PRIVACY ACT REVIEW

SUBMISSION TO THE ATTORNEY-GENERAL'S DEPARTMENT

January 2022

EXECUTIVE SUMMARY

1. ANZ thanks the Attorney-General's Department (**AGD**) for the opportunity to comment on the *Privacy Act Review Discussion Paper* (**Discussion Paper**).

2. The ability to safely use data is fundamental to a vibrant digital economy. Data enables the development of new technologies like artificial intelligence (**AI**) and innovative products and services that enhance people's lives. The expansion of personal information captured in the digital economy also presents privacy risks and potential for adverse impacts. As the AGD reviews and resets Australia's privacy regime, we believe that the nation's policy should continue to involve the balancing of the protection of personal information with the facilitation of prudent data use. This balancing approach is consistent with reform ongoing in some other jurisdictions.

3. To achieve the appropriate balance and enable businesses to confidently and responsibly use data, the *Privacy Act 1988* (Cth) (**Act**) must set clear requirements for entities. Without clarity, an entity may fail to protect personal information appropriately and in accordance with the will of the Parliament. Equally, given the potential significant impact on customers and reputation, and increasing penalties under the Act, an entity cautiously interpreting ambiguous requirements may avoid using data altogether or to a degree short of what Parliament may have intended to be permissible.[1] This outcome would inhibit the societal and economic benefits that responsible data use can provide.

4. We note that more than three years following the introduction of the General Data Protection Regulation (**GDPR**) regime in the United Kingdom (**UK**) the UK government is consulting on reforms to reduce barriers to responsible innovation and to clarify aspects of the Act that 'continue to cause persistent uncertainty'.[2] The experience in the UK highlights the importance of setting clear requirements to support safe and responsible innovation.

5. To assist the AGD achieve its policy objectives, we have made some observations on selected proposals in the Discussion Paper. These comments are made within the context of our overall support for a strengthened privacy regime which is fit for the digital economy.

6. Our key points are summarised below. We set these points out in more detail in the section that follows the summary.

---

[1] We refer to the increased penalties detailed in the exposure draft *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021.*

[2] UK Department for Digital, Culture Media & Sport, *Data: A new direction*, 10 September 2021, p. 2

- **Ensure the objects of the Act are clear**

  Proposal 1.1(b)

  Section 2A(b) of the Act recognises that a balance is required between the public interest associated with protecting the privacy of individuals[3] and the public interest associated with permitting entities to carry out their functions and activities.[4] The Discussion Paper proposes to amend the objects of the Act by introducing a 'public interest' qualification for the 'functions and activities' of an entity to be balanced with protecting the privacy of individuals. This amendment introduces ambiguity concerning which functions or activities of an entity are undertaken in the public interest. As the objects of the Act can inform interpretation of substantive provisions and regulatory priorities, we suggest some clarifications for consideration if this proposal is adopted.

- **Provide clarity concerning the scope of information protected by the Act and consider the practical implications of 'singling out'**

  Proposal 2.2

  We support the intention underlying proposal 2.2 to clarify that specific types of technical information are *capable* of being personal information. Incorporating a list of types of technical information within the definition has potential drawbacks. It may be more appropriate to include this list in guidance together with examples of when certain technical information is, and is not, considered personal information.

  Proposal 2.3

  We support the proposal to define 'reasonably identifiable' as this could help to determine when information will be 'personal information'. We suggest the proposed definition of 'reasonably identifiable' would benefit from further clarification.

  If the definition of 'personal information' is expanded to include information that relates to an individual who can be distinguished from others, even where that individual's identity is not known (**singling out**), we would anticipate operational difficulties. Where an individual's identity is not known, practical compliance with some Australian Privacy Principles (**APPs**) will be challenging (eg where there is an obligation to communicate with an individual for whom there are no contact details) and, for others, will involve a high compliance cost but low privacy benefit. We recognise concerns that individuals

---

[3] See ALRC, *Serious Invasions of Privacy in the Digital Era 2014*, p. 32-33 for a discussion of the public interest in protecting privacy.

[4] The Discussion Paper, p. 19 notes that activities of commercial entities contribute to the economic wellbeing of the country.

'behind the device' could be at risk of manipulation and discrimination.[5] We suggest further consideration of how these concerns can be practically addressed.

Proposal 2.4

We support proposal 2.4 to update the definition of 'collection' to provide greater certainty as to when it captures inferred information.

