in relation to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth) (**Privacy Amendment Bill 2022**),[48] which has since been enacted. The Law Council did not support the proposed repeal of paragraph 5B(3)(c),[49] arguing that it would have broader unintended consequences.[50]

[48] Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission, 8 November 2022) <https://www.lawcouncil.asn.au/resources/submissions/privacy-legislation-amendment-enforcement-and-other-measures-bill-2022>.
[49] This has since come into effect by way of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) s 9.
[50] Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission, 8 November 2022) <https://www.lawcouncil.asn.au/resources/submissions/privacy-legislation-amendment-enforcement-and-other-measures-bill-2022> 8-11.

150. Of note is that there are many foreign corporations that carry on business in Australia that are headquartered outside Australia and carry on business in many other jurisdictions. Foreign banks[51] and airlines[52] are obvious examples. As currently drafted, section 5B(3) purports to apply the provisions of the Act to the conduct of these entities in respect of conduct that has no connection with Australia.

151. The Law Council queries why, as a matter of policy and international comity, Australian law should seek to regulate the conduct of a European airline in respect of its handling of passenger data for flights between destinations that do not include an airport in Australia, or the conduct of an American bank in respect of its purely domestic American banking business, simply because that airline or that bank happens to carry on business in Australia.

152. The Law Council is therefore of the strong view that for Australian law to apply to the extraterritorial conduct of such an entity, there should be a rational nexus between the conduct and Australia.

153. At present, the only basis on which a foreign entity that carries on business in Australia could avoid liability under the Act for extraterritorial conduct would be to rely on section 13D, which provides that 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, many lawful and socially useful activities would not be captured by section 13D because those activities are not compelled by law.[53]

154. The Law Council notes that defining an appropriate geographical nexus is not a problem that is new to Australian law, even in relation to cross-border conduct associated with the digital economy. For example, in the criminal law context, Part 2.7 of the *Criminal Code Act 1995* (Cth) provides several tests that must be satisfied to establish a geographical nexus between Australia and conduct that is potentially criminal under Commonwealth law.[54]

155. Prior to the commencement of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) (**Privacy Amendment Act 2022**), an essential element of the test for an 'Australian link' was that 'the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice':

    - The Law Council understands that there was never any actual doubt or practical difficulty in applying the requirement that the information be 'held' in Australia, but the question of where information had been 'collected' had never been settled and the OAIC experienced difficulties in relation to the practical application of this test in some cases.[55]

[51] See the list of foreign banks which have been approved to have an Australian branch at APRA, Register of authorised deposit-taking institutions (Web Page, March 2023) <https://www.apra.gov.au/register-of-authorised-deposit-taking-institutions>.
[52] E.g., British Airways, Cathay Pacific Airways, Emirates, Finnair, Qatar Airways Group, Singapore Airlines and United Airlines are among the entities registered with the Australian Securities and Investments Commission ('ASIC') as foreign companies carrying on business in Australia.
[53] Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission, 8 November 2022) <https://www.lawcouncil.asn.au/publicassets/4d6e625a-8760-ed11-9475-005056be13b5/2022%2011%2008%20-%20S%20%20Privacy%20Legislation%20Amendment%20Bill%202022.pdf> 9.
[54] See, e.g., *Criminal Code Act 1995* (Cth), Part 10.7 ('Computer offences'), where section 15.1 applies in relation to geographical jurisdiction.
[55] See, e.g., *Facebook, Inc v OAIC* [2022] FCAFC [9] at [115]-[153].

- Some organisations adopted the position that information was not 'collected' until it was received by the organisation, and that the place of collection was, therefore, the place at which the information was received for storage by the organisation. There was some merit in that argument, given that the definition of 'collect' in the Act provides that 'an entity collects personal information only if the entity collects the information for inclusion in a record or generally available publication'.

Options for reform

156. The Law Council notes that section 5B of the Act was introduced by the *Enhancing Privacy Protection Act 2012* (Cth) following the Australian Law Reform Commission's (**ALRC**) comprehensive review of the Act in 2008.[56] The accompanying explanatory memorandum provided:

> *The collection of personal information 'in Australia' under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.*[57]

157. The Law Council accordingly considers that one option for reform that would be available to the Parliament, to give effect to the intent expressed above in the explanatory memorandum, would be to re-instate paragraph 5B(3)(c). In addition, additional wording could be provided to clarify that personal information will be taken to be collected in Australia or an external Territory for the purpose of paragraph 5B(3)(c) when it is received by the organisation or operator by electronic means from an individual who appears to be in Australia or an external Territory,[58] regardless of the location of the organisation or operator who collects or stores the information.

158. The Law Council is of the view that this would be the simplest approach, consistent with the original intention of the Parliament, which will likely have the joint effects of removing the difficulties faced by the OAIC in proving the place of collection in matters involving cross-border digital practices, as well as ensuring that the Act does not purport to regulate the conduct of entities that carry on business in Australia in respect of personal information that has no nexus to Australia.

159. The explanatory memorandum to Privacy Amendment Bill 2022 stated that a purpose of removing paragraph 5B(3)(c) from the Act was to:

> *…reflect that in the digital era, organisations can use technology such that they do not collect or store information directly from Australia. However, these organisations will often still otherwise be carrying on a business in Australia, and should be required to meet the obligations under the Privacy Act.*[59]

---

[56] ALRC, For Your Information: Australian Privacy Law and Practice (Report 108, August 2008) <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/>.
[57] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 218.
[58] There may need to be exceptions for individuals using a Virtual Private Network which obscures their original IP address or other location information.
[59] Explanatory Memorandum, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, 13 [19].

160. However, the Law Council notes that, to the extent that a foreign entity carrying on business in Australia indirectly collects personal information about Australians from an intermediary that is an APP entity with an Australian link, section 16C of the Act imposes liability on the APP entity that disclosed the information (i.e., the intermediary) in respect of conduct by the foreign recipient that would have contravened the Act, had it occurred within Australia.

161. Consequently, if the Government's intention is to introduce primary liability for offshore recipients that carry on business in Australia and receive personal information about Australian citizens or residents indirectly (that is, not directly from individual data subjects), then the re-introduction of paragraph 5B(3)(c), accompanied by a deeming provision (as proposed above) would not achieve that intention, since the deeming provision only contemplates direct collection by the foreign entity from an individual in Australia.

162. Instead, it would be necessary to introduce a requirement that the personal information relates to an individual in Australia, and that it be collected by the foreign organisation or entity from a source in Australia. In addition, it would be appropriate to make a consequential amendment to section 16C to excuse an exporter from liability to the extent that an offshore recipient is primarily liable under the Act.

Enforcement (25)

Creating tiers of civil penalty provisions

163. The Law Council considers that introducing separate 'mid-tier' and 'low-level' civil penalties pursuant to Proposal 25.1 would add a significant level of complexity to the enforcement regime for the Act, and even more so if a direct right of action and/or a statutory tort for serious invasions of privacy were to be introduced.

164. According to the Report, mid-tier civil penalties would be awarded by a court for any contravention of the Act that the Information Commissioner, in their discretion, decides is not sufficiently 'serious' to justify action under section 13G, and low-level penalties would be levied by the Information Commissioner through infringement notices issued in accordance with the framework set out in Part 5 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth).[60]

165. The Law Council supports the introduction of a 'mid-tier' civil penalty provision as proposed, with a maximum penalty of 2,000 penalty units. This could be utilised by the Information Commissioner in cases that involve conduct falling short of the 'serious' standard to which section 13G applies, but which are nevertheless sufficiently important to justify enforcement action in a court in order to deter similar conduct by others.

166. However, the Law Council is not supportive, at this time, of the introduction of an infringement notice regime for 'minor administrative breaches' as proposed.

[60] Attorney-General's Department, Privacy Act Review Report (2022), 253-256.

167. In relation to 'low-level' penalties, the Report states that 'the amount payable under an infringement notice is typically 20 per cent or less of the maximum amount of the related civil penalty provision.'[61] If the benchmark to which the 20 per cent is applied is section 13G as currently in effect, that would result in the Information Commissioner having power to issue a 'low level'' penalty of up to $10 million. The Law Council regards this penalty to be significantly disproportionate to the need to deter 'minor administrative breaches'.

168. The Law Council submits that it would be preferable to keep this potential amendment under review as experience emerges in relation to the operation of a direct right of action and/or a statutory tort.

