Law Council
OF AUSTRALIA

Privacy Act Review: Discussion Paper

Attorney-General's Department

27 January 2022

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

Table of Contents

About the Law Council of Australia **3**
Acknowledgement **4**
Executive summary **5**
General comments **6**
Part 1: Scope and application of the Privacy Act **6**
Objects of the Privacy Act 6
Personal information 7
De-identified, anonymised and pseudonymised information 7
Flexibility of APPs 8
Emergency declarations 8
Exemptions 8
Small business exemption 8
Employee records exemption 9
Journalism exemption 10
Political exemption 11
Part 2: Protections **11**
Standardisation 11
Privacy Notices 11
Consents 12
Standard Contract Clauses for Overseas Disclosures 13
When an APP 5 collection notice is required 13
Restricted and Prohibited Practices 14
Children and vulnerable individuals 15
Right to erasure 15
Behavioural marketing 16
Automated Decision-Making 16
Security and destruction of personal information 17
Privacy by Design 17
Overseas data flows 18
Part 3: Regulation and enforcement **19**
Enforcement 19
Direct Right of Action 20
Statutory Tort of Privacy 20
Notifiable Data Breach Scheme 21
Definitions 22
Interactions with other schemes 22

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote 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 16 Australian State and Territory law societies and bar associations and Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

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

Through this representation, the Law Council effectively acts on behalf of more than 90,000[1] lawyers across Australia.

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 the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2022 Executive as at 1 January 2022 are:

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

The Chief Executive Officer of the Law Council is Mr Michael Tidball. The Secretariat serves the Law Council nationally and is based in Canberra.

1 Law Council of Australia, *The Lawyer Project Report*, (pg. 9,10, September 2021).

Acknowledgement

The Law Council appreciates input received from the following of its Constituent Bodies in relation to this submission:

- the Law Society of New South Wales;
- the Queensland Law Society;
- the Law Institute of Victoria;
- the Law Society of South Australia; and
- the New South Wales Bar Association.

The Law Council also appreciate the contribution of the Business Law Section's Privacy Law Committee, and Media and Communications Committee in the preparation of this submission.

Executive summary

1. The Law Council commends the Attorney-General's Department on the long-term consultation process regarding the review of the *Privacy Act 1988* (Cth) (**Privacy Act**). The comprehensive Discussion Paper considers the submissions made in the first round of consultation in detail and has continued to refine the proposals to balance the best interests of individuals and organisations in relation to privacy.

2. The Privacy Act has now been in operation for over 30 years and the *Privacy Amendment (Private Sector) Act 2000* (Cth) was introduced some 20 years ago, extending privacy obligations to the private sector to provide a minimum set of privacy protections for individuals. During this time there have been significant changes to the landscape in which these pieces of legislation operate and therefore the Law Council welcomes the current review of the legislative framework.

3. While the Law Council has not had the opportunity to respond to all of the proposals set out in the Discussion Paper in the time provided, this submission addresses the following key matters set out in the consultation process:

    - support for updating and clarifying the definition of 'personal information' under the Privacy Act, including a reconsideration of the definition of personal information with a view to clarifying the uncertainty regarding technical data;
    - recognised opportunities to implement standardisation with respect to complying with particular requirements of the Privacy Act and Australian Privacy Principles (**APP**), particularly in relation to Privacy Notices, Consents, and Standard Contract Clauses for overseas disclosures;
    - in-principle support for the proposal set out in the Discussion Paper to create tiers of civil penalty provisions to provide the Office of the Australian Information Commissioner (**OAIC**) with more options to better target regulatory responses, noting that it is critical that the OAIC be appropriately resourced to apply to the courts for civil penalties for serious or repeated interferences with privacy and to further its enforcement activities;
    - a need to clarify (and in some cases reconsider) existing exemptions under the Privacy Act, including in relation to small businesses, employee records and journalism;
    - reflections on the proposal to create a private right of action under the Privacy Act's data protection regime, noting that any such step will require careful consideration of the drafting to ensure that there are no unintended consequences and all causes of action as updated by the reform process can be considered in context;
    - support for the development of a statutory tort of serious invasion of privacy, on the condition that there are sufficiently high thresholds in place to ensure actions are limited to serious invasions of privacy and that the scope of the statutory tort is carefully considered and drafted to address the risk of unintended consequences; and
    - support for the creation of a Commonwealth, state and territory working group to harmonise privacy laws and focus on key privacy issues.

4. In relation to the final point above, and in the context of other current reforms impacting on Australian privacy law, it is critical that there be a concerted effort to avoid fragmentation in the reform process in order to reduce the likelihood of uncertainty and unintended consequences for those subject to the Australian privacy framework.

General comments

5. The world has transformed considerably since the Privacy Act's inception with the advent of the internet facilitating a proliferation of data and information. Social media, new banking and payment methods, and a shift to move business to online formats (including legal transactions such as conveyances, and anti-fraud measures) have substantially altered the way in which we use, treat and generate information. The amount of personal information (much of which will be considered sensitive) being transferred with little to no oversight has expanded exponentially, and the Law Council is of the view that the Privacy Act can be modified to better safeguard against misuse, mistake, or malfeasance. The implications for an individual in the event of a privacy breach can be significant, and permanent.

6. With this context in mind, the Law Council considers that the Privacy Act can be enhanced to better equip entities, regulators, and individuals to deal with emerging technologies and new methods (and speed) of generating and transferring information. The current review is an ideal time to address these areas for improvement.

7. The Law Council recognises that privacy concerns are a focus of several concurrent consultations, including the Department of Home Affairs' consultation on Strengthening Australia's Cyber Security Regulations and Incentives and the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (**Online Privacy Bill**). While these consultations focus on different aspects of privacy in the Australian context, the Law Council is of the view that a complementary and holistic approach is important for improving transparency for consumers and regulatory consistency for organisations.