Proposals 2.5 and 2.6

The Discussion Paper proposes that personal information be 'anonymous' (ie the risk of re-identification must be 'extremely remote or hypothetical') before it is no longer protected by the Act. We believe the current standard for information to be considered 'de-identified' as set out in guidance of the Office of the Australian Information Commissioner (**OAIC**) achieves an appropriate balance between protecting privacy and enabling data utility. This guidance provides that the risk of re-identification in the data access environment must be very low with no reasonable likelihood of re-identification of the information. We recognise that de-identifying personal information is technically complex and the use or release of poorly de-identified information gives rise to privacy risks. These risks could be addressed by proposal 2.6 to prohibit improper re-identification of data and measures to support robust de-identification practices.

The definition of 'sensitive information'

The Discussion Paper notes that submitters have raised concerns that 'sensitive information' could be inferred from financial transaction information. Where an entity infers 'sensitive information' from this information – for example, it forms an opinion that an individual has a medical condition from transactions with a doctor – the Act already provides that the entity has collected 'sensitive information'. This information would be subject to the additional protections that apply to 'sensitive information'. As such, we would ask the AGD to consider whether additional reform is needed in this area.

Proposal 2.4, if adopted, would further protect individuals in this regard by providing greater certainty that a 'collection' can include *inferred* information.

- **Promote more accessible collection notices**

Proposals 8.1 – 8.3

We support the intention underlying proposal 8.1 to make notices clearer and more accessible. We recommend that the proposed requirements for notices to be 'current' and 'understandable' are clarified if this proposal is adopted. We support the proposal to

[5] Discussion Paper, p. 23

make notices more targeted by limiting the matters a notice must address, the use of layered notices for digital channels and an optional standardised privacy language and framework for notices.

Proposal 8.4

We are concerned that proposal 8.4 may not be sufficiently flexible to permit entities to provide no notice where an entity collects, uses or discloses personal information on behalf of another entity. To provide this flexibility the existing 'reasonableness' test set out in APP 5.1(a) could be retained.

- **Consider how a 'fair and reasonable' test could be implemented that recognises the interests of entities in carrying out their functions and activities and avoids unnecessary complexity**

Proposals 10.1 and 10.2

We support the principle that the collection, use and disclosure of personal information be 'fair and reasonable'. However, applying an *overarching* 'fair and reasonable' test in addition to the existing APP requirements may require further consideration. The AGD could, as an alternative, revise the APPs to incorporate additional 'fair and reasonable' requirements. Carefully crafted, this could result in a single set of coherent privacy norms for entities to follow, rather than needing to apply the test independently from the APPs.

If an overarching test is adopted, the Act could include a list of functions and activities for which it is deemed 'fair and reasonable' to collect, use or disclose personal information (without the need for consent).

- **Require entities engaging in 'restricted practices' carrying higher risk to assess privacy impacts and mitigate privacy risks**

Proposal 11.1 – Option 1

We support the introduction of a requirement for entities engaging in certain 'restricted practices' which carry higher risk to assess privacy impacts and to implement measures to mitigate identified risks. The proposed list of restricted practices may benefit from further refinement as some of the listed practices do not appear to be inherently high risk.

7. We look forward to the next steps in the AGD's review and would welcome the opportunity to discuss the points in this submission with the Department if this would be useful.

DETAILED POINTS

Section 2A(b) 'Objects of this Act'

Proposal 1.1(b)

8. Proposal 1.1(b) would amend the objects of the Act in section 2A(b) '…to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest.'*[6] We appreciate the concerns underpinning this proposal.

9. The inclusion of the proposed amendment would suggest that there are some activities which are undertaken in the public interest and some which are not. The Discussion Paper notes that the public interest includes, '…regarding commercial entities, the economic wellbeing of the country'.[7] It is, however, not clear which functions and activities would be considered to be undertaken for the 'economic wellbeing of the country' as opposed to those that would not. This ambiguity could affect how the Act is interpreted.[8]

10. If a public interest qualification is incorporated into section 2A(b) of the Act, the Act could:

- Clarify what public interest matters will be balanced with individual privacy protection;
- Recognise the legitimate interests of entities in carrying out their functions and activities (we note that the GDPR recognises processing necessary for the purposes of legitimate interests of organisations as lawful except where those interests are overridden by an individuals' interests or fundamental rights and freedoms);[9] and
- Clarify what functions or activities of a commercial entity are considered to be *undertaken in the public interest*.

[6] Ibid, p. 20
[7] Discussion Paper, p. 19
[8] Under Section 15AA of the *Acts Interpretation Act 1901* (Cth), a statutory provision is to be interpreted in a way that best achieves the purpose or object of the statute.
[9] GDPR, Article 6

Provide clarity concerning the scope of information protected by the Act and consider the practical implications of extending to singling out

Proposal 2.2

11. The Discussion Paper proposes to include a non-exhaustive list of information types capable of being covered by the definition of personal information. This could help to clarify the specific types of technical data (eg location data) that may be caught by the definition.

