Law Council
OF AUSTRALIA

Online Privacy Bill Exposure Draft

Commonwealth Attorney-General's Department

14 December 2021

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**
Introduction **5**
Timeframe and process for developing the OP code **5**
Definition of OP organisation **6**
Banking and related services 6
Extension beyond digital platforms 7
Categorisation **8**
Social media services 8
Data brokerage platforms 8
Large Online Platforms 9
Loyalty Schemes 9
Attorney-General's discretion 9
Interaction with the Australian Privacy Principles **9**
APP 1.4(c) – Privacy policy inclusions 9
APP 5 – Notice requirements 10
Individual rights to personal information **10**
Cease of use requests 10
Right to Erasure 11
Protection of children **12**
Reasonable steps 12
Carers 12
Consent **12**
Information Sharing **13**
Enforcement and penalties **14**

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 2021 Executive as at 1 January 2021 are:

- Dr Jacoba Brasch QC, President
- Mr Tass Liveris, President-Elect
- Mr Ross Drinnan, Treasurer
- Mr Luke Murphy, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, 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 of Australia acknowledges input received from the Law Society of South Australia and Law Institute of Victoria in the preparation of this submission.

The Law Council also appreciates the contributions of the Business Law Section's Privacy Law Committee and Media and Communications Committee.

Introduction

1. The Law Council of Australia welcomes the opportunity to comment on the Commonwealth Attorney-General's Department's exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (**Exposure Draft**) and accompanying Explanatory Paper.

2. The Law Council acknowledges that the Exposure Draft represents an initial step towards addressing the privacy challenges posed by social media and certain other online platforms by strengthening the operation of the *Privacy Act 1988* (Cth) (**Privacy Act**). The Exposure Draft approaches this challenge by allowing for the introduction of a binding Online Privacy (**OP**) code for such platforms, setting out how they will comply with the Australian Privacy Principles (**APP**).

3. The Exposure Draft Bill, if passed in its current form, will also substantially increase the scope and size of the penalties applicable to all APP entities. This increase will take place *before* any substantive reforms as to the content of the Privacy Act. This fragmentation in the reform process is regrettable and may expose APP entities to an increase in their respective compliance burden without a corresponding uplift in certainty of the standards that they are required to meet.

4. The Law Council is engaging with the concurrent review of the Privacy Act and notes the importance of consistency and compatibility between Australia's existing privacy legislation, anticipated reforms, and the OP code. To this end, there must be a concerted effort to avoid fragmentation in the reform process, as set out below. Consideration should be given to progressing the OP code only after the Privacy Act review is complete to help ensure that the instruments are complementary.

Timeframe and process for developing the OP code

5. The Regulation Impact Statement (**RIS**) accompanying the Exposure Draft outlines an initial process by which industry bodies and organisations will act as the 'OP code developer' and draft the OP code. The RIS then outlines a process of public consultation of at least 28-days before submitting the finalised code for approval to the Commissioner.

6. From the outset, the Law Council has a concern that a 28-day public consultation period to provide feedback on the industry-developed draft OP code may be unduly restrictive and suggests that the public consultation period be extended to a minimum of 60-days to ensure there is adequate opportunity for consultation and detailed consideration. Extending the consultation period will provide stakeholder bodies and organisations with an appropriate amount of time to consider the OP code in its entirety, including its long-term and direct impact on the general public.

7. While industry engagement in the development process is important to account for the commercial realities of the proposed OP code, the Law Council also encourages ongoing involvement of the eSafety Commissioner and other relevant regulators throughout the industry development phase. This would promote alignment with the objectives of the Exposure Draft and ensure that its core objectives are not undermined. The Law Council also notes that industry stakeholders should be encouraged to consider and limit potential regulatory barriers for new industry entrants, which may arise upon the implementation of the OP code.

8. There are many obligations that are proposed to be included in the OP code that are impacted by the reforms set out in the Discussion Paper for the concurrent Privacy

Act review – not least potential changes to the definition of 'personal information'. As a consequence, there is a risk that, if the OP code is put in place before the review process is complete, those bound by the OP code will be required to make a second round of substantial compliance changes when the Privacy Act amendments occur – thereby significantly increasing compliance costs.

9. Considering this concern, the Law Council submits that the development of the OP code provisions should align with the Privacy Act review, which may mean that the OP code is delayed until the review is complete, or the Privacy Act review is prioritised to align these important reforms and measures they seek to introduce.

