



Australian Banking  
Association

17 December 2021

Attorney-General's Department  
4 National Circuit  
BARTON ACT 2600

By email: [Privacyactreview@ag.gov.au](mailto:Privacyactreview@ag.gov.au)

## Privacy Act Review – Discussion paper

The Australian Banking Association (**ABA**) welcomes the opportunity to make a submission to the Attorney-General's Department (**AGD**) Discussion Paper. The Discussion Paper represents the latest step in the ongoing review of the *Privacy Act 1988 (Cth)* (**Privacy Act**).

### Our position

The Privacy Act review is a once-in a generation opportunity to improve our nation's information economy to support responsible innovation while empowering and protecting individuals.

Information is now the driving force of the global economy. Access to information through the digital economy has brought with it immense benefits including new and better products and services. The fact that governments and businesses were able to share data efficiently and ethically during the pandemic has saved lives and kept the economy running during a period of unprecedented disruption.

However, the need to provide banking and other services without face-to-face contact during the pandemic has also highlighted a requirement for clarity about responsible use of information. As Australians spend more of their time online, and innovative technologies emerge, more personal information (**PI**) about individuals is being captured and processed.

The use of this information is often limited by barriers to its access; including when access rights are unclear or when organisations cannot make effective use of the data they already have. These barriers undermine the performance of public services and our economy, risking poorer outcomes for individuals.

The Privacy Review is a timely opportunity to consider what information should and should not be made available and in what circumstances. By setting out a framework for the collection, use, and disclosure of personal information, emerging technology and uses can be developed safely while maintaining consumer confidence.

The ABA supports an approach to information privacy that harnesses all the potential benefits of data when it is used responsibly, while protecting data that can negatively impact society and individuals.



## Key issues

The ABA highlights the following key issues regarding the proposals in the Discussion paper.

### 1. Objects of the Act

The Government's approach to privacy of information affects the ease, costs, and risks of developing innovative technologies and services. The Objects of the Act should allow for innovators and entrepreneurs to use data responsibly and securely, without undue regulatory uncertainty or risk, to drive growth across the economy.

The ABA considers that the proposed insertion of a public interest test in subsection 2A(b) of the Privacy Act would disrupt this longstanding balance, tipping the scales towards the privacy interests of an individual where APP entities<sup>1</sup> collect, use, and disclose personal information for their own legitimate commercial purposes. We submit that the current iteration of the Act's objects strikes a better balance between the privacy of individuals and the legitimate commercial interest of APP entities in the collection, use and disclosure of personal information.

### 2. Personal information – reasonably identifiable test

The proposed addition that "an individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly" must be accompanied by clear regulatory guidance as to how this test is to be applied in practice.

The ABA suggests that this guidance should err on the side that information is 'identifiable' if there is a reasonably serious probability of a particular individual being identified from it (rather than a lower standard of individuation). This is important for the regime to protect the privacy of information that could negatively impact society and individuals, while reducing barriers to access for data that could spur innovation.

### 3. Definition of sensitive information

The discussion paper contemplates whether the current scope of sensitive information is adequate, or whether it should be expanded to include other types of personal information such as transaction data. The ABA considers that such an expansion would not be appropriate and would significantly impede ordinary banking services to the detriment of our customers.

### 4. Deidentified and anonymous information

The Discussion Paper proposes to require personal information to be anonymous before it is no longer protected by the Act. The ABA respectfully disagrees with the proposed change. We submit that data should not be considered personal information once it has been de-identified.

It is not clear to us why the terminology of de-identification would not remain fit-for-purpose if and when the scope of information that may reasonably identify an individual is broadened. 'De-identification' is well understood by industry and data technologists, whereas a substitution of the term may create confusion for these participants as to the proposed policy intent.

### 5. Collection, use and disclosure of personal information must be fair and reasonable

The ABA is supportive of the principle that the collection, use and disclosure of personal information be fair, within individuals' reasonable expectations, and that it does not cause them harm. However, we consider that this fairness principle already underlies many of the existing provisions of the Privacy Act, alongside the other proposals put forward in the Discussion Paper.

We ask the Government to clarify how it would envisage the new provision would operate alongside the other provisions of the Act.