8. Further, the Law Council notes that many of the legal issues raised are highly definitional and warrant careful analysis of the draft legislation to ensure that policy objectives and community expectations are met by the law. Adequate time will be needed to review the exposure draft legislation by civil society, regulators and other interested parties and stakeholders.

Part 1: Scope and application of the Privacy Act

Objects of the Privacy Act

9. The Law Council notes that the objects do not form part of the operative provisions of the Privacy Act. However, the Law Council is broadly supportive of Proposal 1.1 in the Discussion Paper, which suggests amending subsections 2A(a) and (b) of the Privacy Act to focus on the protection of privacy of individuals with regard to their personal information and recognises that the protection of privacy must be balanced with the protection of other public interests.

10. As a general principle, data protection regulation should enable a balance between an individual's right to control their private information and the general public's commercial interest in data 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.

11. 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. The Law Council also suggests that a

further objective be included of providing enforceable rights for individuals to seek redress for an interference with their privacy, in addition to any complaints process. This would be subject to the inclusion of a direct cause of action, as commented on below.

Personal information

12. The Law Council considers that the definition of 'personal information' should be broad enough to encompass an 'identified individual' and 'individuals who are reasonably identifiable' and remain technology neutral. The Law Council supports a reconsideration of the definition of personal information to clarify the uncertainty regarding technical data, in line with recommendations arising out of the Australian Competition and Consumer Commission's (**ACCC**) Digital Platforms Inquiry.[2]

13. The Law Council is therefore supportive of the definition of personal information contained at proposals 2.1 to 2.3 of the Discussion Paper to explicitly include technical information (including metadata) that can be linked to an individual, or from which an individual's identity can be constructed by reference to unique patterns of online behaviour. In providing this support, the Law Council is of the view that any such definition should aim for consistency with the approach adopted by the (European) General Data Protection Regulation (**GDPR**), which is sufficiently broad such that it should capture most technical information of potential concern, allowing for flexibility moving forward and for greater interoperability between international privacy regimes.

14. The Law Council also welcomes the proposal that any new definition should replace the reference to 'about' to 'relates to' and supports the inclusion of a non-exhaustive list of specific examples of the types of technical information that might be captured. Despite this, the Law Council notes that the examples of technical information currently set out in the Discussion Paper are still described in quite broad terms (e.g. 'online identifier' and 'location data'). To avoid any ambiguity or uncertainty, it is suggested that these examples should either be expanded upon in the Privacy Act itself, or that any supplementary guidance published in respect of the definition should provide greater specificity. The Law Council's preference is to do so as guidance, as this would preserve the technological neutrality of the Privacy Act.

De-identified, anonymised and pseudonymised information

15. The Law Council cautions against an approach within the Privacy Act to require de-identification to remove the risk of re-identification of any individual entirely. Rather, an assessment of whether an individual is identifiable should be made based on whether, in the circumstances, the risk of re-identification that may cause harm to an individual can be reasonably assessed as very low. This is addressed by a solid and clear definition of what is personal information which, if implemented, would assist in addressing this issue.

16. Consistently with proposal 2.5 in the Discussion Paper, the Law Council suggests that the Privacy Act could be amended to require information to be 'anonymous' rather than 'de-identified' in order for the Privacy Act to no longer apply, together with the inclusion of a new definition of anonymous information. Consistent with the Discussion Paper, information would be considered 'anonymous' if it were no longer possible to identify someone from the information. To the extent this occurs, the Law Council considers that supplementary guidance would be necessary to help APP entities (particularly those that might be less sophisticated) understand the distinction between

[2] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, July 2019) rec 16(a)

anonymisation and de-identification, and the practical steps that the APP entity would be required to undertake to truly and effectively anonymise personal information.

Flexibility of APPs

Emergency declarations

17. The Law Council provides in-principle support for the Discussion Paper's proposal 3.4 that the Privacy Act be amended to permit organisations to disclose personal information to appropriate state and territory authorities when an Emergency Declaration is in force. In terms of additional safeguards that could be implemented to protect the personal information disclosed in those circumstances, ideally, an organisation would advise a person that their personal information might be disclosed to a state/territory authority at the point that it is collected and obtain their consent to that type of disclosure.

18. Other requirements might include that an organisation or recipient should only use the information disclosed whilst an Emergency Declaration is in force for the purpose for which it was disclosed (i.e. a 'permitted purpose' as provided for in section 80H of the Privacy Act), and/or only disclose the personal information in circumstances where it is reasonably satisfied that the state/territory authority requires the information to respond to the emergency, that it will only be used for that purpose, that the personal information can be stored securely, and that it is in the public interest that the personal information be disclosed. Consideration should also be given to ensuring personal information during times of emergency are appropriately destroyed when no longer required by the authority.

Exemptions

19. The Law Council supports the prior recommendation of the OAIC that exemptions from the Privacy Act should be minimised or removed in order to achieve uniformity and consistency of application of privacy legislation, and that a clear public interest for any exemptions should exist to support their creation or continuation.[3]

Small business exemption

20. In its current form, the Privacy Act provides an exemption for agencies and organisations with an annual turnover of less than $3 million, although these entities may be bound by the APPs in certain circumstances.[4] Small businesses and not-for-profit organisations that would otherwise not be covered by the Privacy Act may choose to be treated as an organisation for the purposes of the Act, by publicly committing to good privacy practices and adhering to the APPs.[5]

21. Where handling of personal information is a core business activity, the carve-in from the small business exemption will generally mean that the Privacy Act already operates – such as for businesses sharing such data for commercial purposes as a business activity. In most cases, businesses do not pay or otherwise give an individual any benefit for collection or use of their personal information. Without any obligations being imposed on small businesses, individuals may in some cases be at both a significant disadvantage commercially (it is well established that personal information is a valuable

[3] Office of the Australian Privacy Commissioner, Submission PR 215 (28 February 2007) cited in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, August 2008) [33.41]
[4] *Privacy Act 1988* (Cth) ss 6C, 6D.
[5] See, Office of the Australian Privacy Commissioner, 'Privacy Opt-in Register' <www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register>.

revenue-generating commodity when leveraged), and are subject to their personal information being exposed without protection. The benefits that businesses gain from collection and handling of personal information may mean that the burden of compliance with the Privacy Act is a reasonable cost of doing business responsibly and fairly – at least for larger businesses with the resources, technology and practices available to support those burdens.