Definition of OP organisation

Banking and related services

10. The Law Council has reservations about the breadth of the definition of 'OP organisation' as defined at proposed section 6W of the Exposure Draft, which may extend beyond the 'digital platforms' as identified in the Australian Competition and Consumer Commission (**ACCC**) Digital Platforms Inquiry.[2] The result is the potential for this definition to unintentionally capture other types of platforms, such as banking and related services. The extension of the OP code to a broader range of types of organisations beyond those identified by the ACCC as demonstrating concerning practices does not appear to be supported by evidence.

11. The Law Council notes the current exclusions from the definition of 'electronic service' provided in subsection 6X(2) and endorses the exclusions for services that process payments or provide access to payment systems in paragraphs (c) and (d) respectively. There are concerns, however, with the practical implications of the requirement currently in paragraphs 6X(2)(c) and (d) for the relevant payment-related purpose to be the sole purpose. It is recognised that:

    - businesses that are not financial institutions may provide applications/services that provide access to payment services, and there is the potential for such an application or service to have multiple functions, some of which relate to payments and others of which enable online social interaction and/or have a purpose of marketing goods and services that are not financial services; and

    - where a service has more than one purpose, it may not be appropriate for the exception to apply.

12. However, the result of a sole purpose test would be that the existence of a secondary purpose, no matter how ancillary or incidental to the main purpose it is, would remove payment processing services and services providing access to a payment system from the relevant exception. Many such services offer ancillary functions (for example, account balance enquiries, account balance transfers between accounts with the same organisation, currency conversion services). Accordingly, it is suggested that the sole purpose test, currently referenced in paragraphs 6X(2)(c) and (d) of the Exposure Draft, be replaced with a test that does not disentitle a service from relying on the exception because that service offers ancillary functions. This could be achieved by replacing the sole purpose test with a predominant purpose test, or with some other test that recognises the existence of ancillary and other related functions.

[2] Australian Competition and Consumer Commission *Digital platforms inquiry - final report* (July 2019).

13. Paragraph 6X(2)(d) of the Exposure Draft proposes that a 'payment system' be given the meaning in the *Payment Systems (Regulation) Act 1998* (Cth) (**PSR Act**). The review of the Australian Payments System[3] identified that the current definition may no longer adequately capture the full suite of payment systems within the payments ecosystem and recommended that the definition be expanded. The Government response to the recommendations in that review states that the Government agrees with this recommendation and that Treasury will commence consultation on amendments to the PSR Act in early 2022. Given the recognition that the current definition may not be broad enough to capture new and emerging payment systems, and that the current definition is unlikely to be amended until sometime after the Exposure Draft progresses, consideration should be given to a definition of 'payment system' for the purpose of paragraph 6X(2)(d) that better reflects the full suite of payment systems and payment networks within the payments ecosystem.

Extension beyond digital platforms

14. Similar issues arise in other sectors of the economy, as noted above. The Exposure Draft provides that the OP code will bind OP organisations. OP organisations fall within three categories under the proposed new section 6W, namely organisations providing social media services, organisations providing data brokerage services and large online platforms.

15. The Explanatory Paper for the Exposure Draft, as well as the RIS provide two primary rationales for the proposed reforms and the creation of the OP code. The first is that this is a necessary response to the 2016 Facebook/Cambridge Analytica data harvesting incident. The second is that the need for the OP code is reinforced by a recommendation from the ACCC in the Digital Platforms Inquiry. Neither of these rationales support the broad definition of OP organisations that has been included in the Exposure Draft.

16. Looking at the first rationale, the Facebook/Cambridge Analytica data harvesting incident involved only one specific social media platform. The Law Council queries whether sufficient evidence is provided in either the Explanatory Paper or the RIS that suggests the data practices involved in that incident are engaged in by other Australian businesses or by other social media platforms.

17. Looking at the second rationale, particular attention is drawn to Recommendation 18 of the Digital Platforms Inquiry Final Report, which proposed a privacy code for digital platforms. The ACCC's recommendation was that such a code should apply *only* to digital platforms and not more broadly. A code was recommended to address data practices of digital platforms that the ACCC had found, through extensive examination and investigation, to be problematic. For completeness, the Law Council notes that for the purposes of the Digital Platforms Inquiry, the term 'digital platforms' was limited to:

    - search engines;
    - social media platforms; and
    - digital content aggregation platforms, being online intermediaries that collect information from disparate sources and present that information to consumers as a collated, curated product.