---

<sup>1</sup> An APP entity is either a government agency or an organization that must comply with the Privacy Act.



## 6. Defining primary and secondary purposes in APPs 3 and 6

The proposal to limit secondary purposes to activities that are 'directly related' to the primary purpose of collection is unnecessarily restrictive. The result may be that purposes that are reasonable and expected from a societal or organisation perspective are no longer undertaken.

In addition, this proposal will not achieve its intended purpose of improving transparency and could have unintended consequences. For example, an unintended consequence may include entities adopting vague and broad descriptions for each primary purpose to capture potential or unclear future uses or disclosures.

## 7. Vulnerable individuals

The ABA has spent considerable time working with the OAIC to map rules to assist banks when they are handling the personal information of customers experiencing vulnerability. We have concluded there are limited circumstances when banks can use or disclose personal information for the purposes of taking extra care of customers without explicit and informed consent.

The ABA believes that the current review should consider an amendment to the Privacy Act that allows for 'good faith' disclosure of information for circumstances where an individual's financial safety may be compromised. This would be in line with the operation of the UK regime.


## 8. Right to erasure

The ABA supports the right to erasure in a defined manner. However, consistent with the approach applied under GDPR, this right should not be absolute.

The Act should allow an APP entity to refuse a request in whole or in part in circumstances in which the interests or obligations of the APP entity, or the public interest, outweigh an individual's privacy interests. The introduction of clear principles outlining when an individual can request the erasure or destruction of their personal information should balance customer fairness with business requirements.

## 9. The benefit of OAIC guidance

Finally, in this submission, and with the context of a constantly evolving information environment, the ABA highlights at multiple points that the OAIC could provide further and specific guidance rather than embedding the detail in the Privacy Act. Frequently issued and updated guidelines will enable the privacy protection practices of banks (and all other industry sectors) to remain current and fit-for-purpose.

Further comments on the consultation materials are provided in Appendices A to D of this letter. 

Kind regards



Jess Boddington  
Policy Director, Australian Banking Association

## About the ABA

The Australian Banking Association advocates for a strong, competitive, and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

## Table of contents

The ABA's feedback is organised in the following appendices to this letter.

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| Appendix A: Summary of ABA recommendations .....                                             | 6  |
| Appendix B: Scope and application of the Act .....                                           | 9  |
| 1. Objects of the Act .....                                                                  | 9  |
| 2. Personal information, de-identification, and sensitive information .....                  | 9  |
| 2.1 Personal information .....                                                               | 9  |
| 2.2 De-identified, anonymised and pseudonymised information .....                            | 11 |
| 2.3 Definition of sensitive information .....                                                | 11 |
| 3. Employee records exemption .....                                                          | 12 |
| Appendix C: Protections .....                                                                | 13 |
| 4. Notice of collection of personal information .....                                        | 13 |
| 4.1 APP 5 notices to be clear, current, and understandable .....                             | 13 |
| 4.2 Clarifying the interaction between privacy notices and privacy policies .....            | 13 |
| 4.3 Standardisation of APP 5 notices .....                                                   | 14 |
| 4.4 Expanding the situations where notice is required .....                                  | 14 |
| 5. Consent to the collection, use and disclosure of personal information .....               | 15 |
| 5.1 Strengthening what is required to demonstrate consent .....                              | 15 |
| 5.2 Standardisation of consent requests .....                                                | 15 |
| 6. Additional protections for collection, use and disclosure of personal information .....   | 16 |
| 6.1 Collection, use and disclosure of personal information must be fair and reasonable ..... | 16 |
| 6.2 Factors relevant to the fair and reasonable requirement .....                            | 16 |
| 6.3 Additional requirements in APPs 3 and 6 - requirement on third party collections .....   | 17 |
| 6.4 Additional requirements in APPs 3 and 6 - define primary and secondary purposes .....    | 18 |
| 7. Restricted practices .....                                                                | 18 |
| 8. Pro-privacy default settings .....                                                        | 20 |
| 9. Children and vulnerable individuals .....                                                 | 20 |
| 9.1 Children's privacy .....                                                                 | 20 |
| 9.2 Vulnerable individuals' privacy .....                                                    | 21 |
| 10. Right to object and portability .....                                                    | 22 |
| 11. Right to erasure of personal information .....                                           | 23 |
| 11.1 Introduce a right to erasure on certain grounds .....                                   | 23 |
| 11.2 Exceptions to a right of erasure .....                                                  | 24 |
| 11.3 Include a process for responding to erasure requests .....                              | 25 |
| 12. Direct marketing, targeted advertising, and profiling .....                              | 25 |