169. The Information Commissioner currently has powers to investigate (either in response to a complaint or on their own initiative) contraventions of the kind proposed as candidates for 'administrative breaches' and to make a determination under section 52 of the Act. A declaration of contravention,[62] coupled with a declaration that the respondent take specified steps to ensure that conduct is not repeated,[63] is an appropriate remedy for or a minor administrative breach. If the Information Commissioner considers that their determination powers are insufficient in a particular case, then a 'mid-level' civil penalty would be available.

Replacing 'serious or repeated' with 'serious'

170. The Law Council supports Proposal 25.2, which recommends replacing the phrase 'serious or repeated' with 'serious' in section 13G of the Act and clarifying what a 'serious' interference with privacy may include. However, there will be a need to consider how this amendment will be applied, also noting the role of the OAIC.

171. Given the very large maximum penalties now available after the enactment of the *Privacy Amendment Act 2022*, there should not be any scope for argument that a contravention in respect of every individual whose privacy has been interfered with is a separate 'serious' contravention.

172. Rather, if there has been a course of conduct affecting many individuals, it is appropriate for one 'serious' contravention to apply, with the number of individuals affected to be taken into account in assessing the seriousness of the conduct and the corresponding penalty.

A direct right of action (26)

173. The Law Council's previous submission to the Department indicated that there was a diversity of views amongst its membership on the private right of action under the Act's data protection regime, but nonetheless provided in-principle support for such a right, provided that the scope of the cause of action is well defined and articulated in the updated Act.[64]

[61] Ibid 255.
[62] *Privacy Act 1988* (Cth) sub-para 52(1)(b)(i).
[63] Ibid sub-para 52(1)(b)(ia).
[64] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 20.

174. In relation to Proposal 26.1, there remains a diversity of views within the Law Council's membership, albeit to a lesser extent. Its Business Law Section's Privacy Law Committee and submitting Constituent Bodies have expressed in-principle support. However, the Business Law Section's Media and Communications Committee does not support the proposal and is of the view that, together with the proposed introduction of a statutory tort for serious invasions of privacy, this reform would have a significant adverse impact on press freedoms and the Constitution's implied freedom of political communication in Australia. The Law Council reiterates that any reform in this area must have careful regard to the High Court's test in *Lange v Australian Broadcasting Corporation*[65] in this respect.

175. On balance, and subject to further consideration being given to the consequence that a direct right of action for affected individuals could potentially lead to an exacerbation of their loss of privacy, the Law Council continues to support, in principle, a direct right of action, and reiterates the following observations made in its previous submission:[66]

- Careful consideration of the drafting of the right is required to ensure that there are no unintended consequences and all causes of action, as updated by the reform process, can be considered in context.
- The creation of such a right and corresponding remedies must not detract from the powers and resources afforded to the OAIC in its investigative and enforcement functions.
- Any proposed process to pursue a right of action (first through the OAIC and then the Federal Court) would need to be balanced and not become an impediment to a person's right of action. This requires the OAIC to have sufficient resources dedicated to responding to initial claims so that the process does not unduly delay a resolution. At present, it is understood that the OAIC expends considerable time and resources in conciliation processes following complaints, often in circumstances which do not raise issues which relate to the Act at all, or which are of a trivial manner. This issue will also need to be addressed.

Statutory tort for serious invasions of privacy (27)

176. The Law Council has received a variety of views on Proposal 27.1, which recommends introducing a statutory tort for serious invasions of privacy in the form recommended by the ALRC. It is expected that reasonable minds across the legal profession will differ in respect of any introduction of a new cause of action which would expand tort law in Australia, as would be the case should this proposal be adopted. It is therefore essential that certainty and clarity in respect of the scope of any such cause of action be provided.

[65] 189 CLR 520.
[66] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 20.

177. The Law Council has previously expressed in-principle support for the introduction of a statutory tort for serious invasions of privacy as recommended by the ALRC,[67] and for the reasons it outlines,[68] on the condition that there are sufficiently high thresholds in place to ensure actions are limited to serious invasions of privacy.[69] However, as with a direct right of action noted above, the scope of the statutory tort must be carefully considered and drafted to address the risk of unintended consequences,[70] particularly having regard to more recent developments affecting these issues, both domestically and internationally.

178. The Law Council acknowledges that there are practitioners within its membership who do not support the introduction of a statutory tort for serious invasions of privacy. As noted above, a divergence of views across the profession is to be expected, given the significant nature of what is being proposed and the varied interests that legal practitioners represent. By way of illustration, its Business Law Section's Media and Communications Committee has provided a coherent rationale for not supporting Proposal 27.1, instead favouring increased resourcing being provided to the OAIC to assist in enforcement. These views are set out in Part 2.

179. The Business Law Section's Media and Communications Committee has expressed the view that should the Government proceed with the statutory tort and/or the direct right of action, all content produced for journalistic, academic, artistic and literary purposes should be exempt. Further, if a statutory tort is introduced, the Business Law Section's Media and Communications Committee has indicated in-principle support for the ALRC's model, in which 'the cause of action should not extend to negligent invasions of privacy, and should not attract strict liability.'[71]

180. On balance, noting the developing international jurisprudence in this area,[72] and its previous positions on this issue, the Law Council supports, in principle, the introduction of a statutory tort in the form recommended by the ALRC, and on the condition that further consideration is given to the consequence that such a tort could lead to an exacerbation of loss of privacy, there are sufficiently high thresholds in place to ensure actions are limited to serious invasions of privacy. The Law Council therefore encourages the provision of additional clarity and further consultation, including with the States and Territories, to promote a consistent approach. It may be that a statutory duty to maintain the confidentiality of personal information would be sufficient to ground an action for breach of that duty, thereby importing existing principles of negligence rather than requiring a new branch of jurisprudence for a wholly separate statutory tort.

---

[67] ALRC, Serious Invasions of Privacy in the Digital Era (Report 123, June 2014) <https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf>.
[68] Some reasons provided by the ALRC included that invasions of privacy by intrusion or misuse of private information are known to occur in a wide variety of circumstances; where Australian media have unjustifiably invaded a person's privacy and the plaintiff complains, they may have settled the plaintiff's claims to avoid litigation, publicity and the setting of the precedent; litigants have been reluctant to risk lengthy and costly proceedings and appeals arguing a novel point of law; there is more flexibility in the development of the law by statute than by common law and it can be effected more rapidly; and statutes may be more effective in having a normative impact on behaviour.
[69] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 20.
[70] Ibid.
[71] ALRC, Serious Invasions of Privacy in the Digital Era (Report 123, June 2014) <https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf> 109.
[72] See, e.g., *Lloyd v Google* [2021] UKSC 50.

181. The Business Law Section's Privacy Law Committee has expressed concerns that the simultaneous introduction of both the direct right of action and the statutory tort would risk confusion and create potentially overlapping processes. It has accordingly expressed the view that the direct right of action should, subject to the Law Council's comments above, be prioritised over the statutory tort. For that right to have practical utility, consideration should be given to absolving applicants for relief from the need to provide security for costs.

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

Notifiable data breaches scheme (28)

183. The NDB scheme creates a mechanism for the notification to the OAIC and to individuals of an eligible data breach, where that data breach is likely to result in serious harm to an individual whose personal information is involved.

184. With the implementation of the NDB scheme in 2018, and with additional powers created in 2022, the Law Council recognises that several practical issues have arisen with respect to the administration of the NDB scheme and difficulties for APP entities to comply with the NDB scheme, as outlined in Part 2. Given these existing issues, the current process of review provides an opportunity to refine and improve the NDB scheme to align with the changing environment.

185. Many of the issues concern the interaction of APP entities with other entities and the consequences of having multiple organisations involved in the supply chain and therefore the impact assessment and notification process that forms an essential part of steps taken by APP entities to comply.

186. The Law Council welcomes Proposal 28.1 and invites further consideration of the following matters (amongst others) as the reforms progress:

- The legal status (if any) of informal, preliminary or voluntary notifications, especially where they are subsequently updated by some or all the APP entities and there is a view by some—but not all—entities that, based on further investigations, the data breach is one that is not 'likely to result in serious harm'.
- Updating the guidance on interpretation of 'likely to cause serious harm' to reflect changes that have been, or may be made, to definitions of serious harm or any matters that are to be covered by civil penalties.
- Effective means of communicating with impacted individuals and the legal status of these communications in respect of any actions that the individual may take. This is required because many data breaches involve APP entities that supply services to another entity and may not always have a requisite relationship with impacted individuals.