22. 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 data from such larger small businesses and employee records have merged into the same risks that exist for storage of personal information collected for business reasons. 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.

23. Some stakeholders have queried whether the small business exemption in its current form strikes the right balance between protecting the privacy rights of individuals and avoiding imposing onerous obligations on smaller enterprises. While the Privacy Act has now been in place for many years and its requirements are generally understood by many medium and larger businesses, the same cannot necessarily be said for the majority of smaller/micro businesses. It is acknowledged, as the Australian Law Reform Commission (**ALRC**) has stated, that simply removing the small business exemption would increase compliance costs for small businesses, and that, options other than simply removing the exemption are available.[6]

24. Any tightening of the exceptions for small businesses must also be accompanied with consultation of the sector to achieve a workable and appropriate means to balance individual rights and small business operating costs. If any changes are to be made to the exemption for small business, recognising that new compliance requirements may be an impost on business, it would be worth considering a transition period and ensuring that those amendments are accompanied by Government-issued guidance, training and other assistance to support small business compliance. These would need to be considered in the context of the reformed legislation and the drafting of any pending amendments.

25. If the small business exemption were to remain in place, the Law Council suggests that consideration should be given to including within the exceptions to the exemption those businesses that routinely collect and handle an individual's identity documents due to a legal requirement or general business practice in the relevant industry. A further option which the Law Council considers to have merit is to consider the suggestion from the ALRC to introduce an accreditation scheme to encourage small businesses to 'opt in' under section 6EA of the Privacy Act.[7]

Employee records exemption

26. The Privacy Act, together with guidelines provided by the OAIC, suggest that employers can lawfully store employee data without breaching the Privacy Act, if the data relates

[6] Australian Law Reform Commission, *Review of the Small Business Exemption* (15 July 2014) [16.55] <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/16-new-regulatory-mechanisms/review-of-the-small-business-exemption/>.
[7] Ibid, [16.56].

to their employment.[8] However, this has been cast into doubt by the decision of the Fair Work Commission in *Jeremy Lee v Superior Wood,*[9] which decided that requiring an employee to consent to biometric attendance scanning was not a lawful direction, as it infringed the employee's rights under the Privacy Act. The effect of this decision is that the exemption relating to employee records only applies to data already held by the employer and does not encompass records that are 'yet to be held by an organisation'.[10] The decision that the employment exemption does not apply until the information is collected, subjects only the collection process to the Privacy Act, which is a significant departure from the way privacy practitioners apply these exemptions.

27. The utility of the employee records exemption in Australia has been challenged since its introduction,[11] with similar concerns over employee records being one of the most sensitive categories of personal information maintained. Further, the employee records exemption fails to provide the required clarity to employers seeking to comply with their respective compliance obligations and employees seeking to have certainty as to their privacy rights in the workplace. The exemption is of itself not comprehensive and remains difficult to apply as a matter of practice.

28. Given the range of personal information that employees may provide to their employees, the Law Council supports the conclusion of the Standing Committee on Legal and Social Affairs that they should be entitled to expect that the necessary confidentiality of this information is ensured.[12] The Law Council suggests that these entities ought to be subject to the same privacy obligations as APP entities and should not benefit from the exemptions under the Privacy Act. As noted above in relation to the small business exception, appropriate defences can be created that reflect the considerations pertinent to the employment relationship and align to the existing workplace legislation.

Journalism exemption

29. The Law Council appreciates that assertion of legitimate expectations of individuals to personal privacy should not be allowed to automatically block fair and vigorous reporting and free speech enjoyed in an open democracy. In this regard, the Media and Communications Committee of the Law Council's Business Law Section notes that the retention of the journalism exemption provides a necessary pre-requisite for the provision of public interest journalism, and that a robust media and journalism sector is vital to the maintenance of a healthy democracy as it promotes the free flow of reliable information to the Australian public.

30. The Law Council notes the response of the OAIC to the current Discussion Paper, in which it is suggested that the journalism exemption be amended to confine it to journalism that is, on balance, in the public interest, as recognised in existing journalism privacy standards. While the Law Council does not yet have a settled view on this proposal, it remains supportive of steps to clarify and provide certainty to the balancing of public interest journalism and legitimate expectations of privacy of individuals.

---

[8] Office of the Australian Information Commissioner, '*Employee Records Exemption'* (December 2015) <https://www.oaic.gov.au/privacy/privacy-for-organisations/employeerecords-exemption/>; see also Fair Work Legal Advice, '*Fingerprints in the Workplace'* (9 October 2019) <https://fairworklegaladvice.com.au/fingerprints-in-the-workplace/>.
[9] (2019) FWCFB 2946.
[10] *Privacy Act 1988* (Cth) s 7B; *Jeremy Lee v Superior Wood* (2019) FWCFB 2946 [54].
[11] Standing Committee on Legal and Constitutional Affairs, *'Advisory Report on the Privacy Amendment (Private Sector) Bill 2000'* (Report, June 2000) [3.22] <https://www.aph.gov.au/parliamentary_business/committees/House_of_Representatives_Committees?url=/laca/privacybill/contents.htm >; Victorian Government, Department of State and Regional Development (Submission) 199.
[12] Ibid [3.33].