18. Given the issues identified by the ACCC and the issues arising in the Facebook/Cambridge Analytica scandal which are referred to in the Explanatory

[3] The Treasury, '*Review of the Australian Payments System – Final Report* (August 2021).

Paper and the RIS, it is appropriate that an OP code within the regulatory framework established by the Privacy Act is put in place. However, to address these concerns, the OP code should apply only to 'digital platforms' as defined for the purposes of the Digital Platforms Inquiry.

Categorisation

19. As set out above, the OP code captures a range of online services and platforms, including social media services, data brokerage services, and large online platforms.[4] The Law Council welcomes moves to implement the recommendations of the ACCC as they relate a privacy code for digital platforms, but maintains reservations about the Exposure Draft extending beyond this scope. Specific comments on the categories of online services are set out below.

Social media services

20. There is no requirement that a social media service collect personal information to be subject to the OP code, although this threshold is required for other categories. The absence of this requirement for social media services ensures that any unintentional collection of personal information that may occur incidentally either through the platform's operations or within the information hosted on the platform, such as forum discussions, is regulated under the OP code.

21. The Law Council has received feedback that regard should be had to social media services that are delivered in a manner that retains no personally identifiable information and are delivered on a framework of anonymity or de-identification. The exclusion of this subset of social media services may encourage new and existing services to reframe their personal data retention requirements, reducing the need for regulation within the industry from the outset. While this situation may already be covered by APP 2 it may still be a matter for the broader review of the Privacy Act.

22. Further, the OP code is proposed to apply to social media services that have the 'sole or primary purpose of enabling online social interaction between two or more end-users' but excludes organisations which 'enable online communication, interactions and content sharing as an additional feature'.[5] While this exemption is welcome, the Law Council cautions that organisations may adjust service functionalities in order to align with the exclusion criteria, and thereby avoid regulation under the OP code under this approach. The potential for this shift should be monitored closely as the measures are implemented.

Data brokerage platforms

23. Data brokers may provide data to government, law enforcement, investigators, and high target businesses for the purposes of, amongst others, preventing fraud, finding missing persons, investigating crimes (such as illicit tobacco, and firearm, drug and human trafficking), monitoring internal and external threat activity, financial scams and cyber security risks and events.

24. While the Law Council queries the inclusion of data brokerage platforms (for reasons set out above), should this policy position remain, the OP code would benefit from a limited exclusion for data brokers distributing personal information for this narrow set

[4] Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (October 2021) p 6.
[5] Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (October 2021) 7 ('Online Privacy Bill Explanatory Paper').

of purposes, or the inclusion of a specific exemption for these purposes under the OP code may be an appropriate alternative.

Large Online Platforms

25. The proposed threshold for a large online platform of 2.5 million end users potentially limits the application of the OP code to key organisations and excludes other relevant organisations which handle a significant amount of personal and sensitive information, despite a lower number of end users.

26. As outlined in the RIS, the personal information of over 300,000 Australians was harvested and shared without consent in the Cambridge/Analytica incident.[6] It is understood that several major online platforms would not meet the end user threshold to be considered a large online platform, despite holding large amounts of personal information.[7] Consideration could therefore be given to reducing the end user requirement to ensure the protective purposes of the OP code are realised. This would also provide for organisations that are likely to reach the threshold for coverage as a large online platform under the OP code in the near future, and ensure relatively new platforms demonstrate a level of compliance at earlier stages of organisational growth and development.

Loyalty Schemes

27. The Law Council queries the exclusion of customer loyalty schemes from coverage under the OP code given their similarities to online shopping platforms, which collect personal information in order to engage in targeted advertising.

28. While it is recognised that customer loyalty schemes fall within the scope of the current review of the Privacy Act, given the types of personal information captured, the methods of capture and storage, and the potential risks associated with the misuse of data within a customer loyalty scheme, consideration should be given to extending the OP code where such a scheme goes beyond the 'collect[ing of] information about members in order to generate consumer insights that are often used for targeted advertising'.[8]

Attorney-General's discretion

29. The Law Council submits that the Attorney-General's ability to include or exclude organisations from coverage under the OP code should be clarified, given the broad range of platforms and organisations sought to be covered under the OP code.