187. Finally, any legislative response to data breaches under the Act must be consistent with the Government's 2023-2030 Australian Cyber Security Strategy,[73] once finalised, which the Law Council notes the Department of Home Affairs is currently consulting on. The Law Council cautions that care ought to be taken to ensure that any changes to the Act in this respect do not conflict with the ultimate outcome in the Australian Cyber Security Strategy.

[73] Department of Home Affairs, 2023-2030 Australian Cyber Security Strategy (Web Page, 2023) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>.

Part 2: Law Council positions and additional comments on each proposal

No.	Proposal	LCA Position	Comments
Objects of the Act			
3.1	Amend the objects of the Act to clarify that the Act is about the protection of personal information.	Support in principle	• This is not an overarching right (as in the EU) but informs how the balancing of interests is to be addressed. • Consider impact on new broad rights (i.e., Proposal 12—fair and reasonable personal information handling).
3.2	Amend the objects of the Act to recognise the public interest in protecting privacy.	Support in principle	• On one hand, there is potential benefit in clarifying upfront in section 2A that the Act is about the protection of personal information and recognising the public interest in protecting privacy. • On the other hand, the Law Council acknowledges the concerns of some practitioners, including its Business Law Section's Media and Communications Committee, that Proposal 3.2 risks elevating the public interest in privacy above countervailing public interests, including the public interest in freedom of expression. Australia does not have the broad protections for the right to freedom of expression that is enshrined in the laws of the UK, USA, Canada and New Zealand, so this risk is very real.
Personal information, de-identification and sensitive information			
4.1	Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.	Support in principle	<u>History and interpretation of definition of 'personal information'</u> • The definition of 'personal information' in section 6 of the Act was introduced as part of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (**Enhancing Privacy Protection Act 2012**). These changes, which came into effect in 2014, were substantial, as they expressly: – removed references to 'information or opinion (including information or an opinion forming part of a database'; and – removed references to 'an individual whose identity is apparent or can reasonably be ascertained', replacing them with the terms 'identified' and 'reasonably identifiable'. • The result of these changes was a substantial expansion in the type of information that would now comprise 'personal information' under the Act. The Law Council notes that the intention of these changes was to:

No.	Proposal	LCA Position	Comments
			…cast in terms of identification of individuals because this language is more consistent with the APEC Privacy Framework and other international instruments, which means that international jurisprudence and explanatory material will be more directly relevant to the Privacy Act.[74] • The only time that the definition of personal information has had the benefit of judicial review was in 2017, in *Privacy Commissioner v Telstra Corporation Limited*.[75] Importantly, the Federal Court of Australia was making its decision on the definition of 'personal information' which preceded the-Enhancing Privacy Protection Act 2021, not the definition which is the subject of this Report and accompanying proposals. • Much has been said about the fact that the Federal Court focused on the significance of the word 'about', noting that it had important work to do in identifying what information could have an appropriate link to the individual and hence be included in the definition of personal information. • The emphasis on the word 'about' continues to be a point of discussion and debate since the decision was made in 2017. In this respect, Proposals 4.1 to 4.4 inclusive, if appropriately drafted, would address the ambiguity, and create the required alignment. • However, the current definition of 'personal information' has not been the subject of judicial review. This is important to note during the current window of reform as the current Review process provides an opportunity to clarify critical aspects of the definition. This should extend not only to the first limb of the definition and the use of the word 'about', but also to other components of the definition, most notably the second and significant part of the definition as to what makes an individual 'identified' or 'reasonably identifiable' in the circumstances. • The Law Council notes that in several significant determinations by the OAIC, where the scope of the definition was an issue, the OAIC favoured a more expanded definition of 'personal information'.[76]

[74] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 61.
[75] [2017] FCAFC 4.
[76] See, e.g., Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) and Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021).

No.	Proposal	LCA Position	Comments
4.2	Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.	Support	• Guidance can be industry-specific and can reflect input by relevant associations and other regulators. • Considerations can include, by way of example: – whether information was previously de-identified and that process has been reversed; – risk factors as per the GDPR; and – factors listed in the definition of 'personal data' under Article 4 of the GDPR. – Consider an independent source of guidance, noting the materiality of the issues
4.3	Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.	Support	• This is a clarification as this information is arguably already in scope, noting the definition of 'personal information' and data generated and express inclusions of opinions.
4.4	'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.	Support	• This is a clarification.
4.5	Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.	Does not support	• The Act's purpose is to regulate personal information as defined. 'De-identified information' is outside of its scope. • See discussion in submission.
4.6	Extend the following protections of the Privacy Act to de-identified information: (a) APP 11.1—require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure.	Does not support	• The Act's purpose is to regulate personal information as defined. 'De-identified information' is outside of its scope. • See discussion in submission.

No.	Proposal	LCA Position	Comments
	(b) APP 8—require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification. (c) Targeting proposals—the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.		
4.7	Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.	Support consulting, but caution recommended regarding introducing a criminal offence	The Law Council makes the following preliminary points, based on feedback received from its Constituent Bodies and its Business Law Section's Privacy Law Committee: • The civil nature of the privacy regime should be solely supported by a civil penalty regime. • Where re-identification occurs as the result of poor information handling practices, in the absence of intent, the imposition of a criminal offence is unlikely to be appropriate, but consideration should be given to providing further guidance to assist entities to avoid negligent or inadvertent re-identification. • While there may be some justification for instituting a criminal offence for very severe and malicious re-identification, such harm would be more appropriately dealt with under the proposed statutory tort for serious invasions of privacy in accordance with Proposal 27.1. • Should a criminal offence be introduced, it would require careful delineation to ensure that privacy rights are balanced against the ability of individuals to know what conduct would be unlawful. • The definition of 'illegitimate benefit' could include the re-identification of de-identified information for commercial gain. • A defence may be introduced where the re-identification of de-identified information is in the public interest and strictly necessary.

No.	Proposal	LCA Position	Comments
			• Other impacts of criminalising behaviours on the current market and submarket in data should be considered, as well as issues created by ransomware and payments of ransoms.
4.8	Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where: (a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way. (b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information.	Does not support	• The Act is to regulate personal information as defined. • Steps to prohibit an APP entity from re-identifying are part of steps to protect personal information.
4.9	Sensitive Information (a) Amend the definition of sensitive information to include 'genomic' information. (b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act. (c) Clarify that sensitive information can be inferred from information which is not sensitive information.	Support	• This is a clarification.
4.10	Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.	Supports in principle	• This proposal will require more clarity, as tracking is an ongoing activity (like surveillance) and geolocation data is a type of information. • See discussion in submission.

No.	Proposal	LCA Position	Comments
Flexibility of the APPs			
5.1	Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code. In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.	Does not support	• Requires more clarity as there is the potential for conflict and uncertainty, as well as a potential risk to the separation of powers. • Can be addressed by having a clear and robust system of issuing opinions.
5.2	Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.	Position reserved	
5.3	Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to: (a) entities, or classes of entity (b) classes of personal information, and (c) acts and practices, or types of acts and practices.	Position reserved	
5.4	Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.	Position reserved	

No.	Proposal	LCA Position	Comments
5.5	Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.	Position reserved	• Some concerns and queries with this approach (i.e., Is this proposal intended to support the information sharing as contemplated under the amendments to the *Telecommunications Regulations 2021* (Cth)?).
Small business exemption			
6.1	Remove the small business exemption, but only after: (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations.	Support in principle	• Need to consider timing and implementation structure. • See discussion in submission.
6.2	In the short term: (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.	Support in principle	• These short-term measures may not be necessary if addressed per Proposal 6.1. • See discussion in submission.

No.	Proposal	LCA Position	Comments
Employee records exemption			
7.1	Enhanced privacy protections should be extended to private sector employees, with the aim of: (a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for; (b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information; (c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and (d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.	Support in principle	• Need to consider timing and implementation structure. • See discussion in submission.