12. We note that this type of approach may (1) not easily accommodate changing technology and (2) result in a tendency to treat this data as personal information without the required factual evaluation prescribed by the Grubb case.[10]

13. Instead, the definition could be supported by OAIC guidance providing examples of when different types of technical data are and are not regarded as (1) relating to an individual and (2) capable of reasonably identifying the individual. This could help to clarify that technical data must still meet these threshold tests before being considered personal information. Guidance can also be updated more easily to accommodate new types of technical data.

Proposal 2.3

14. The definition of 'personal information' triggers the operation of the Act. Determining whether data is personal information requires an assessment of whether the data is 'about an identified individual, or an individual who is reasonably identifiable.' A clear definition of 'reasonably identifiable' could therefore help in determining the application of the Act including when information will be 'de-identified' or 'anonymous'.[11]

15. The Discussion Paper proposes that '*An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly'.*[12] It also suggests that this definition could be supported by a list of objective factors within the Act to help entities assess whether an individual is 'reasonably identifiable'. This would include the context in which the

[10] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4, [63]. In this case the Federal Court clarified that determining whether information falls within the definition requires a factual evaluation as to whether (1) the information is about an individual (we note that the proposal to alter this test to 'relates to') and (2) the identity of the individual can be reasonably ascertained.

[11] If proposal 2.5 in the Discussion Paper is adopted the test will be 'anonymised' rather than 'de-identified'.

[12] Discussion Paper, p. 26

information is to be held or released, the costs and amount of time required for identification and available technology.[13]

16. We support the proposal to define 'reasonably identifiable'. We would make some observations that could help the AGD to develop the proposed definition.

- **What does 'identified, directly or indirectly' mean?**
  The Discussion Paper comments that this would clarify that an entity should consider other information available when assessing whether information is 'personal information'.[14] We consider that the existing definition of personal information works this way. However, the Discussion Paper also notes that submitters called for the Act to cover singling out and 'individuation'. These concepts are defined as the ability to 'single out a person in the crowd, *such that* they can be tracked, profiled, targeted, contacted or subject to a decision or action which impacts them, even if that individual's identity is not known' (our emphasis).[15] It is not clear whether 'identified, directly or indirectly' is intended to capture singling out. We comment on this further below.

- **Whose capability is to be considered?**
  Is capability to be assessed by reference to the means available to the specific collecting entity to identify an individual from the data (even though it may be identifiable in another entity's hands)?[16] We support retaining the existing position that where an entity discloses data that is personal information in its own hands but is not personal information in the hands of the receiving entity (because it has been de-identified) this is not a disclosure of personal information.[17] This position could be clarified in the law.

- **What is the threshold for *reasonably* identifiable?**
  The Discussion Paper notes that the '…definition would not capture information where there is only an extremely remote or hypothetical risk of identification'.[18] This implies a change to existing OAIC guidance that information is not captured where there is only a 'very low risk of identification'.[19] The Discussion Paper cites international case law that supports a 'very low risk' threshold rather than an 'extremely remote or hypothetical risk'

---

[13] Ibid, p. 27 - 28
[14] Ibid, p. 27
[15] Submission to the Issues Paper: Salinger Privacy, p. 5
[16] We note that the UK government is considering legislation to clarify that the test for anonymisation is a relative one following the Court of Justice of the European Union decision of *Breyer vs Germany*. See UK Department for Digital, Culture Media & Sport, *Data: A new direction*, 10 September 2021, p. 46
[17] The OAIC states that assessing whether information is about a reasonably identifiable individual requires a contextual consideration of the circumstances of the case including 'who will hold and have access to the information'. See *De-identification and the Privacy Act* March 2018, p. 8
[18] Discussion Paper, p. 27 - 28
[19] OAIC, *De-identification and the Privacy Act* March 2018, p. 4

threshold.[20] Our strong preference would be that the existing 'very low risk' standard is incorporated into the definition of 'reasonably identifiable'.

17. We recognise concerns that individuals 'behind the device' could be at risk of manipulation and discrimination.[21] Practically addressing these concerns is complex and likely requires further consideration. Below are some observations of challenges that may arise from extending the definition of 'reasonably identifiable' to capture singling out.

- **It isn't clear how an entity could practically comply with some APPs.**
  For example, what would be the appropriate response to an access or correction request or, if introduced, a right to objection or erasure, from an individual whose identity is not known? What authentication method should an entity implement to ensure that access is being provided to the correct singled out individual?