31. It is noted, however, that the Discussion Paper does not appear to point to evidence that the journalism exemption does not currently operate effectively in its current form. If any such evidence were to emerge, that evidence would need to be considered in detail, together with the question of whether that evidence warranted a change to the journalism exemption.

Political exemption

32. The Law Council considers that the political exemption should be removed from the Act. The exemption is not necessary to protect the freedom of political expression in Australia as that freedom is already protected by Australia's defamation laws, and whilst there are ultimately other means (which do not require the collection of individuals' personal information) by which political parties/politicians can communicate their views/agenda.

33. The Law Council anticipates that resources of most political parties would be such that it would not be an unfair administrative burden for those parties to implement internal frameworks/ infrastructure to ensure compliance with the relevant APPs. To assist in any transition away from the exemption, Government-issued guidance, training and other assistance to support compliance should be developed for political entities.

Part 2: Protections

Standardisation

34. The Law Council recognises that there are opportunities to implement standardisation with respect to complying with particular requirements of the Privacy Act and APPs. This includes with respect to:

    - Privacy Notices;
    - Consents; and
    - Standard Contract Clauses for overseas disclosures.

35. At first instance, Privacy Notices and Consents could be standardised with respect to those APP entities subject to the proposed Online Privacy Bill.[13] In due course, standardisation could be expanded sector by sector, much in the same way as has been proposed with Consumer Data Right standards.[14]

36. The Law Council would be pleased to assist with the drafting of relevant provisions if the Attorney-General's Department proposes to implement standardisation with respect to development of the content of standard Privacy Notices, Consents and Standard Contract Clauses for overseas disclosures.

Privacy Notices

37. The Law Council notes the recommendations made by the ACCC in its Digital Platforms Inquiry that all collections should be accompanied by notice (unless the individual already has the information or there is an overriding legal or public interest reason), that notices should be concise, transparent and written in clear and plain language and,

[13] The draft Online privacy Bill proposes to apply to the following categories of private sector organisation that are already subject to the Privacy Act: (i) organisations that provide social media services; (ii) organisations that provide data brokerage services; and (iii) large online platforms.
[14] See, <https://consumerdatastandards.gov.au/standards/>.

where possible, that any associated information burden could be reduced through the use of standardised icons or phrases.[15]

38. The Law Council supports the introduction of an express requirement in APP 5 that Privacy Notices must be clear, current, and understandable. Standardisation of privacy notices is an effective way for consumers to engage with, and digest large amounts of information regarding privacy law (thus minimising information fatigue) and would increase transparency and improve comprehension of privacy notices in the community. The use of standardised layouts, wording and icons is particularly useful in increasing consumer confidence and familiarity with complex privacy laws and exercising the individual's choices regarding how their personal data is used.

39. As mentioned in the Discussion Paper's proposal 13.2, standardised privacy notices could also be adapted for information specifically addressed to children, through tailored language and the inclusion of practical examples that children are more likely to understand.

40. Standardised privacy notices should also be accessible to ensure supported decision making for individuals that require simple and easy to read information for key messages. Easy Read Guides will ensure individuals from culturally and linguistically diverse backgrounds (**CALD**), and those living with disabilities which impact their ability to read and understand documents such as privacy notices, are able to better understand key privacy decisions as well. Regular feedback and input from vulnerable groups will be crucial to ensure the privacy notices are serving their intended purpose for individuals.

41. Generally, most Privacy Notices incorporate standard categories. As part of the Discussion Paper's consideration of this issue, particular attention has been drawn to the Online Privacy Code (**OP Code**) and how it may be useful with respect to Privacy Collection Notices issued by APP entities regulated by the OP Code. At first instance, consideration could be given to implementing a standard format/layout for a Privacy Collection Notice with respect to entities subject of the OP Code.

42. Clause 90 of the *Competition and Consumer Regulations 2010 (Cth)* (**Regulation 90**) prescribes standard language with respect to warranties against defects. With the introduction of the Australian Consumer Law, Regulation 90 was initially, peculiarly, limited to goods only and did not refer to services. Subsequently, Regulation 90 was amended to incorporate a reference to services. A similar approach could be adopted with respect to Privacy Collection Notices. In due course, if the standard format/layout proves useful, consideration could be given to extending its application to particular sectors (e.g. banking, insurance). At each instance of expansion, there would be an opportunity for further refinement of the standard format layout following stakeholder consultation.

Consents

43. The Law Council notes that the development of standardised consent taxonomies has already commenced in the context of Consumer Data Right standards. Currently, these apply to the banking industry.

44. Given that the foundation has already been created, again, at first instance, the OP Code could replicate the approach adopted by the Consumer Data Right. Similar standards could be prescribed as to how an entity, which is subject to the OP Code, is

[15] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, July 2019) rec 16(b).

to comply with the requirements in order to obtain consent for the collection, use and disclosure of personal information.

45. The Law Council would be pleased to assist with the development of these standardised consent taxonomies if there is a willingness to implement such a regime.

Standard Contract Clauses for Overseas Disclosures

46. The Law Council notes that the New Zealand Office of the Privacy Commissioner has published model contract clauses (**SCCs**) with respect to its Information Privacy Principle (**IPP**) 12 relating to cross-border privacy transfers.[16]

47. With respect to the transfer of personal information to recipients located overseas, consideration could be given to introducing SCCs, modelled on the New Zealand approach appearing in Appendix 2 of IPP 12 Model Clauses Template. These clauses could be readily adapted to incorporate language consistent with the Privacy Act. Again, the Law Council would be pleased to assist with this process.

When an APP 5 collection notice is required

48. The Discussion Paper proposes at 8.4 to raise the threshold for requiring an APP 5 collection notice – that is, to require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:

    - the individual has already been made aware of the APP 5 matters; or
    - notification would be impossible or would involve disproportionate effort.