No.	Proposal	LCA Position	Comments
Political exemption			
8.1	Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.	Position reserved	
8.2	Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.	Position reserved	
8.3	The political exemption should be subject to the following requirements: (a) Political acts and practices covered by the exemption must be fair and reasonable. (b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union. The political exemption should include a savings clause as per Recommendation 41–2 of ALRC Report 108.	Position reserved	
8.4	The political exemption should be subject to a requirement that individuals must be provided with the means to: (a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and (b) opt-out of receiving targeted advertising from a political entity.	Position reserved	

No.	Proposal	LCA Position	Comments
8.5	The political exemption should be subject to a requirement that political entities must: (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.	Position reserved	
8.6	The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.	Position reserved	
Journalism exemption			
9.1	To benefit from the journalism exemption a media organisation must be subject to: (a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), *or* (b) standards that adequately deal with privacy.	Position reserved	The Law Council notes that in response to the specific proposals in the Report relating to the journalism exemption, its Business Law Section's Media and Communications Committee has raised the following concerns: • To accept that some APPs might apply to media organisations is inconsistent with the underlying policy of the exemption and opens the door to more provisions of the Act applying over time, significantly limiting the benefits of the exemption and impeding the effective functioning of media businesses. • As outlined in the Report, relatively few complaints in relation to privacy regarding journalism are upheld.[77] • The combined effect of Proposals 9.1 and 9.2 is that the journalism exemption will only apply to media companies that are subject to privacy
9.2	In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.	Position reserved	
9.3	An independent audit and review of the operation of the journalism exemption should be commenced three	Position reserved	

[77] Attorney-General's Department, Privacy Act Review Report (2022), 85.

No.	Proposal	LCA Position	Comments
	years after any amendments to the journalism exemption come into force		standards overseen by a recognised body or that otherwise, in the opinion of the OAIC, adequately deal with privacy. – This means the OAIC would have approval rights for privacy standards for media organisations. – This would not be appropriate, given the lack of experience of the OAIC in undertaking the role of balancing the protection of personal information against rights of freedom of expression.
9.4	Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.	Position reserved	
9.5	Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.	Position reserved	• It is difficult to see how APP 11, which relates to the security of personal information, could sensibly be applied to activities within the journalism exemption, as is set out in Proposal 9.4. • The role of journalism is to disclose information, and APP 11.1 is an example of a rule which does not sit well with that role.[78] • The application of APP 11.2 is also problematic.[79] The Business Law Section's Media and Communications Committee queries that as the records of journalists provide a history of matters of public interest, what basis can there be for these to be destroyed? • There is no clear policy rationale or empirical evidence provided in the Report to support Proposal 9.5, which provides that a modified version of the NDB scheme should apply to acts and practices in the course of journalism, which would undermine the efficacy of the journalism exemption.
Privacy policies and collection notices			
10.1	Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.	Support in principle	• The Law Council notes some conflicting priorities of additional details (e.g., on retention) and clarity.
10.2	The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the	Support in principle	

[78] An APP entity is required to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.
[79] An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

No.	Proposal	LCA Position	Comments
	individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice: (a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.		
10.3	Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	Support	• There is a need for independent structures and status of opinions.
Consent and privacy default settings			
11.1	Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.	Position reserved	• The Law Council notes that the regime is not consent-based and overreliance on consent has unintended consequences.[80] • It also notes the medical origins of the word 'informed' and the different setting in the information context.
11.2	The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing	Position reserved	• Note the need for independent structures and status of opinions.

[80] See Eugenia Politou et al., Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, *Journal of Cybersecurity* (2018) 1, <https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056>.

No.	Proposal	LCA Position	Comments
	standardised consents as part of any future APP codes.		
11.3	Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	Position reserved	• If this proposal is adopted, it will be important to have guidance regarding circumstances in which it is not practically feasible to withdraw consent.
11.4	Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.	Position reserved	• Arguably already part of the law.
Fair and reasonable personal information handling			
12.1	Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.	Support in principle	<u>Notions of 'reasonable' and 'fairness'</u> • The term 'reasonable' is not defined in the Act. However, the concept of reasonableness is well known and understood, having been the subject of considerable case law[81] and regulatory guidance.[82] It is generally accepted that the APP entity has the onus of establishing that its conduct was reasonable. Embedded in the concept of reasonableness is the notion of balancing different factors, interests and considerations and applying these to the given facts. • The notion of 'fairness' is well known in consumer protection and anti-discrimination legislation. The requirement for fairness is referenced in some data protection requirements and typically is formulated to address a notion of transparency, such as under the EU GDPR and UK GDPR the requirement is to process information 'lawfully, fairly and in a transparent
12.2	In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (b) the kind, sensitivity and amount of personal information being collected, used or disclosed	Support in principle.	

[81] *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).
[82] OAIC, Chapter B: Key Concepts (Web Page, 2022) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#key-concepts-r-to-z>.

No.	Proposal	LCA Position	Comments
	(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and (g) the objects of the Act. The Explanatory Memorandum would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and (c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.		manner in relation to the data subject'.[83] It could also be said that fairness is component of valid consent under the GDPR.[84] • While notions of fairness and unfairness tend to be used interchangeably in international jurisdictions (e.g., Recital 42 of the GDPR provides that a declaration of consent 'should not contain unfair terms'), there appears to be no similar test of fairness *and* reasonableness as a positive overarching obligation imposed, as recommended in Proposals 12.1 to 12.3. • The notion of 'fairness' has received attention in the context of data ethics and guidance on the use of artificial intelligence (**AI**). For example: – In the Monetary Authority of Singapore's Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, the notion of fairness is referenced as part of the need for justifiability, freedom from discrimination and governance frameworks requiring that individuals (or groups of them) 'are not systematically disadvantaged through AI-driven decisions unless these decisions can be justified.'[85] – The UK Information Commissioner's *Guidance on AI and data protection* also references fairness in the context of non-discrimination and freedom from bias, recognising the need to balance different, competing interests.[86] • Consideration of data uses is based on developed concepts of automated decision making, expressly regulated under the data protection regime.[87] Importantly, these are *specific additional* rules applying to 'solely

[83] See Article 5(1)(a) of the UK GDPR and Information Commissioner's Office, Guidance for the use of personal data in political campaigning (Web Page, 2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/>.
[84] See GDPR (EU) Recital 42.

[85] Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector (November 2018) <https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf> 6.
[86] Information Commissioner's Office, Annex A: Fairness in the AI lifecycle (Web Page, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/annex-a-fairness-in-the-ai-lifecycle/>.
[87] See UK GDPR and EU GDPR, Article 22.

No.	Proposal	LCA Position	Comments
12.3	The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.	Does not support	automated decision-making that has legal or similarly significant effects'[88] on individuals, not to *all* processing of personal data in *all* circumstances.
Additional protections			
13.1	APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.	Support in principle	• The Law Council notes the need for guidance on what is 'high risk'. • The production of any Privacy Impact Assessment to the OAIC should only extend to those Privacy Impact Assessments undertaken subsequent to the implementation of Proposal 13.1, if implemented. • See discussion in submission.

[88] Information Commissioner's Office, What is the impact of Article 22 of the UK GDPR on fairness? (Web Page, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-is-the-impact-of-article-22-of-the-uk-gdpr-on-fairness/>.