  There are also questions as to how accurately the 'consumer behind the device' can be singled out. Devices are often shared by multiple people in a household (eg sharing use of a computer or children accessing a parent's phone). Extending the APPs to singling out could have the unfortunate result of increasing surveillance (eg to monitor keystroke pattern and any authenticated environments visited) to reduce the risk of incorrectly disclosing the personal information of one household user to another.

  It is unlikely that an entity will be able to identify the same singled out user from one visit to an entity's website to the next. This would mean that notifications and, where necessary, consents would be required for each visit resulting in consumer frustration and notification / consent fatigue.

- **The cost of compliance with some APPs may outweigh the privacy benefit**.
  For example, the proposal would require collection notices to be provided to every singled out visitor to a website, and possibly consent sought to collect and use information from that website visitor. The UK government has observed that this type of requirement[22] has (1) diminished organisations' ability to collect data to improve their websites and services and (2) resulted in complaints by website users about the number of cookie pop-ups, with many people not engaging with privacy information and controls

---

[20] The Discussion Paper cites Canadian case law that held that there must be a 'serious possibility' of identification and UK case law that considered information to be ''identifiable' if a motivated intruder could identify someone from it, including by linking with other information' at p. 27. This case law is not consistent with an 'extremely remote or hypothetical risk of identification.'

[21] Discussion Paper, p. 23

[22] In the UK, the UK General Data Protection Regulation (**UK GDPR**) and the Privacy and Electronic Communications (EC Directive) Regulations (**PECR**) require data controllers to obtain consent to use analytics and tracking cookies. Consent is typically sought via pop-up notifications when a user visits a website or accesses a service. See UK Department for Digital, Culture Media & Sport, *Data: A new direction*, 10 September 2021, p. 75

because they wish to access the website. The UK government is consulting on possible responses including removing the requirement for consent to use analytics cookies based on the low impact to users' privacy and low risk of harm.[23]

- **De-identification techniques can compromise utility.**
  Expanding the definition of personal information in this way would require entities to apply more comprehensive de-identification techniques (eg aggregating the information to more generic data sets) for information to be considered de-identified under the Act. De-identification techniques can compromise the value of the data set for re-use, inhibiting innovation.

18. If the Act is amended to capture singling out, this type of 'personal information' would likely need its own regime of rules and constraints.

Proposal 2.4

19. We support proposal 2.4 to 'amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.'[24] We believe that inferred information applied to an identified individual's profile is already captured by the definition of personal information: it is an opinion about that person. The proposed amendment clarifies that the method of obtaining information does not impact whether it constitutes 'personal information'.

20. As previously submitted, it will be important to provide clarity as to when inferred information is 'collected' and becomes personal information relating to an identified individual.[25] We believe the collection occurs at the point that the opinion is formed. This means that when inferred information (such as an insight about a particular cohort of people) is applied to, or collected and held against, an individual's profile, the inference would be personal information.

[23] Organisations would still be required to provide clear information regarding cookies that are active on their device including the purpose of the use of the cookies. See UK Department for Digital, Culture Media & Sport, *Data: A new direction*, 10 September 2021, p. 75

[24] Discussion Paper, p. 28

[25] Submission to the Issues Paper: ANZ, p. 6

Proposal 2.5 and 2.6

21. Anonymising data involves applying de-identification techniques so that the information is no longer about an identifiable or reasonably identifiable individual.[26] Applying these techniques to information can impact its utility for re-use.[27] For example, a high level of aggregation can conceal important differences between and among subgroup categories that may cause the aggregated data to be misleading.

22. Current OAIC guidance provides that, to be considered de-identified, the risk of re-identification in the data access environment must be very low with no reasonable likelihood of re-identification of the information.[28] The Discussion Paper notes that 'information could be considered anonymous provided that the risk of re-identification was extremely remote or hypothetical'.[29] While we recognise this point raises the balance to be struck, requiring this higher standard of de-identification may impact data utility because it would require the application of more comprehensive de-identification techniques.