Interaction with the Australian Privacy Principles

APP 1.4(c) – Privacy policy inclusions

30. There is value in including APP 1.4(c) under the OP code. However, this is already a requirement to ensure minimum compliance with the APPs. In order to achieve substantive impact, it is suggested that the OP code build on APP 1.4(c) through the introduction of a requirement for consistency and clarity with all defined APPs as to

[6] Regulatory Impact Statement, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (October 2021) p 3 ('Regulatory Impact Statement').
[7] David Correll, Social Media Statistics Australia (1 February 2021). Available at <https://www.socialmedianews.com.au/social-media-statistics-australia-january-2021/>.
[8] Discussion Paper, Privacy Act Review (October 2021) p 125.

how information is collected, held, used and disclosed. This could require consideration of, but is not limited to:

- the complexity of the language used within a privacy policy;
- the length of a privacy policy;
- the possible including of layered privacy policies with specific requirements for each layer (i.e. a simplified privacy policy which is supported by a more detailed privacy policy); and
- the inclusion of high interest information, such as:
  - the jurisdictions within which personal or sensitive information may be transmitted to;
  - where a user can revoke their consent or maintain control over their privacy settings; and
  - a minimum standard for explanation of the type of testing or beta programs in which user information may be included.

31. It is acknowledged that the inclusion of standardised policies is currently being considered within the Privacy Act review. This is a further example of the potential for misalignment as noted below. Nevertheless, as matter of substance, implementation of standardised policies is supported, subject of course to alignment to avoid duplication and inconsistencies.

APP 5 – Notice requirements

32. The Law Council welcomes notice requirements aligning with those proposed in the Privacy Act review.[9] The Law Council suggests that it may be appropriate to expand notice requirements under the OP code to promote alignment with the key objective of ensuring users and consumers are adequately informed regarding how their information will be used, noting the need for consistency as discussed above. This may involve an explicit reference to an objective standard and use of approved or template style notices to help ensure this requirement is well understood and is uniformly and consistently applied.

Individual rights to personal information

Cease of use requests

33. The proposed OP code requires 'provision for or in relation to requiring OP organisations to take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose, the personal information of an individual if so requested by the individual'.[10] The Law Council notes that these obligations appear to be less rigorous than comparative privacy frameworks internationally.[11]

34. In this regard, the use of language relating to 'reasonableness' is potentially overly vague. Large organisations and social media platforms have considerable resources available to ensure bare minimum compliance with existing regulations, so it is likely that this language enables further flexibility to continue operations which do not align

[9] [9] Attorney-General's Department, Privacy Act Review Discussion Paper (October 2021) p 68.
[10] Exposure Draft, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (October 2021) cl 26KC(2)(h).
[11] Regulation (EU) 2016/679 (General Data Protection Regulation) art 18; *California Consumer Privacy Act (2018)* s 1798.

with international expectations relating to cease of use obligations. This is perhaps a matter that should be addressed in the OP code.

35. In circumstances where an individual requests the organisation to cease using or disclosing personal information, the RIS outlines that OP code organisations will 'only be able to impose reasonable charges for responding to the request', although charges should not be imposed when an individual makes the request or if the organisation is unable to comply with the request, in line with APP 12.[12]

36. The Law Council queries the appropriateness of the imposition of charges against a user for responding to a cease of use request. Cease of use rights may provide certainty and peace of mind to individuals, although value remains in the information held by an organisation, whether it is quarantined from use or otherwise. The information is beneficial to the holding organisation, and other organisations who may be able to access the data through legal means, or threat actors who target the information and gain access. As the personal information collected from the individual provides value to the organisation, the individual should retain free access rights and should not be subject to a financial penalty for requesting amendment or cease of use, or as a result of an organisation responding to a request. Again, this could be a matter that is addressed in the OP code.

Right to Erasure

37. The European Union's General Data Protection Regulation (**GDPR**) contains a right of erasure provision enabling an individual to request that personal data stored by an online organisation be deleted without undue delay in certain circumstances.[13] Similarly, the *California Consumer Privacy Act (2018)* enables consumers to request the deletion of personal information that has been directly collected from the consumer by the organisation,[14] while China's Personal Information Protection Law also contains right of erasure provisions.[15] The Law Council acknowledges that the right to erasure and corresponding implementation of such a right 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.[16]

38. The Law Council is aware that similar rights are being contemplated under the Privacy Act review, so setting a higher standard for OP code organisations would not be overly burdensome, given their existing compliance obligations for right of erasure provisions under the aforementioned comparative laws.