No.	Proposal	LCA Position	Comments
13.2	Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.	Position reserved	• See discussion in submission.
13.3	The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.	Support	
13.4	Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.	Position reserved	
Research			
14.1	Introduce a legislative provision that permits *broad consent* for the purposes of research: (a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply. (b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.	Support	

No.	Proposal	LCA Position	Comments
14.2	Consult further on broadening the scope of research permitted without consent for both agencies and organisations.	Support	• Any interference with the right to privacy should be consistent with the principles of legality, necessity and proportionality. • Prior and informed consent to the use of private information should be considered the foundation for legitimate use. • Any broadening of the scope of permitted use without such consent should be limited to that which is specified in law, strictly necessary and appropriate.
14.3	Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.	Support	
Organisational accountability			
15.1	An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.	Position reserved	
15.2	Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.	Position reserved	
Children			
16.1	Define a child as an individual who has not reached 18 years of age.	Support	
16.2	Existing OAIC guidance on children and young people and capacity should continue to be relied upon by APP entities. An entity must 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, an entity may assume an individual over the age of 15 has	Support	

No.	Proposal	LCA Position	Comments
	capacity, unless there is something to suggest otherwise. The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).		
16.3	Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child. In the context of online services, these requirements should be further specified in a Children's Online Privacy Code.	Support	
16.4	Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.	Support	
16.5	Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.	Support	

No.	Proposal	LCA Position	Comments
	The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted. The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.		
People experiencing vulnerability			
17.1	Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.	Support	• This list of factors could include:[89] – age-related impairment; – cognitive impairment; – disabilities; – First Nations status; – English fluency; – literacy levels; – socio-economic capacity; – physical or mental illness; and – any other personal or financial circumstances that might indicate vulnerability. • These facts should act as 'red flags' to put institutions on notice that a more considered and careful approach is required in relation to that particular customer, while taking case to preserve that individual's autonomy to the greatest extent possible.
17.2	OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.	Support	• Individuals should not be assumed to lack requisite capacity merely because they exhibit factors that point to vulnerability. • Capacity, as well as supported and substitute decision-making are protective concepts as opposed to restrictions on or removal of people's rights.[90]

[89] See, as a starting point, the Australian Banking Association ('ABA'), Banking Code of Practice (Revised 5 October 2021), Chapters 14 and 17; ABA, Preventing and responding to family and domestic violence (Industry Guideline, updated March 2021); ABA, Preventing and responding to financial abuse (including elder financial abuse) (Industry Guideline, updated March 2021).
[90] Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 15.

No.	Proposal	LCA Position	Comments
			• Therefore, lay people should be cautious of making their own 'assessments' of capacity, which may have flow on impacts for an individual and that assistance should be sought from a health practitioner.[91]
17.3	Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.	Support	• The Law Council notes that the right to privacy is not unqualified and that any interference with the right to privacy should be consistent with the principles of legality, necessity and proportionality.
Rights of the individual			
18.1	Access and explanation: Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features: (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act) (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual.	Position reserved	• The Law Council queries the appropriateness of organisations, particularly large organisations, charging 'nominal fees' under Proposal 18.1(e). • An entity's costs in complying with its privacy its privacy obligations under the Act should arguably be construed as reasonable costs of doing business, noting that exceptions for frivolous or vexatious requests are included under Proposal 18.6(c). • Consideration could perhaps be given to allowing small businesses to charge nominal fees to comply with Proposal 18.1 given the costs associated with removing the small business exemption.

[91] Ibid.

No.	Proposal	LCA Position	Comments
18.2	Objection: Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.	Support in principle	• This right is somewhat limited in its utility and application: see discussion in submission.
18.3	Erasure: Introduce a right to erasure with the following features: (a) An individual may seek to exercise the right to erasure for any of their personal information. (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.	Position reserved	• See discussion in submission.
18.4	Correction: Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.	Position reserved	
18.5	De-indexing**:** Introduce a right to de-index online search results containing personal information which is: (a) sensitive information [e.g. medical history], or (b) information about a child, or (c) excessively detailed [e.g. home address and personal phone number], or (d) inaccurate, out-of-date, incomplete, irrelevant, or misleading.	Position reserved	The Law Council notes potential adverse practical implications and consequences which may arise for platforms, the media and freedom of expression, should the right to de-index be implemented, as provided by its Business Law Section's Media and Communications Committee. Impact on freedom of expression • Although the Report notes that de-indexed content 'remains at its source on the internet',[92] when information is not accessible through a search engine (typically Google, the dominant search engine), it is lost to users. The practical reality is that the information will be effectively removed from the internet upon its de-indexing because it will be virtually impossible to find, which will significantly impact freedom of expression.

[92] Attorney-General's Department, Privacy Act Review Report (2022), 178.

No.	Proposal	LCA Position	Comments
	The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.		• Moreover, search results provide valuable referrals to media company websites. The right of de-indexing will negatively impact such referral traffic. • Should the proposed right to de-indexing be implemented, a slippery slope may occur in which this right is extended beyond online search results to other online resources (i.e., in order to block 'inaccurate' Wikipedia entries about public figures, or the news webpage that contains the inaccurate media reporting). <u>Adjudication process</u> • In relation to the proposed adjudication process, at least in the majority of cases, search engines will make determinations of whether to de-index content based *only* on information provided by the requester. It is unclear what the public policy rationale would be to allow Google, or any other search engine (as a private company operating without oversight in this process), and based on incomplete information, to determine whether or not to de-index content. • It is inappropriate and undesirable to assign platforms the role of arbiters of what is 'inaccurate or misleading', especially given the potential volume of requests. If whether or not a piece of public interest reporting is 'inaccurate or misleading' is part of the balancing exercise, the platform has a deficit of information. It has no access to original sources, no context and no concept of whether or not the material qualifies as 'in the public interest' beyond what is apparent on the face of the material. • The statistics in the Report indicate that Google does not truly undertake a thorough analysis of whether or not to de-index content and will generally simply undertake the de-indexing requested,[93] largely looking only at whether or not the relevant content includes personal information. • The problematic practical operation of this right in Europe and the UK is compounded by the fact, in reality, only the individual seeking the de-indexing has a right of appeal from Google's arbitrary decision making process. In other words, individuals have rights of appeal to a third party regulator, but website owners, such as media companies, do not.

[93] Ibid.

No.	Proposal	LCA Position	Comments
			• The Business Law Section's Media and Communications Committee therefore suggests that if there is to be any form of a de-indexing right, it should probably involve a preliminary process as between the originator of the content and the requesting person. The requesting person can show the content originator that material is inaccurate or misleading, and test that assertion with the originator. It is preferable for news media to be provided with proof of the inaccuracy from the requesting person in the first instance, rather than risk having stories rendered completely invisible in search by virtue of a risk-based decision made by a platform without access to the underlying facts. <u>Lack of clarity on burdens of proof and interaction with defamation law</u> • The Business Law Section's Media and Communications Committee has also raised that there is a lack of detail in this proposal about burdens of proof, particularly, who bears the burden of establishing that the relevant information is incomplete, irrelevant, inaccurate or out of date in order to enliven the right to de-index it. In addition, there is a lack of clarity in relation to how long the platform has to make its decision. While the Report points to the EU as having a proof of concept,[94] the EU is still grappling with these fundamental mechanics. • It is also unclear how this proposal will interact with defamation law, which has been used as a proxy for a 'right to be forgotten' in Australia for the last decade. Search engines already receive de-indexing requests and sometimes they act on them, and other times they do not, including for the reasons described above. It is a difficult endeavour for a search engine (or any other platform for that matter) to essentially reverse-engineer a public interest news story, to assess whether it is defensible in defamation. • This proposal is an ideal candidate for further consideration in a later tranche of privacy reforms. This should be aligned with, and complement, the adjacent Stage 2 defamation reforms and therefore this proposal should be progressed further after Stage 2 is settled and implemented.
Exceptions			
18.6	Introduce relevant exceptions to all rights of the individual based on the following categories:	Position reserved	• Some caution may need to be exercised in considering Proposal 18.6(b), as entities may attempt to contract out of rights and responsibilities.

[94] Ibid 177.

No.	Proposal	LCA Position	Comments
	(a) **Competing public interests:** such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. (b) **Relationships with a legal character:** such as where complying with the request would be inconsistent with another law or a contract with the individual. (c) **Technical exceptions:** such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.		• Anti-avoidance measures may assist to guard against unintended consequences. • The Business Law Section's Media and Communications Committee is of the view that additional exceptions to the rights of access and erasure would help provide a more proportionate balance between the burden on regulated entities and the perceived privacy benefits, including: – broadening the proposed exception of technical 'impossibility' in 18.6(c) to 'impracticability'; – introducing an exception similar to the *Privacy Act 2020* (NZ) that provides an access request may be refused where personal information is not held in a way that enables the information to be 'readily retrieved'; and – clarifying that the proposed exception in 18.6(b) for legal relationships covers when the exercise of rights would interfere with legal processes (which appears to be suggested in the Report) and extends to potential claims and litigation, noting the various statutes of limitations which may allow an individual to make a claim and commence proceedings sometime after an event.
Response			
18.7	Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.	Position reserved	
18.8	An APP entity must provide *reasonable assistance* to individuals to assist in the exercise of their rights under the Act.	Position reserved	
18.9	An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for	Support	

No.	Proposal	LCA Position	Comments
	the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.		
18.10	An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding. An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	Position reserved	
Automated decision making			
19.1	Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.	Support	
19.2	High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.	Support	• See discussion in submission.
19.3	Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	Support in principle	• The Law Council notes that there is likely to be significant ambiguity in what is meant by 'meaningful information' as it relates to complex algorithms. • For the proposed right to be meaningful, it will be critical to anticipate, for resourcing purposes, that the exercise of this right may result in a large number of complaints to OAIC, as Proposal 18.9 notes. • It also notes the established body of law on automated decision making in the European Union and the United Kingdom. • See discussion in submission.