23. We recognise that current de-identification techniques can be inconsistent and lack the appropriate rigour. Consideration could be given to strengthening de-identification practices through legal standards, perhaps by drawing on the de-identification decision making framework issued by the OAIC and CSIRO's Data 61.[30] We also support proposal 2.6 to introduce a re-identification offence with appropriate amendments as a further safeguard against inappropriate re-identification.[31]

The definition of 'sensitive information'

24. The Discussion Paper asks what the benefits and risks would be of amending the definition of 'sensitive information' to include financial transaction data. It highlights concerns from submitters that 'sensitive information' can easily be inferred from financial data.[32]

25. The collection, use and disclosure of 'sensitive information' (ie personal information about particular matters such as health, race or political opinions) is subject to more rigorous requirements concerning collection, use and disclosure. This is because this information

---

[26] These techniques involve 'removal or replacing of direct identifiers in a dataset, followed by the application or any additional techniques or controls required to remove, obscure, aggregate, alter and/or protect data in some way', see OAIC and Data 61, *The De-Identification Decision-Making Framework*, 18 September 2017, p. 67

[27] OAIC, *De-identification and the Privacy Act* March 2018, p. 10

[28] Ibid, p. 3

[29] Discussion Paper, p. 30-31

[30] OAIC and Data61, *The De-identification Decision-Making Framework*, 18 September 2017

[31] Submission to the Issues Paper: ANZ, p. 12

[32] Discussion Paper, p. 34

carries greater risk of harm (such as discrimination) if misused. However, APPs 8 (concerning cross-border disclosure of personal information) and 11 (concerning security of personal information) do not prescribe different requirements for 'sensitive information'. While the sensitivity of the personal information to be protected will be a consideration in determining what 'steps are reasonable in the circumstances' under these APPs, all personal information, including 'sensitive information', must be appropriately secured.

26. The 'raw' financial transaction data of an individual is personal information about payments made or received by that individual; it is not per se 'sensitive information'. For example, if an individual makes a payment to a medical provider that is not, per se, information or an opinion about that individual's health. Submitters have raised concerns that 'sensitive information' could be *inferred* from a payment. In this case, information about the health of an individual could be inferred from a payment to a medical provider.[33]

27. We believe that the additional protections sought by submitters for 'sensitive information' (ie information *inferred* through positive steps from raw financial transaction data and applied to an individual's profile) are already provided under the Act. For example, transaction information may include subscriptions to political organisations. Alone, this raw data is personal information but not sensitive information. However, if an entity forms an opinion from this information (eg through the use of analytics) that the account holder holds particular political opinions, this opinion would be a collection of 'sensitive information' and subject to the additional protections set out in the Act. [34] Proposal 2.4 (which we support) would, if adopted, further clarify that an inference applied to an individual's profile is a collection under the Act.[35]

28. If the definition of 'sensitive information' was amended to include financial information, the normal operation of the payment system and commerce would require much more explicit and granular consents. Financial system participants (eg banks, credit card schemes, merchants, payment intermediaries and fraud monitoring service providers) would require consumers' consent to process payment information. This could result in consent fatigue for consumers and a significant compliance burden for financial system participants with minimal privacy benefit.

---

[33] Ibid, p. 34

[34] We note this is unlikely to be a reliable inference as payment of a political membership may be on behalf of someone else who is not identified.

[35] Ibid, p. 28

Promote more accessible collection notices

29. Clear, accessible, timely notice helps individuals understand how, why and what data is being captured about them. This transparency underpins individuals' trust and confidence in the organisations they choose to engage with. Privacy notices should be clear and concise, appropriate to the particular delivery channel (eg mobile app) and provide opportunity to obtain more detail as required.

30. Proposals 8.1 to 8.3 could help to make privacy notices more accessible. To assist development of these proposals and effective compliance, we have made some observations concerning their implementation.

Proposal 8.1

31. The Discussion Paper proposes to introduce an express requirement that APP 5 notices 'must be clear, current and understandable'. This proposal has been made in response to submitters' legitimate concerns that entities have significant discretion concerning how APP 5 notices are provided.[36] We support this proposal in principle. However, the proposed requirement for notices to be 'current and understandable' may be unclear. For example:

    - The term 'current' when applied to the ongoing collection, use and disclosure of information could mean:
        - A notification continues to be accurate;
        - Notice is updated at regular intervals;
        - Notice is provided at each collection; or
        - Any consent provided has not been withdrawn.

      In the context of a banking relationship, with ongoing collection of personal information over a long period of time, notification provided when the relationship commences should be 'current' while it continues to be accurate. Updating this information at regular intervals or at each collection would likely result in notification fatigue.

    - 'Understandable' may be satisfied through the use of plain English, or it may require holistic subjective assessment of the importance, audience, volume and

[36] Discussion Paper, p. 68

format of information to be provided in the context of a particular channel (eg a mobile app).

32. We recommend that these requirements are clarified if this proposal is adopted. Alternatively, the OAIC's recommendation that notices must be 'concise, transparent, intelligible and written in clear and plain language'[37] is clear and unambiguous and therefore may more effectively address the concerns raised.