49. The Law Council notes that this approach would remove the current qualifier that an entity take 'such steps (if any) as [are] reasonable in the circumstances'. This qualifier recognises that in some circumstances it is reasonable not to give an APP 5 collection notice, and also that there are some circumstances where omission of some of the specified content of a collection notice in APP 5 may be reasonable (permitting a short notice). The current reasonable steps qualifier allows entities to assess the type of personal information collected, the risk of harm to an individual if they do not receive an APP 5 collection notice (or some of the APP 5 information) and the practicability of giving a notice.

50. The current qualifier is an important and necessary qualifier in the context of everyday business and professional interaction. If an entity is collecting only basic business or professional contact details (such as name, title or position, business address, business phone number and business email address) and the purpose of the collection is clear from the context, then the view has been taken that it is a reasonable step not to give a collection notice. For example, if an entity is collecting personal information about the sender of an email from the sender's 'signing block' in the email and the email is sent in the ordinary course of business or professional dealings, then it is a reasonable step not to give a collection notice. Another example would be the obtaining of a company search to check due execution of a contract by that company where the search results include personal information of directors, secretaries and shareholders derived from a register maintained by the Australian Securities and Investments Commission (**ASIC**). In this case, all the information is publicly available (albeit on payment of the fee) and is being collected and used only for the purpose for which it was collected by ASIC and made available through search facilities.

[16] See, <https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/>

51. Clearly, in these cases notification would not be impossible. If the proposal were adopted, then entities would need to assess whether giving a collection notice would involve 'disproportionate effort'. The Law Council considers this test to not be a well understood legal concept and has the potential to create more issues (and less certainty) than the current (reasonable steps) test, which is an objective test about which there is judicial guidance.

52. There is little public benefit in entities spending resources considering all the contexts in which they collect basic business or professional contact details in the ordinary course of their day-to-day business and determining when giving a collection notice would or would not involve disproportionate effort. It is entirely possible that if proposal 8.4 were to be adopted, entities may set up their email systems so as to trigger an automated message containing a collection notice in response to any email communication. To do so would not involve 'disproportionate effort' on the part of the sender, but it would result in vast numbers of collection notices arriving by email in response to business and professional communications, subjecting individuals to notice fatigue, resulting in inbox limits being reached so that genuine communications are blocked and serving no public interest or benefit.

53. Further, the current qualifier permits an entity to determine not to give an APP 5 collection notice where:

    - notification may pose a serious threat to the life, health or safety of an individual;
    - notification would be inconsistent with another legal obligation, for example it would breach a legal obligation of confidence; or
    - notification may jeopardise the purpose of the collection – this might be the case in the context of an investigation by an entity, or by an enforcement agency, of suspected illegal conduct.

54. In each of these cases notification would be possible and unlikely to involve a disproportionate effort, however, would clearly be contrary to the public interest. It is noted that the Discussion Paper states (at pages 72 and 73) that:

> *… some flexibility in the requirement to provide notice should be retained for situations where notice is unnecessary as the individual is already aware of the matters that would be notified and where providing notice would be impossible or would involve disproportionate effort or may actually be harmful. Examples of such situations are set out in the APP Guidelines, including where notification may pose a serious threat to the life, health or safety of an individual or public health or safety, or where a law enforcement agency obtains personal information from a confidential source for the purpose of an investigation'.* [Emphasis added]

55. This comment does not appear to reflect the proposal in proposal 8.4, which does not have an exception for where disclosure may be harmful. The proposal in the Discussion Paper does not cover the situations in the three dot points above and those situations clearly should be an exception to any obligation to give an APP 5 collection notice.

Restricted and Prohibited Practices

56. The Law Council agrees that different types of personal information handling can present differing risks and potential impacts to individuals, and therefore certain practices require a higher level of protection and continuing oversight. Privacy Impact Statements, and regularly reviewed Privacy Impact Assessments, may be an effective

way of ensuring ongoing compliance from APP entities, and increase community confidence that emerging, higher risk practices are clearly identified as such, with tighter regulation and oversight.

57. Environmental Impact Statements and Assessments prescribed in environmental protection legislation are an example of addressing ongoing risk, given community expectations of corporate responsibility in minimising serious harm, and the concept of Privacy Impact Assessments have the potential to provide a further degree of organisational accountability in relation to the collection of personal information.

Children and vulnerable individuals

58. As noted at pages 109 to 110 of the Discussion Paper, the ALRC responded to the issue in the '*For Your Information: Australian Privacy Law and Practice'* (ALRC Report 108), and concluded that the Privacy Act should not contain an express test allowing APP entities to assess capacity.[17] The ALRC's conclusion was reached on the basis that the presumption of capacity exists at common law and capacity assessments are better dealt with in specialised legislation.[18] The ALRC acknowledged that capacity assessments are complex tasks which often require a medical assessment and that, imposing capacity assessments on APP entities would be overly burdensome.[19] However, as noted by the ALRC, those entities should be alert to the possible occurrence of issues concerning capacity and take those matters into account.[20]

59. The Law Council agrees with the ALRC's position and submits that an express provision should not be provided for in the Privacy Act to allow APP entities to assess capacity on an individualised basis. This position is predicated on the basis that:

- tests for decision-making capacity currently differ across jurisdictions and to impose any legal test or permission to undertake capacity assessments in the Privacy Act, without any nationally consistent approach to assessing capacity (or Commonwealth capacity assessment guidelines), would further complicate an already complex legal regime; and
- capacity, as well as supported and substitute decision-making are protective concepts as opposed to restrictions on or removal of people's rights. 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.