No.	Proposal	LCA Position	Comments
Direct marketing, targeting and trading			
20.1	Amend the Act to introduce definitions for: (a) **Direct marketing—**capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material. (b) **Targeting—**capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class). (c) **Trading—**capture the disclosure of personal information for a benefit, service or advantage.	Support in part, in principle. Do not support including deidentified and unidentified information in the definition of 'targeting'.	'Direct marketing' *'Aims and ideals of any organisation'* • The Law Council supports the Department's view in the Report that direct marketing should extend to the promotion of the 'aims and ideals of any organisation'.[95] • Entities regulated by the Act may seek to market their brand in broader ways than merely in relation to their goods and services. Organisations may also seek to promote political, charitable or other agendas that do not relate directly to their goods or services. • On balance, the Law Council supports the proposal that the use of personal information for the purpose of the promotion or communication of these broader forms of agendas should be subject to the Act. *Potential overlap between 'direct marketing' and 'targeting'* • The summaries of the proposed definitions of 'direct marketing' and 'targeting' (in Proposal 20.1(a) and (b) respectively) indicate that there would be a significant degree of overlap between these two concepts. The Law Council that the OAIC's current guidance provides that, in an online context, *targeting* constitutes *direct marketing* where a business is 'targeting online advertising at an individual using their personal information'.[96] By way of example, this may occur where: – a visitor to a website who is logged into their user account receives specific forms of advertising on that website which has been targeted to, and based on, that individual's personal information; or – an organisation uses personal information about a customer to tailor a particular form or subject matter of advertisement that is of relevance to that individual and which is sent directly to them via email. • These examples would appear to fall within both the proposed definition of 'direct marketing' and the definition of 'targeting' in the Report.

[95] Attorney-General's Department, Privacy Act Review Report (2022), 210.
[96] OAIC, Direct marketing (Web Page, May 2019) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-governmentagencies/organisations/directmarketing#:~:text=Direct%20marketing%20involves%20the%20use,to%20promote%20goods%20or%20services>.

No.	Proposal	LCA Position	Comments

			• The Law Council understands that in other circumstances:
			  – personal information may be used only for the purpose of 'communicating marketing', which is of a generic nature, and has not been specifically targeted to a particular individual; or
			  – some marketing might be specifically targeted based on particular personal information, but is not communicated directly by an entity because it is instead communicated to an individual by another entity.
			• To ensure that the regulatory scheme operates in a clear and cohesive manner, the Law Council accordingly suggests that the Department clarify whether the intention is that some forms of marketing could fall within one, or both, of the definitions of 'direct marketing' and 'targeting'.
			• As set out below, the Law Council does not support expanding the scope of the Act to regulate 'targeting' undertaken in the context of de-identified or unidentified/anonymous information, pursuant to the proposed definition in Proposal 20.1(b). If this position is accepted, the Law Council submits that both definitions of 'direct marketing' and 'targeting' should be tied, respectively, to where personal information is used to communicate directly with an individual for marketing purposes, or where personal information is used to target advertising to an individual.
			'Communicate directly'
			• The Law Council acknowledges that the inclusion of the phrase 'communicate directly' in the proposed definition of 'direct marketing' is consistent with the explanatory memorandum for the Enhancing Privacy Protection Act 2012 and more recent OAIC guidance.
			• The Law Council also notes that the Report gives consideration to the potential repeal of APP 7, but does not make a formal proposal in relation to this.[97] The outcome of any further consideration in this respect is critical, having regard to the proposed 'directly' wording and given that APP 7.8 expressly provides that APP 7 does not apply to the extent that, among other things, the *Spam Act 2003* (Cth) (**Spam Act**) or the *Do Not Call Register Act 2006* (Cth) (**DNCR Act**) apply.
			• While the Law Council broadly supports the inclusion of 'communicate directly', it commends the recommendation in the Report that further short-term work should be undertaken to achieve alignment and

[97] Attorney-General's Department, Privacy Act Review Report (2022), 211-212.

No.	Proposal	LCA Position	Comments
			harmonisation of concepts across direct, electronic and telephone marketing under the Privacy Act, Spam Act and DNCR Act respectively.[98] This is a necessary pre-condition to making substantial amendments to APP 7, given that at present, these laws require similar steps to be undertaken by organisations but are inconsistently drafted. For example: – under the Spam Act and the DNCR Act, consent may either be express or reasonably inferred in the circumstances; – under the Privacy Act, consent must be express or implied; and – the requirements for opt-out mechanisms are expressed in different ways, and subject to different exceptions. • The Law Council understands that it is generally accepted that the sending of direct marketing to an email address or telephone/messaging account is regulated by the Spam Act and not by APP 7. However, the use of personal information for the purpose of sending direct mail is regulated by APP 7 and not the Spam Act. • The different definitions and requirements under these pieces of legislation continue to cause confusion and difficulty for both consumers and organisations. This has resulted in a fragmented approach to obtaining consents from consumers and it is often the case that consents and opt-outs for commercial electronic messages are (for the purposes of the Spam Act) dealt with separately to opt-outs for other forms of direct marketing governed by the Privacy Act. • The Law Council submits that, at a minimum, APP 7.8 will need to be retained in some form if the remainder of APP 7 is to be repealed. However, a preferable approach would be to undertake a broader reform and harmonisation of APP 7 and the Spam Act as part the imminent reform process. <u>'Targeting'</u> • The Law Council is of the view that 'targeting' should, in the context of the Act, be limited only to where that targeting involves the collection, use or disclosure of personal information for advertising or marketing purposes, noting the following: – Where targeting occurs based on unidentified or anonymous information, it is not always the case that this information relates to

[98] Ibid 212.

No.	Proposal	LCA Position	Comments
			a single individual. This information may, in certain circumstances, relate to multiple individuals who use the same IP address or device, and an entity may not know whether this is the case or not. – Requiring the option of an opt-out for the use of de-identified or anonymous information would have significant limitations. By definition, any such opt-out could not be actioned where an identified individual has made such a request, because it will not be possible to associate that individual with unidentified information held by the relevant entity. – If targeting occurs on the basis of de-identified or anonymous data, it will not be possible for an entity to determine whether the relevant individual is under 18 years of age or not. The Law Council considers that it would not be appropriate for entities to be required to collect additional age verification information in order to comply with a new obligation of this nature. – Most internet browsers have technical functionalities available which already allow users to control cookies and, in some cases, personalised advertisements.
20.2	Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.	Support in principle	• Clarity will be required in relation to how this proposal will interact with Proposal 20.3 and existing requirements for organisations, such as under the *Spam Act 2003* (Cth). • See discussion in submission.
20.3	Provide individuals with an unqualified right to opt-out of receiving targeted advertising.	Support in principle	• Clarity will be required in relation to how this proposal will interact with Proposal 20.2 and whether it is intended to impose new procedures for organisations. • See discussion in submission.
20.4	Introduce a requirement that an individual's consent must be obtained to trade their personal information.	Position reserved	

No.	Proposal	LCA Position	Comments
20.5	Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.	Support in principle	
20.6	Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.	Support in principle	• There will be a great deal of subjectivity and uncertainty involved for entities in assessing what is in the 'best interests' of persons under 18. This will partly depend on the age of the individuals and the nature of the relevant products. • Clear guidance will be needed as to the interpretation of what is 'in the best interests of the child' to assist organisations and legal advisors as to what this means in practice. • There is good guidance domestically, via the eSafety Commissioner, and from other jurisdictions, as to age-appropriate design and marketing.[99] • The Law Council queries whether 18 is an appropriate age level for this proposal, given Proposal 16.2 proposes that an entity may assume that an individual over the age of 15 has capacity (unless there is something to suggest otherwise).
20.7	Prohibit trading in the personal information of children.	Position reserved	
20.8	Amend the Act to introduce the following requirements: (a) Targeting individuals should be fair and reasonable in the circumstances. (b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.	Position reserved	The Law Council has several concerns about how this would work in practice: • Requiring that targeting may only occur if it is fair and reasonable, and prohibiting targeting based on sensitive information, could only apply where the information used to 'target' is personal information. – In the case of de-identified or anonymous information, it would not—as a matter of definition—be possible for entities to determine whether the relevant information was in fact the individual's sensitive information, or was instead of a more general nature. – For example, the fact that an anonymous individual visits a particular website page would not, in any way, mean that the content of that internet page is health information about that individual.