Proposal 8.2

33. We support the proposal to reduce the number of matters that APP 5 collection notices must address. While comprehensive notices may be considered more transparent, long notices can overwhelm customers. Shorter, concise notices are more likely to be accessible and fulfil their purpose.

34. The Discussion Paper notes that limiting notification matters per proposal 8.2, 'may also promote the adoption of layered approaches to the provision of privacy information'.[38] While proposal 8.2 apparently permits a notification to link to a privacy policy when addressing 'the location of the entity's privacy policy which sets out further information', it is not clear that an entity can layer privacy information regarding other listed notification matters.

35. Layered notices offer the advantage of efficient and more targeted disclosure, allowing consumers to view higher level information about, for instance, purposes for collection, secondary purposes and third party disclosures, with the ability to 'click through' to more detailed information about areas of particular interest.

36. Layering notice information can promote customer understanding, particularly in digital channels, where they can enable efficient, more targeted disclosure. To avoid concerns that reading the full notice requires too many 'clicks', the 'top layer' of a layered notice could offer the opportunity to 'read the collection notice in full'.

37. APP 5 requires entities to either 'notify the individual' of the relevant matters or 'otherwise ensure that the individual is aware' of any such matters. We do not believe this requirement is flexible enough to permit the use of layered notices. This is because the obligation is to either notify them upfront, or *ensure they are aware*. To enable a layered approach, we recommend that APP 5 permits the use of layered notices by an entity. APP 5 could make it explicit that providing a link to information may satisfy the obligation to ensure the

[37] Submission to the Issues Paper: Office of the Australian Information Commissioner, p. 74
[38] Ibid, p. 70

individual has been made aware of the relevant matters (subject to meeting any requirement that notices be clear and understandable as set out in proposal 8.1) even though the individual may choose not to access it.

38. Proposal 8.2 describes the matters to be addressed by a notice including 'if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection'. We recommend that this requirement is modified so that the notice addresses the *types* of entities that personal information is collected from and the circumstances of that collection (eg a notice could provide that a bank collects personal information from brokers who may have introduced the individual to the bank). To require the specific third party entity to be identified and the specific circumstances of the collection described would require bespoke notices to be provided to individuals at the point of each collection. This is impractical and would potentially result in a consumer receiving multiple notices in the course of a single application for a financial product resulting in notification fatigue. For example, when applying for a credit product information may be collected from brokers, other credit providers and credit reporting bodies. It will not necessarily be clear at the commencement of an engagement which specific entities a bank will collect information from.

Proposal 8.3

39. We support the development of an optional standardised privacy language and framework for notices informed by broad customer experience testing. As previously submitted, this would have the dual benefits of making notices more intelligible for individuals and providing more certainty for business regarding notice requirements, both in terms of wording and structure of required notices.

40. We suggest that adopting a standardised approach should be voluntary to avoid creating barriers to innovative approaches to notice suited to different channels. Where an entity elects not to adopt a standardised approach it must still meet the overarching requirements of APP 5.

41. The Discussion Paper suggests that a standardised language and framework could be developed on a sector-specific basis.[39] We support this approach. The financial sector collects, uses and discloses information to deliver highly regulated products and services.[40]

[39] Discussion Paper, p. 71

[40] Banks use personal information to meet a range of regulatory obligations including for example anti-money laundering and counter terrorism financing obligations under the *Anti-money Laundering and Counter-terrorism Financing Act 2006* (Cth), responsible lending obligations under the *National Consumer Credit Protection Act 2009* (Cth) and design and distribution obligations under the *Corporations Act 2001* (Cth).

The development of a financial sector collection notice language and framework could clearly address specific collections, uses and disclosures of personal information common to the sector in a more accessible and consistent way.

Proposal 8.4

42. The Discussion Paper asks whether proposal 8.4 is sufficiently flexible to permit entities to provide no notice where an entity collects, uses or discloses personal information (**Entity A**) on behalf of another entity (**Entity B**). We are concerned that the proposal may not clearly provide this flexibility.

43. The proposal provides two exceptions to the requirement to notify:

- If the individual has already been made aware of the APP 5 matters (**Exception 1**); or
- Notification would be *impossible* or would involve *disproportionate effort* (**Exception 2**).[41]

44. Exception 1 is not clear about when prior notification of APP 5 matters will be sufficient to avoid the need for multiple notices where Entity A collects, uses or discloses personal information on behalf of Entity B. We would note that it does not address:

- The level of detail to be provided by Entity B regarding the APP 5 matters; and
- The circumstances in which that detail should specifically reference Entity A, Entity B or both Entity A and Entity B. For example, it is not clear whether Entity A would need to provide notification of the identity and privacy policy details of both Entity A and Entity B to avoid the need for subsequent notice by Entity B. We suggest such a requirement is likely to make notices more complicated.