Right to erasure

60. The Discussion Paper seeks feedback on the most appropriate means of introducing a right to erasure (as exists under the GDPR) that would provide individuals with greater control over their personal information without negatively impacting other public interests The right to erasure and corresponding implementation of such a right fundamentally requires striking an appropriate balance between an individual's right to control their personal information and other rights to retain and or share or access information.[21]

---

[17] Australian Law Reform Commissioner, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) (Final Report, 12 October 2008) [70.52] 2350.
[18] Ibid [70.49] - [70.53] 2349 - 2350.
[19] Ibid [70.49] 2349 -2350.
[20] Ibid [70.52] 2350.
[21] Monique Magalhaes, '*Why the GDPR's Right to Erasure May Sometimes be Wrong'* (May 2018), available at <https://techgenix.com/right-to-erasure/>.

61. 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. As stated in the Law Council's response to the Issues Paper, careful consideration will need to be given to the following factors:

    - the right to erasure often applies only to personal information collected based on consent. Substantial questions about the role of consent as part of a broader regulatory structure need to be addressed before considering the right to erasure; and
    - the right to erasure is the subject of multiple intricate exemptions which will need to be considered in the context of the law in Australia. This will raise questions of intellectual property rights, competition law and media law related issues. Careful and detailed analysis will be required of a regime that will require entities to retain data and address how these requirements interact with protection of personal information in the context of a right to erasure.

62. There is limited support for a right to erasure amongst the Law Council's membership. This is because the rights of individuals are addressed by the right to make a correction (APP13) and the obligation to destroy or de-identify the information (APP11.2). One specific suggestion is that if a right to erasure is introduced, an APP entity should be able to reject the request on specific grounds. Reversing an erasure request in this way would enable individuals to always be able to make such a request, and an APP entity being able to grant such a request, but also balancing this request against a specific set of reasons why an APP entity may not wish to erase the information, for example, because it is still needed to fulfil a contract. Under this approach, clear guidance and example scenarios would need to be published by the OAIC.

63. Further, the Law Council is supportive of the view expressed in the Discussion Paper that erasure rights should not impede the functions of investigative or law enforcement activities. The Law Council notes that it may be appropriate to extend this to investigations by private companies as private companies have an interest in preventing fraud, cybersecurity attacks, monitoring civil unrest, investigating internal and external threats to businesses or employees, or providing services to law enforcement organisations outside regular law enforcement activity.

Behavioural marketing

64. Proposal 16.2 in the Discussion Paper suggests that the use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

65. The Law Council agrees with the principle behind this proposal, however notes that the term 'influencing an individual's behaviour' is very broad, and would likely pick up any form of advertising and marketing, and not just the behavioural marketing discussed (noting that the purpose of advertising, after all, is to influence behaviour).

Automated Decision-Making

66. In response to the question posed after proposal 17.1 in the Discussion Paper, the Law Council suggests that a non-exhaustive list of examples should be developed and made available. It should also be supplied in a form (i.e. through some form of subordinate legislation) that would allow it to be focussed on the technology of the day and to be updated on a regular basis.

67. Automated Decision Making (**ADM**), and what is currently known as artificial intelligence, or machine learning, is currently one of the most rapidly developing fields in the information technology. While the Privacy 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.

Security and destruction of personal information

68. Proposals 19.1 and 19.2 in the Discussion Paper aim to strengthen cybersecurity requirements around personal information. The Law Council agrees with proposal 19.2 that a list of factors should be included to indicate what will be considered to be reasonable steps to protect personal information by mitigating cyber risk and emerging threats.

69. However, the Law Council suggests that proposal 19.2 (regarding the need for a list of factors that indicate what reasonable steps may be required steps to protect personal information) be implemented as subordinate legislation so that it can, as discussed above, be focussed on the technology and best practices of the day and updated quickly and efficiently if/as required. Similarly, proposal 19.2 could be expanded to include the minimum cybersecurity practices which should be binding on APP entities.

70. In this respect the Law Council notes that the cybersecurity landscape has changed significantly over the last decade, with cloud services becoming mainstream and the use of artificial intelligence growing rapidly. The cybersecurity practices of a decade ago, or even five years ago, would not necessarily be relevant to today's information technology landscape. In that context, it is readily apparent that any cybersecurity recommendations or requirements will very much need to be able to 'move with the times.' It is important to retain technological neutrality noting how dependent security practices are to new technologies.

71. In supporting this proposal, the Law Council notes that making recommendations binding emphasises the importance of good cybersecurity practice when storing personal information and can be expected to increase confidence in APP entities that collect personal information, as well as setting a baseline for how such information should be managed that is aligned with current cybersecurity practice.

Privacy by Design

72. The Law Council is generally supportive of suggestions set out in the Discussion Paper regarding the implementation of 'privacy by design' and 'privacy by default' measures[22] in the Privacy Act noting, as the Discussion Paper does, the existence of such measures in the GDPR.

73. In the experience of the Law Council, many APP entities already implement security by default/design principles, and doing so has become common practice in the information technology industry. Notably, this has happened without the kind of regulation discussed, but there is a self-interest component to security by default/design that has served as a motivating factor (i.e. it would be in the interests of a business to ensure its

[22] For further information on these concepts, see Office of the Australian Information Commissioner, '*Privacy by design*' <https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design#:~:text='Privacy%20by%20design'%20is%20a,of%20new%20systems%20and%20processes>.

systems were kept as secure as possible to ensure the efficient operation of the business and protection of its reputation).

74. In contrast, there is no corresponding self-interest component in privacy by default/design. The data protected is 'other people's data' and, indeed, it appears that the relevant self-interest would tend towards less privacy instead of more privacy, due to business efficiency concerns.

75. Therefore, the Law Council is of the view that there is a possible need for legislation to step in and provide for that 'self-interest', so as to ensure that personal information of individuals is protected. These protections exist in the GDPR and the Law Council submits that consideration should be given to similar protections being added to the Privacy Act.