39. A further issue relates to a possible right to erasure for children or vulnerable groups, with no associated cost for compliance. In circumstances where children and vulnerable people do not have control over the collection or storage of their personal information, the right to erasure becomes more important. Children and vulnerable groups are subject to the protection of their legal guardian, however, the interests of a legal guardian may not always align at all stages of development and these groups are unlikely to be able to provide express and informed consent. Consideration could be given to how children and vulnerable groups are able to be empowered under the OP code to address this potential imbalance.

---

[12] Regulatory Impact Statement p 15.
[13] Regulation (EU) 2016/679 (General Data Protection Regulation) art 17.
[14] California Consumer Privacy Act (2018) Div 4 Part 4
[15] Personal Information Protection Law (2021) Art 47.
[16] Monique Magalhaes, 'Why the GDPR's Right to Erasure May Sometimes be Wrong' (May 2018). Available at <https://techgenix.com/right-to-erasure/>.

Protection of children

Reasonable steps

40. Proposed paragraph 26KC(6)(a) of the Exposure Draft purports to govern how an OP organisation (as defined at section 6W) verifies the age of a person under 16, stating that it must 'take all reasonable steps to verify the age of individuals to whom the OP organisation provides an electronic service'.

41. The Law Council considers that measures put in place to protect children could be strengthened further, noting that the provision is not sufficiently defined, particularly in a context of, firstly, the protection of children, and secondly, the ease with which children currently circumvent age verification processes on social media. It is suggested that OP organisations should be held to current best practice and should use the available technology at their disposal to take all appropriate steps to verify the age of a new subscriber, rather than the current practice of self-declaration of age which is not sufficient.

42. One option is to require OP organisations to take more than just 'reasonable' steps by requiring, as a minimum, the taking into account of available technology, as a similar test does in Article 8(2) of the GDPR, and also current best practices available to the industry.

43. By way of example, the resources and expertise of a company such as Google would be expected to include the knowledge and financial resources to take reasonable steps to verify the age of the individuals to whom it would provide an electronic service. In contrast, a smaller company that may nonetheless meet the definition by having large subscribers may not have the same resources or expertise in technology to undertake the same steps that a company like Google would have the capacity to undertake.

Carers

44. Proposed subsection 26KC(6) of the Exposure Draft does not include 'parent, guardian or carer' as is included in other parts of the Privacy Act, for example, in obtaining consent relating to the CovidSafe app.[17] The Law Council queries whether the omission of a child's carer was intentional, or an oversight, noting a preference for the consistent use of the term 'parent, guardian or carer' as is currently used in the Privacy Act in relation to vulnerable individuals.

Consent

45. Proposed paragraphs 26KC(2)(d) and (e) of the Exposure Draft govern the consent regime for the OP code and provides that it must:

> *(d) set out how an OP organisation is to comply with Australian Privacy Principles 3 and 6 in ensuring that an individual has provided consent for the collection, use or disclosure of personal information; and*
>
> *(e) make provision for, or in relation to, the providing of such consent, including setting out the circumstances in which:*

[17] *Privacy Act 1988* (Cth), s94E.

(i) consent is taken to be provided voluntarily, and is informed, unambiguous and specific; and

(ii) consent is taken to be current and, in the case of sensitive information, is taken to have been renewed periodically or when circumstances change.

46. The Law Council notes the policy objective of making consent voluntary, informed, unambiguous, specific and current. However, the following potential shortcomings should be addressed:

- the OP code should include an obligation for an OP organisation to demonstrate as well as to '[set] out the circumstances' (proposed section 26K(2)(e)) in which consent is taken to be provided, noting this is similar to the requirements of Article 7 of the GDPR;
- consent for sensitive information should be 'explicit consent', similar to GDPR Art 9; and
- proposed paragraph 26KC(2)(e) states that consent should be current but only periodically renewed for sensitive information. The notion of currency itself implies periodic assessment. Therefore, preferable wording may require all consent to be renewed 'periodically or where circumstances change', unless it is unreasonable or impractical to do so.