45. Exception 2 is available either where:

- It is *impossible* to notify (there are limited situations where this test will be met); or

[41] Discussion Paper, p. 73

- Notification would involve *disproportionate effort* (there may be situations where providing a further notice is confusing or results in notification fatigue even though it does not involve disproportionate effort).

46. To retain sufficient flexibility Exception 1 could retain the existing 'reasonableness' test set out in APP 5.1(a). This test provides the flexibility to consider whether further notification from Entity B is necessary for transparency in the context of the associated privacy risks.

47. Separately, there are a range of situations where an individual will provide the personal information of another individual to a bank (eg to make a payment). Where the information is used only for a primary purpose or other permitted purpose and there is low privacy impact (in this case making a payment and preventing fraud), a collection notification from the bank while *possible* and not involving *disproportionate effort* may serve little purpose and result in notification fatigue. The 'reasonableness' test set out in APP 5.1(a) also provides flexibility regarding notification in these circumstances.

Consider how a 'fair and reasonable' test could be implemented that recognises the interests of entities in carrying out their functions and activities and avoids unnecessary complexity

Proposals 10.1 and 10.2

48. The Discussion Paper proposes to incorporate an overarching requirement that 'a collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.'[42] Proposal 10.2 suggests that a list of factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances be incorporated into the Act (**List of factors**).

49. We support the principle that the collection, use and disclosure of personal information be fair and reasonable in the circumstances. Applying an overarching 'fair and reasonable' test in addition to the existing APP requirements may require further consideration to avoid potential duplication, complexity and ambiguity. A possible alternative to an *overarching* test could be to revise the APPs to incorporate additional 'fair and reasonable' requirements. Carefully crafted, this could result in a single set of coherent privacy norms for entities to follow, rather than needing to apply the test independently from the APPs.

50. The objects of the Act include promoting the protection of individuals' privacy, balancing protection of individuals' privacy with entities' interests in carrying out their functions and

[42] Ibid, p. 85

activities and promoting responsible and transparent handling of personal information by entities.[43] These objects align with ensuring entities' collection, use and disclosure of personal information is 'fair and reasonable'. This is evident in the alignment between the existing APP requirements and the proposed List of factors intended to support a decision as to whether handling is 'fair and reasonable' shown in Table 1.

Table 1: Comparison of List of factors and existing APP requirements

List of factors	Existing APP requirements
Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (**Reasonable expectations**)	APP 5 describes notification requirements concerning the purposes for which an entity collects personal information and usual disclosures of personal information APP 6 describes requirements concerning secondary uses and disclosures that the individual would reasonably expect including more limited secondary uses and disclosures for 'sensitive information'
The sensitivity and amount of personal information being collected, used or disclosed	APP 3 describes requirements concerning how ('only by lawful and fair means') and what (must be 'reasonably necessary for one or more of the entity's functions or activities') information may be collected including specific requirements for 'sensitive information'
Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information	APP 3 and 6 describe more onerous requirements (including obtaining consent) when handling 'sensitive information' that by its nature may put an individual at foreseeable risk of unjustified adverse impacts or harm

[43] Sections 2A(a), (b) and (d) of the Act.

List of factors	Existing APP requirements
Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity	APP 3 requires that only personal information 'reasonably necessary for one or more of the entity's functions or activities' may be collected
Whether the individual's loss of privacy is proportionate to the benefits	APP 5 describes notification requirements that enable an individual to elect not to engage with an entity if they consider that their loss of privacy outweighs the benefits APP 3 and 6 describe more onerous requirements (including obtaining consent) when handling 'sensitive information' that by its nature may put an individual at foreseeable risk of unjustified adverse impacts or harm
The transparency of the collection, use or disclosure of the personal information	APP 5 describes notification requirements including when notice is required and the matters to be addressed in the notice
If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child (**Best interests of the child**)	

51. Any proposed collection, use or disclosure of personal information must be assessed against each APP requirement. If an overarching 'fair and reasonable' test is incorporated, it would require any proposal to be further assessed under that test by reference to the List of factors. It is not clear whether a proposal that meets the existing APP requirements would also meet the 'fair and reasonable' test. For example, if a proposal meets the APP 5 requirements to notify the individual and the APP 6 requirement that use for a secondary purpose must be within the reasonable expectations of the individual, it is not clear whether this proposal also satisfies the 'reasonable expectations' factor in the List of factors. If the answer is yes, the test has little effect. If it is no, an alternative to an overarching test could be to amend APP 5 and APP 6 to clearly prescribe what more is required. Similarly, with the

remaining List of factors, to the extent that the relevant APP is considered inadequate or, as in the case of the Best interests of the child factor, there is no relevant APP, the relevant APP could be amended (or introduced) rather than applying an overarching test. This approach could provide greater clarity and so support compliance.