[99] Attorney-General's Department, Privacy Act Review Report (2022) 152.

No.	Proposal	LCA Position	Comments
			– Similarly, it would be extremely difficult for entities to make an assessment of what is fair and reasonable when the information used for targeting is in anonymous form. • There should also be consideration of whether Proposal 20.8 would, together with the broad definition of 'targeting' at Proposal 20.1(b), prevent or limit legitimate practices of providing additional or tailored services to people with protected attributes. For example, accessibility options to individuals with a disability or developing new technology protects that provide tailored treatment plans for patients with medical conditions. • The proposed exception for 'socially beneficial content' would need to be sufficiently broad so that it does not stifle new and innovative business activity that is beneficial to individuals. The Law Council also notes in this regard that the assessment of what constitutes a benefit to society at large may be different to a benefit to a particular individual.
20.9	Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	Support	• The Law Council welcomes further consultation in respect of this proposal. • A number of considerations will need to be balanced in relation to this, including that information about an entity's targeting practices and/or their algorithms may include commercially sensitive information and/or may be dependent on confidential arrangements with third parties. • The Law Council notes that an exemption for providing information that is commercially sensitive or confidential would be consistent with existing provisions of the Privacy Act[100] and under the GDPR.
Security, retention and destruction			
21.1	Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.	Support	• This is a useful clarification.
21.2	Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023–2030 Australian Cyber Security Strategy.	Support	• The Law Council is of the view that this proposal is very important, given overarching security-related laws. • This needs greater prominence and alignment, noting overlap with obligations on organisations and their directors and officers, information sharing between organisations and public and private sectors and the move to civil penalties.

[100] Under APP 12.3(j), an APP entity can refuse to give an individual access to personal information when it would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

No.	Proposal	LCA Position	Comments
21.3	Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.	Position reserved	• The Law Council reiterates the need for objective and independent guidance and opinions, as discussed above in the submission.
21.4	Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.	Position reserved	
21.5	The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.	Position reserved	
21.6	The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial. However, this review should not duplicate the recent independent review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979* and the independent reviews and holistic reform of electronic surveillance legislative powers.	Support	• The Law Council strongly supports this proposal, noting how many matters go the ability to delete/de-identify and the need to balance this with the legal requirements to keep/retain (e.g., ID verification, anti-money laundering obligations, tax etc.). • It is recommended that the review include consideration of whether all records collected by the Commonwealth should legitimately be the subject of an exception to the privacy principles, including a right to erasure, as currently proposed.
21.7	Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational	Position reserved	• The Law Council notes that this proposal will be very hard to implement. • It recommends that industry-specific initiatives be considered, noting the role of guidance and opinions on best or acceptable practices.

No.	Proposal	LCA Position	Comments
	needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.		
21.8	Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.	Position reserved	
Controllers and processors of personal information			
22.1	Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.	Do not support	• The Law Council considers this proposal can be addressed by dealing with the small business exemption. It has previously expressed that it does not support importing new definitions of controllers and processors into the Act as it unnecessary, because:[101] – where Australian APP entities are also controllers as defined under the GDPR, the matter is addressed under the GDPR and is the subject of relevant guidance to that effect; – where an APP entity 'holds' personal information (as defined under the Act) and are within the scope of the Act, their obligations are described by reference to being in possession or control of the personal information; – introduction of new definitions of controllers and processors would otherwise interfere with contractual arrangements and descriptions of responsibilities and rights of the parties without a corresponding privacy benefit to individuals.

[101] See Law Council of Australia, Privacy Act Review: Discussion Paper (Submission, 27 January 2022) <https://lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf> 22.

No.	Proposal	LCA Position	Comments
Overseas data flows			
23.1	Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.	Support	• The Law Council supports establishing an 'Australian link'.[102] • See discussion in submission.
23.2	Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).	Support	• This proposal would provide necessary clarity for Australians (individuals and businesses of all sizes) regarding the adequacy of ex-Australian privacy laws to which Australian-sourced personal information will be subject.
23.3	Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.	Support	• The Law Council regards this proposal as a significant privacy-positive step for compliance purposes. • The Law Council supports the suggestion that the standard clauses be drafted in a way which is aligned, as far as possible, with the standard clauses which have been promulgated elsewhere.
23.4	Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.	Do not support	• The Law Council is of the view that consent is generally not an appropriate basis for transfers. • If other lawful bases of transfers are sufficiently addressed, then a statutory exemption of this kind would not need to be proposed.
23.5	Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.	Support in principle	• The Law Council notes that this proposal may potentially have a high operational impact, for little benefit.
23.6	Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be	Support	• The Law Council notes the reliance on public interest in this proposal and queries how that is to be determined if the objects of the Act are to be amended pursuant to Proposal 3.2.

[102] See Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission, 8 November 2022) <https://lawcouncil.asn.au/publicassets/4d6e625a-8760-ed11-9475-005056be13b5/2022%2011%2008%20-%20S%20-%20Privacy%20Legislation%20Amendment%20Bill%202022.pdf> 8-11.

No.	Proposal	LCA Position	Comments
	excluded from the requirements of APP 8 where it is in the public interest.		
CBPR and domestic certification			
No proposals.			
Enforcement			
25.1	Create tiers of civil penalty provisions to allow for better targeted regulatory responses: (a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision. (b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.	Support in part	• The Law Council supports Proposal 25.1(a) but does not support Proposal 25.1(b). • See discussion in submission.
25.2	Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature (b) those adversely affecting large groups of individuals (c) those impacting people experiencing vulnerability (d) repeated breaches (e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data. The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.	Support	• The Law Council notes the need to consider how this will be applied, also noting the role of the OAIC.

No.	Proposal	LCA Position	Comments
25.3	Amend the Act to apply the powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.	Position reserved	• In relation to the impact of obligations on directors and officers, the Law Council notes section 92 of the *Regulatory Powers (Standard Provisions Act) 2014* (Cth)—Ancillary contravention of civil penalty provisions.
25.4	Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.	Position reserved	
25.5	Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: *a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.* The OAIC should publish guidance on how entities could achieve this.	Position reserved	
25.6	Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.	Position reserved	• The Law Council notes that this proposal is very broad and considers the need to consider threshold issues.
25.7	Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.	Support in principle	• This proposal aligns with the Law Council's support for proper resourcing for the OAIC and suggests testing if this is the best funding model. • This will require a degree of independence and appropriate oversight. • The Law Council further queries how the effectiveness of this funding model would be assessed.

No.	Proposal	LCA Position	Comments
25.8	Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.	Position reserved	
25.9	Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Support	• The Law Council considers that this proposal will aid transparency.
25.10	The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Support	• The Law Council recommends considering a separate body under the Act to provide opinions on matters of interpretation and guidance similar to the European Data Protection Board but aligned to the Australian structures, legal system and means of enforcement. • The Law Council also suggests considering updating the structure and role of the Privacy Advisory Committee.[103]
25.11	Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.	Support	• The Law Council considers that this proposal will avoid duplication.
A direct right of action			
26.1	Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.	Support in principle	• See discussion in submission.
A statutory tort for serious invasions of privacy			
27.1	Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.	Support in principle	The Law Council has received in-principle support from the Law Institute of Victoria, the Victorian Bar and its Business Law Section's Privacy Law Committee for the introduction of a statutory tort, provided there are sufficiently

[103] ALRC, For Your Information: Australian Privacy Law and Practice (Report 108, Volume 1, August 2009) <https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf> Chapter 46.