Overseas data flows

76. The Law Council favours an application for adequacy under the GDPR as a preferred means of addressing the challenges of cross border data transfers. This is because, once successful, the benefits of adequacy are:

    - economy wide in that it applies to all APPs with minimum steps that the APP entity needs to take at the entity level - this will help reduce complexity and eliminate 'red tape';
    - consistent with other transborder requirements be they regional, such as Asia-Pacific Economic Cooperation, or industry specific as an outcome of any given code or binding scheme (as suggested in chapter 23 of the Discussion Paper);
    - preserving the application of existing measures adopted by many APP entities, including standard contractual clauses, binding corporate rules or similar frameworks under Articles 46 and 47 of the GDPR; and
    - enabling Australian law to develop:
        - without the need to copy or artificially supplant aspects of the GDPR, while still building on some of the more universal aspects of the GDPR, and remain adequate as measured under a 'high water-mark' standard without necessarily copying the standard; and
        - in a manner that supports harmonisation and interoperability.

77. The Law Council appreciates that such an application will require multiple resources and the commitment of various agencies and regulators. It is by necessity a lengthy process. That said, the current law reform process presents an opportunity to update the Privacy Act in a manner that helps build a stronger case for adequacy and is not an impediment to the success of such an application should there be a need or a desire to do so in the future.

78. The Law Council notes that several legal developments have fundamentally changed some of the earlier considerations. For example the approach to exemptions such as the small business exemption. This is especially so in industries that rely heavily on digital commerce or otherwise have a global footprint. The Law Council notes the impact of Article 3 of the GDPR, specifically Article 3(2) which extends the application of the GDPR regime to organisations (processors or controllers) not established in the European Union where the processing activities are related to:

    - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

- the monitoring of their behaviour as far as their behaviour takes place within the Union.

79. The broad scope of definition of 'processing' and 'controller' under Article 4 of the GDPR, means that many APP entities are potentially caught by extraterritorial scope of the GDPR.

80. In addition, latest developments such as the *Schrems II* decision,[23] the newly approved standard contractual clauses[24] and additional guidance issued by the European Data Protection Board [25] have increased the standards of compliance for any entity dealing with transfers of personal data involving the European Economic Area. This makes the need for interoperable mechanisms of lawful transfers that much more important and time critical.

Part 3: Regulation and enforcement

Enforcement

81. The Law Council acknowledges the recommendations of the ACCC in its Digital Platforms Inquiry about bringing the penalties for breaches of privacy into line with the penalties available under the Australian Consumer Law and agrees that such an approach could serve to elevate the status of privacy law and act as a significant deterrent against severe and/or repeated offences against the Privacy Act.

82. Law Council members have expressed in-principle support for the proposal set out in the Discussion Paper to create tiers of civil penalty provisions to provide the OAIC with more options to better target regulatory responses. It is noted that in regimes where penalties are significant, such as the GDPR fines in the EU, large businesses routinely include GDPR compliance in their terms with their supply chain. This creates an economy-wide positive impact on business behaviour.

83. However, the Law Council is aware of concerns that budget constraints faced by the OAIC may at times impede its ability to bring enforcement proceedings. In this regard, it is critical that the OAIC be appropriately resourced to apply to the courts for civil penalties for serious or repeated interferences with privacy and to further its enforcement activities. It would also be important to provide clarity as to what constituted a 'serious' or 'repeated' interference with privacy and the application of the powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) to aid the Commissioner in their investigatory role.

84. The Law Council would also welcome the expansion of the powers of the OAIC to undertake public inquiries and reviews into specified matters provided that it is coupled with an education role to inform APP entities of their obligations with more nuance or detail.

---

[23] Court of Justice of the European Union, *Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems,* available at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155>.

[24] European Commission, '*European Commission adopts new tools for safe exchanges of personal data*' (4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847>.

[25] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Adopted on 10 November 2020), available at *<https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf>.*

85. To support separation of roles, consideration could be given to an alternative regulatory model appointing a Deputy Information Commissioner – Enforcement. This would leave the Information Commissioner to operate conciliation and education operations and leave enforcement operations to the Deputy. A further refinement would be to create a role of Deputy Information Commissioner – Freedom of Information, which would further relieve the Information Commissioner's workload and enable the Commissioner to have a greater focus on privacy issues.

Direct Right of Action

86. The Law Council's membership has provided mixed support for a direct right of action as described in the Discussion Paper with a triage function able to be performed by the Information Commissioner. However as set out below, there is in-principle support for a direct cause of action under the Privacy Act and for the tort of serious invasion of privacy, if the scope of the cause of action is well defined and articulated in the updated Act. This will require careful consideration of the drafting to ensure that there are no unintended consequences and all causes of action as updated by the reform process can be considered in context.

87. While there is a diversity of views on the private right of action under the Privacy Act's data protection regime, the Law Council makes the following observations.

- 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; and
- 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. As noted above, this requires the OAIC to have sufficient resources dedicated to responding to initial claims that the process does not unduly delay a resolution.

Statutory Tort of Privacy

88. In 2021, the Law Council engaged with its Constituent Bodies on the issue of a statutory tort of serious invasion of privacy, and there appears to be strong support for the introduction of such a statutory right, on the condition that there are sufficiently high thresholds in place to ensure actions are limited to serious invasions of privacy and that, as with a direct cause of action noted above, the scope of the statutory tort is carefully considered and drafted to address the risk of unintended consequences.

89. In developing the new tort, consideration should be given to adopting the ALRC's approach from the *Serious Invasions of Privacy in The Digital Era* (ALRC Report 123) of 2014 which covered two types of invasions of privacy: intrusion upon seclusion, and misuse of private information.

90. The Law Council expressly notes and, subject to drafting and further consideration of the matters as part of an exposure draft of any pending changes, supports recommendations 4 to 13 (inclusive) of the ALRC report. The Law Council notes that in applying the reasoning of the ALRC, it will be important to reconcile that the new statutory tort will apply to information privacy only as regulated under the Privacy Act and not to other types of intrusions[26].

[26] For example, intrusions into a person's physical private space.