47. To assist in the above, an approach could be modelled on the cookie consent pop-up notifications that are required under the GDPR and the E-privacy Directive 2009/136/EC.

48. A real-time consent system would enable users to have greater insight into and control over the data sharing process and ensure genuinely informed user consent. Additionally, end-user oversight would serve as a considerable deterrent for the misuse of information, as organisations should consciously assess the risk of alienating their client base when sharing personal information.

Information Sharing

49. The Exposure Draft proposes to grant the Australian Information Commissioner greater information-sharing powers by inserting a new section 33A at the end of division 3 of Part IV of the Privacy Act. In effect, this proposed amendment grants the Commissioner the ability to share information or documents with those 'receiving bodies' defined in subsection 33A(2) (being a law enforcement body, an alternative complaint body, and state, territory or foreign privacy regulators) for the purpose of the Commissioner or receiving authority exercising any of their respective functions and powers.

50. Further, proposed subsection 33A(5) specifically states that to avoid doubt the Commissioner may share information or documents with a receiving body whether or not the Commissioner is transferring a complaint or part of a complaint to the body.

51. The Law Council is concerned that the Commissioner's new information sharing power may be too broad when used in conjunction with the following:

- the Commissioner's current power to assess an entity's compliance with certain parts of the Privacy Act in the absence of any breach of the Privacy Act or complaint having been made; and

- the Commissioner's new power (- new subsection 33C(3)) in the Privacy Act (being the power to issue a notice to produce information or a document relevant to an assessment).

52. Whilst acknowledging that there are clear benefits to the Commissioner's new information sharing powers, the Law Council queries whether the current limitations on that power (as contained in proposed subsection 33A(3)) go far enough, given its potential breadth and the wider extent of information/documents that the Commissioner could possess.

53. In particular, the new power does not appear to contemplate the circumstances in which the Commissioner might refuse to share information/documents in response to a request by a receiving body (other than where not satisfied that the body has 'satisfactory arrangements' in place for protecting the information/documents). To address this:

- consideration could be given to incorporating an express requirement in proposed subsection 33A(3) (similar to that which appears in the proposed section 33B) to the effect that the Commissioner may refuse to share information with a receiving body if he or she considers that it is not in the public interest for him/her to do so; and
- further guidance should be given in relation to what constitutes a 'satisfactory arrangement' for the purpose of proposed paragraph 33A(3)(b). For example, this might include clarifying whether it is expected that, as a minimum, the receiving bodies are fully compliant with the requirements of APP 11.

Enforcement and penalties

54. The Law Council encourages the expanded involvement of the eSafety Commissioner in conducting investigations and assessments under the OP code. An active eSafety Commissioner within the space provides considerable certainty for the public and industry, to ensure that OP code organisations are compliant with the future OP code.

55. However, the Law Council notes that the extension of the penalty framework under the Exposure Draft will apply to *all* APP entities, and not only OP organisations. For example, section 13G currently applies to 'serious interferences with the privacy of an individual' or an act or practice that is a repeated 'interference with the privacy of one or more individuals'. These terms are not defined and have not had the benefit of case law. These are substantive legal questions that will be considered in more detail as part of the current review of the Privacy Act.

56. Assuming the Exposure Draft passes in its current form and steps are taken to enforce the penalties as increased, the lack of clarity as to the precise meaning of these types of interferences and current gaps in the notice and consent regime under the concurrent Privacy Act, will make the enforcement difficult and potentially ineffective. It will be important to maintain the momentum on the pending review of the content of the substantive provisions of the Privacy Act as foreshadowed under the Explanatory Paper to avoid uncertainty and unintended consequences created by the fragmented approach to reform. As a minimum, careful consideration needs to be given to revising the requirements of section 13G of the Privacy Act, by:

- adding a note to address what may amount to a *serious interference* in paragraph 13G(a) and adding that the provision applies to the privacy of one or more individuals; and

- deleting paragraph 13G(b) or as a minimum, deleting the reference to a *repeated act* or practice. This would address the fact that strictly speaking, many contraventions of the Privacy Act are potentially repeated in that the digital environment operates in real time and relies on systems and process that are by their nature repeatable (for example, providing inadequate notice to users of a platform in contravention of APP 5). Emphasis on types of harms to be avoided would better protect a consumer's right to privacy and provide certainty to relevant APP entities.