No.	Proposal	LCA Position	Comments
	Consult with the states and territories on implementation to ensure a consistent national approach.		high thresholds in place to ensure actions are limited to serious invasions of privacy. However, the Business Law Section's Media and Communications Committee has provided the following reasons for not supporting Proposal 27.1, instead favouring increased resourcing being provided to the OAIC to assist in enforcement: • Combined with the direct right of action, this will place significant strain on the court system and have a significant adverse impact on press freedoms and freedom of expression in Australia. This is of particular concern, given that Australia lacks the broad statutory and constitutional protections for freedom of expression that other jurisdictions such as the UK, the United States and Canada have enshrined. • There is arguably no 'gap' in legal protections to be filled by a statutory tort, given the following legal protections already exist which go well beyond the Act's remit: – existing defamation laws; – common law causes of action, including breach of confidence, trespass, nuisance and malicious falsehood; – suppression orders in court proceedings; – the *Online Safety Act 2021* (Cth), Spam Act and the DNCR Act; – State and Territory privacy legislation that imposes obligations on public authorities and, often, health service providers; – other privacy related federal legislation, including the *My Health Records Act 2012* (Cth), the *Healthcare Identifiers Act* 2010 (Cth), the Commonwealth Spent Conviction Scheme and the *Data-matching Program (Assistance and Tax) Act 1990* (Cth); – the *Telecommunications (Interception and Access) Act 1979* (Cth) and *Telecommunications Act 1997* (Cth), as well as surveillance laws at a State and Territory level; – criminal laws at a Commonwealth, State and Territory level which prohibit a range of privacy intrusive crimes; and – laws at a Commonwealth, State and Territory level prohibiting identification of certain classes of persons. • In the case of media organisations, complaints may be made, and redress sought, through existing mechanisms.

No.	Proposal	LCA Position	Comments
			• There is no evidence provided in the Report that the current OAIC conciliation and early resolution processes are not providing individuals with adequate remedies. • From a consumer perspective, a well-resourced regulator will provide more effective and timely compensation than a potentially lengthy and costly court process. • It is likely that the experience of the UK, which has seen significant misuse of similar direct rights, and a consequent impact on the ability of media companies to publish information that is in the public interest, will be emulated in Australia. This problem extends beyond journalism to other areas, particularly literary works. • Specifically, the use of the equivalent tort of misuse of private information in the UK, together with rights to take direct action under its data protection law has been used predominantly by wealthy individuals to stifle debate.
Notifiable data breaches scheme			
28.1	Undertake further work to better facilitate the reporting processes for NDBs to assist both the OAIC and entities with multiple reporting obligations.	Support	The Law Council notes the following observations and suggestions from its membership in respect of the NDB scheme, which the current review process offers an opportunity to address. <u>Voluntary notification</u> • The Law Council understands that at present, many APP entities are notifying the OAIC of data breaches out of an abundance of caution as soon as a data breach has become apparent and prior to seeking legal advice, regardless of whether the data breach is 'likely to result in serious harm'. • By notifying the OAIC, APP entities are then exposed to significant extended enquiries by the OAIC, leading to administrative compliance over and above the costs and resources dedicated to attending to the data breach and, say, implementing new software and security, undertaking assessments and audits, and reinstating systems. • Prior to the implementation of the NDB scheme, many APP entities made voluntary notifications. With the benefit of the NDB scheme being in operation for over four years, the Law Council recommends re-consideration be given to amending the NDB scheme to facilitate an outcome whereby an APP entity may notify the OAIC on a voluntary or preliminary basis, and then within an appropriate time period (reflective of
28.2	(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the	Position reserved	

No.	Proposal	LCA Position	Comments
	same time, the information may be provided in phases as soon as practicable. (c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.		how most matters require a sense of urgency and promptness), communicating with the OAIC whether the APP entity considers that data breach to be one that is 'likely to result in serious harm'. • A more informal, yet prompt, means of communication would provide an opportunity for transparency and collaboration, including early input of various parties, when a data breach becomes known. Clarity of status of these early voluntary or preliminary reports would assist. • Noting that Proposal 6.1 recommends removing the small business exemption, it is likely that more entities will be inclined to notify the OAIC with respect to data breaches that are not objectively notifiable, which may lead to otherwise avoidable financial burdens on entities that may not be in a position to absorb such costs. • Consideration should accordingly be given to implementing a voluntary or preliminary notification scheme and articulating the status of these communications in the context of the NDB scheme. <u>The OAIC's wide interpretation of 'likely to cause serious harm'</u> • At the outset, the Law Council acknowledges that: – the current 'serious harm' threshold was developed to avoid the risk of notification fatigue to individuals and to not impose an unreasonable compliance burden on APP entities; – the threshold was devised as an objective test to flexibly suit a variety of data breaches and to avoid the complexity associated with defining every form of harm likely to result from a breach; and – the onus is on the relevant entity to assess serious harm from the perspective of a reasonable person's position in their circumstances. The entity that experienced the breach would be best placed to make such an assessment. • However, further to the above, APP entities find themselves in a potentially ambiguous position once they have voluntarily notified the OAIC of a data breach, then consider that the data breach is one that is not 'likely to result in serious harm'. The Law Council understands from its Business Law Section's Privacy Law Committee that, in practice, the OAIC often applies a wide interpretation of 'likely to cause serious harm'.

No.	Proposal	LCA Position	Comments
			• While not proposed in the Report, the Law Council recommends consideration be given to amending section 26WG of the Act to have specific regard to: – the likelihood that persons have accessed personal information, including the length of time of that access; – whether any personal information was exfiltrated and, if so, the amount of personal information that was exfiltrated relative to the amount held; and – whether any personal information entered the public domain as a result of the data breach (noting overlap with other remedies, if any). • Alternatively, the OAIC should develop guidance to address the matters immediately above. <u>APP entities that are service providers</u> • The Law Council acknowledges the practical reality that many data breaches involve APP entities that supply services to another entity that has a direct relationship with individuals. • In this instance, even if the APP entity subsequently considers the breach as not 'likely to result in serious harm', the OAIC, in the event it becomes aware of the data breach, will then contact other entities and make detailed enquiries of them, especially regarding whether potentially affected individuals have been notified of the data breach. • The additional powers afforded to the OAIC with the recent implementation of section 26WU of the Act provides greater scope for the OAIC to make enquiries of entities that did not report a data breach, and who may consider that the data breach that was suffered by their service provider was not notifiable, as it was not 'likely to result in serious harm'. Regardless, the OAIC is in a position to compel the production of documents in circumstances where, objectively, the data breach was not 'likely to result in serious harm'. • One of the related complications that has developed with the NDB scheme and the ability for APP entities to comply with the scheme is where the data breach impacts an APP Entity that is a service provider to another entity, where that entity is not an APP Entity. For example, that entity may be a state government department or agency, or an entity falling below the $3

No.	Proposal	LCA Position	Comments
			million threshold (noting New South Wales has recently adopted a notification scheme). • Whilst an APP entity-service provider may be in possession of some personal information, it may not be in possession of personal information constituting contact information for an individual. The Law Council also notes the OAIC's guidance that the party with the direct relationship should be responsible for notifying potentially affected individuals. • As a result, the APP entity may not be able to contact potentially affected individuals of which it has no direct relationship. The APP entity then has to ask the respective government department or non-APP entity to contact their users/clients/customers to notify them of the data breach. However: – many state government departments and agencies do not contact potentially affected individuals, as the Act does not apply to them; and – many non-APP entities do not have the resources to contact potentially affected individuals. Again, the Act does not apply to them. Further, many non-APP entities consider contacting their customers as a 'threat' to their brand or reputation and the trust that they have developed with their customers. • The above examples become even more complicated when there is a genuine debate between the relevant parties, or between the parties and the OAIC, regarding whether the data breach falls within the NDB Scheme. • The Law Council recommends that the OAIC develop guidance with respect to the above circumstances and what the APP entity may be expected to do with respect to contacting potentially affected individuals with whom it does not have a direct relationship.
28.3	Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates. However, this proposal would not require the entity to reveal personal information, or where the harm in	Position reserved	• The Law Council considers that entities should be required to take reasonable steps to prevent or reduce harm that is likely to arise for individuals as a result of a data breach. • Such a requirement would be consistent with the United Nations Guiding Principles on Business and Human Rights, and the OECD Guidelines on Multinational Enterprises, to which the Australian Government has committed.

No.	Proposal	LCA Position	Comments
	providing this information would outweigh the benefit in providing this information. Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.		
28.4	Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	Position reserved	
Interactions with other schemes			
29.1	The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.	Position reserved	
29.2	Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.	Position reserved	
29.3	Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.	Position reserved	
Further review			
30.1	Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.	Position reserved	