91. Consistent with the ALRC's recommended approach, the design of legal privacy protection must be sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments. This recommendation is particularly salient in light of the exponential pace at which new technologies such as AI and blockchain are developing, and the evolving scope of their application. This again reinforces the need to carefully frame the materiality threshold to avoid ambiguity and unnecessary conflict and litigation.

92. In providing support for a statutory tort in line with the recommendations of the ALRC, the Law Council notes that:

    - the common law has taken too long to develop a tort and cannot be expected to develop a comprehensive one anytime soon. Developments in other countries indicate that statutory causes of action for the invasion of privacy are now established features of the legal landscape;[27] and
    - intrusion upon seclusion, and misuse of private information are at the core of the right to privacy and, by describing the action as a tort, courts are encouraged to draw on established principles of tort law, giving the cause of action a degree of certainty, consistency and coherence.

93. The Law Council considers it critical that any proposed statutory development for such a cause of action should be subject to an iterative public consultation process, including careful scrutiny of the detail of any proposed legislation. In drafting the legislation, it will be necessary to strike the appropriate balance between privacy protection, freedom of expression and communication and national security, and that courts will need to be empowered to weigh up the public interest in privacy against any other countervailing public interests.

94. This will require a careful and considered review of the draft legislation to ensure that the legislation reflects community expectations and is free of unintended consequences. The Law Council would welcome the opportunity to be involved in this review process.

Notifiable Data Breach Scheme

95. The Law Council is supportive of the proposal in the Discussion Paper that notification of a data breach include steps to mitigate any loss. This is consistent with the current requirements that a statement about an eligible data breach provides recommendations as to the steps an individual must take in the circumstances.[28]

96. Australia has seen a welcome increase in the notification of data breaches since the introduction of the Notifiable Data Breaches (**NDB**) scheme. However, Australia's notification rate remains lower than many European nations who are subject to the notification regime under the GDPR.[29] The Law Council has received anecdotal reports of concern, evidenced by OAIC reports/data, that there is increasing under-reporting of data breaches.

97. The Law Council also notes that matters involving breach reporting need to be considered together with considerations about a direct cause of action or a new statutory tort. This is because any new cause of action and the existing notification regime are underpinned by an assessment of materiality.

---

[27] ALRC, *Serious Invasions of Privacy in the Digital Era: Final Report*, June 2014.
[28] Section 26WK(3) of the *Privacy Act 1988* (Cth).
[29] DLA Piper, *GDPR Data Breach Survey* 2020 (20 January 2020) <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>.

98. Section 26WG of the Privacy Act currently lists a number of non-exhaustive factors that may lead a reasonable person to decide that access, or disclosure of information would be likely (or not likely) to result in 'serious harm to any of the individuals to whom the information relates'. Section 13G deals with 'serious' or 'repeated' contraventions of the Privacy Act and provides for a civil penalty of 2,000 units for such contraventions. These terms are not defined and, unlike section 26WG, are not supported by a non-exhaustive list of factors that would give rise to such a contravention. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) which introduced these terms into the Privacy Act states that the ordinary meaning of the terms 'serious' and 'repeated' will apply. This means that matters that may fall for consideration under this section are addressed by regulatory guidance and applicable guides on regulatory enforcement.[30] The Law Council notes that since the introduction of section 13G, there have been very few instances where it was relied on, the current known example is in the *Australian Information Commission v Facebook Inc* matter. [31]

Definitions

99. The Law Council does not support importing new definitions of controller and processor into the Privacy Act as discussed in chapter 21 of the Discussion Paper. This is considered unnecessary because:

- 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;[32] and
- where an APP entity 'holds' personal information as defined under the Privacy 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. The issue has not been the subject of litigation and has largely been addressed by applicable guidance.[33]

Interactions with other schemes

100. The Law Council supports the creation of a Commonwealth, state and territory working group to harmonise privacy laws and focus on key issues in relation to privacy. Consistency in regulation would support transparency for consumers and reduce compliance burdens on organisations. Cooperation might include recognition that notifications to one scheme met obligations to report under multiple schemes, and consistency in regulation would almost certainly support transparency for consumers and reduce compliance burdens on organisations.

101. Under APP 7, the Privacy Act currently regulates an organisation's use and disclosure of personal information for the purpose of direct marketing. However, APP 7 does not

[30] Office of the Australian Information Commissioner '*Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions*' (June 2020) <https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties>.
[31] *Australian Information Commission v Facebook Inc* [2020] FCA 531 (22 April 2020).
[32] Office of the Australian Information Commissioner, '*Australian entities and the EU General Data Protection Regulation'* (June 2018) available at <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation>.
[33] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) available at <https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf>

apply to the extent that the *Spam Act 2003* (Cth) (**Spam Act**) or *Do Not Call Register Act 2006* (Cth) (**DNCR Act**) apply.[34]

102. Currently, the Spam Act establishes an opt-in regime which prohibits the sending of commercial messages via email, SMS or instant messaging without the consent of the receiver. This differs from the provisions governing the use of information for direct marketing in the Privacy Act.[35] The Spam Act also accepts the 'conspicuous publication' of certain email addresses to satisfy inferred consent from the owner.[36] Under the DNCR Act, consent may be express or inferred, although express consent which is for an indefinite period or unspecified amount of time must be automatically withdrawn after three months.[37]

103. Any reform at a Commonwealth level should ensure that the collection, use and protection of privacy utilises consistent terminology and coverage across the Privacy Act, the Spam Act and the DNCR Act. This would ensure that the processes and protections are more transparent and accessible for consumers and end-users.

[34] *Privacy Act 1988* (Cth), Sch 1 APP 7.8.
[35] Ibid, s 6.
[36] *Spam Act 2003* (Cth) sch 2 cl 4.
[37] *Do Not Call Register Act 2006* (Cth) sch 2 cl 3.