52. If an overarching 'fair and reasonable' test is incorporated into the Act, we offer the following observations for the development of the List of factors.

- **Common 'reasonably necessary functions and activities' could be listed.** The List of factors could include a list of functions and activities for which it is deemed 'fair and reasonable' to collect, use or disclose personal information (without the need for consent) to provide clarity to entities applying the test and support effective compliance.

  The UK now has more than three years of experience of a strengthened GDPR based data protection regime. The UK government has observed uncertainty as to the lawful grounds that allow processing of data under the UK GDPR (including the lawful ground of legitimate interests under Article 6(1)(f)) may have resulted in an over-reliance on consent and consequently consent fatigue.[44] In response, the UK government proposes to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without the need to show that the processing is necessary and outweighs the rights of data subjects.

  The proposed list includes processing activities necessary for:

  a) "Reporting of criminal acts or safeguarding concerns to appropriate authorities

  b) Delivering statutory public communications and public health and safety messages by non-public bodies

  c) Monitoring, detecting or correcting bias in relation to developing AI systems

  d) Using audience measurement cookies or similar technologies to improve web pages that frequently visited by service users

  e) Improving or reviewing an organisation's system or network security

  f) Improving the safety of a product or a service that the organisation provides or delivers

[44] UK Department for Digital, Culture Media & Sport, *Data: A new direction,* 10 September 2021, p. 21

g) De-identifying personal data through pseudonymisation or anonymisation to to [sic] improve data security

h) Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers

i) Managing or maintaining a database to ensure that records of individuals are accurate and up to date, and to avoid unnecessary duplication".[45]

In addition to 'legitimate interests', other permitted reasons for processing personal data under the UK's GDPR based regime include processing:

- Necessary for the performance of a contract;
- To support compliance with a legal obligation imposed on the entity;
- To perform a task carried out in the public interest.[46]

Australia can draw on this UK experience and these other permitted reasons for processing under the GDPR in considering reforms that appropriately balance protection of personal information with the facilitation of prudent data use. A similar list of activities and permitted reasons could be included in the List of factors with supporting OAIC guidance. This would provide certainty to entities that they can lawfully continue to use personal information for important business functions.

- **Detailed guidance could be provided to support assessment under the List of factors.**
  For example, guidance could address how an entity should assess whether 'loss of privacy is proportionate to the benefits'; whether 'benefits' include public benefits and benefits to the entity, as well as benefits to the individual; and how an entity should proceed where it has limited information to assess matters such as benefit to the individual or the best interests of the child (including whether the entity should seek further personal information from the individual or child to enable this assessment).

[45] Ibid, p. 22 - 23
[46] GDPR, Article 6

Require entities engaging in 'restricted practices' to assess privacy impacts and mitigate risks

Proposal 11.1

53. The Discussion Paper proposes two options for strengthening privacy protections where entities engage in certain restricted practices carrying higher risk. Option one would require that an entity engaging in restricted practices take reasonable steps to identify privacy risks and implement measures to mitigate those risks. OAIC guidance concerning reasonable steps and mitigation measures would be helpful to support this requirement.

54. We support option one as it promotes 'privacy by design' by placing the burden of assessing and mitigating privacy risks on entities. Option two places the burden on individuals to assess potentially complex privacy risks by requiring consent for restricted practices.

55. The proposed list of restricted practices may benefit from further refinement as some of the listed practices do not appear to be inherently high risk. For example:

    - 'Direct marketing on a large scale' could include emailing all credit card customers (where direct marketing is permitted) with a rewards or points related offer;
    - 'The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale' could include any large scale marketing activity including television advertising, informed by analysis of customers' pseudonymised personal information relating to their use of products.

56. Article 35 of the GDPR sets out characteristics of high risk processing that requires a data protection impact assessment. It focuses on a type of processing *in particular using new technologies* that, having regard to the nature, scope, context and purposes of processing, is likely to result in a high risk to the rights and freedoms of individuals.[47] Reference to certain characteristics of high risk processing could better inform the list of 'restricted practices' rather than listing practices alone.

ENDS

[47] GDPR, Article 35