|                                             |                                                                                          |    |
|---------------------------------------------|------------------------------------------------------------------------------------------|----|
| 12.1                                        | Unqualified right to object to collection, use and disclosure for direct marketing ..... | 25 |
| 12.2                                        | Influencing an individual's behaviour or decisions must be a primary purpose.....        | 26 |
| 12.3                                        | Remove APP 7 considering other proposals for reform .....                                | 26 |
| 13.                                         | Automated decision-making .....                                                          | 26 |
| 14.                                         | Security and destruction of personal information .....                                   | 27 |
| 14.1                                        | Clarify what reasonable steps may require.....                                           | 27 |
| 14.2                                        | Strengthen destruction requirements.....                                                 | 27 |
| 15.                                         | Overseas data flows .....                                                                | 28 |
| 15.1                                        | Introduce standard contractual clauses (SCCs) .....                                      | 28 |
| 15.2                                        | Strengthen notice requirements.....                                                      | 28 |
| 15.3                                        | Obligations apply only to 'disclosures' .....                                            | 29 |
| 16.                                         | Cross Border Privacy Rules and domestic certification .....                              | 29 |
| Appendix D: Regulation and enforcement..... |                                                                                          | 30 |
| 17.                                         | Enforcement .....                                                                        | 30 |
| 18.                                         | Notifiable Data Breaches scheme .....                                                    | 30 |
| 19.                                         | Interactions with other schemes.....                                                     | 30 |



## Appendix A: Summary of ABA recommendations

Please see the other appendices for a detailed explanation of each recommendation.

### Recommendations

#### *Scope and application of the Act*

- 1.1 The ABA does not support inserting 'undertaken in the public interest' into the Objects of Act.
- 2.1 The ABA is supportive of the proposals to amend the definition of personal information to clarify that it includes technical and inferred information, and to expand the definition of collection to expressly cover inferred information.
- 2.2 Instead of including a list of technical information that is personal information within the Act:
  - a. the OAIC should update its existing guidance '*What is personal information*' to include an up-to-date list of technical information.
  - b. the explanatory memorandum should elaborate on the types of technical information that would be captured as personal information.
- 2.3 It should be clarified that information is 'identifiable' if there is a reasonably serious probability of a particular individual being identified from it (rather than a lower standard of individuation).
- 2.4 Instead of including a list of objective factors relating to determining when an individual is reasonably identifiable within the Act, the OAIC should provide regulatory guidance on the matter after consultation with key stakeholders.
- 2.5 The current standard should remain that, once information is de-identified, it is no longer personal information.
- 2.6 The current definition of sensitive information is fit for purpose. It captures financial information or transaction data as sensitive information in circumstances where there is a clear implication the transaction relates to matters under the definition of sensitive information.
- 3.1 The ABA supports in principle modifying the employee exemption to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship.

#### *Protections*

- 4.1 We support in principle a requirement that privacy notices must be clear, current, and understandable.
- 4.2 The ABA is supportive of the intent to reduce the scope of matters listed in APP 5 notices.
- 4.3 The provision of examples of standardised privacy notices that could be used would be helpful, subject to extensive consumer testing and a transition period.
- 4.4 Regarding the proposed requirement to strengthen and expand the situations where an APP 5 collection notice is required, the ABA suggests that the terms 'impossible' and 'disproportionate effect' should be substituted with meaningful alternatives.
- 5.1 The ABA supports in principle consent being defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.
- 5.2 The standardisation of consent taxonomies, icons or phrases in consent requests could be useful. However, care will need to be taken that the use of such tools does not oversimplify consent requests.
- 6.1 We seek further information to explain the intended operation of the fair and reasonable test under APPs 3 and 6.



- 6.2 If requirements of collection and handling being fair and reasonable are introduced, we agree that greater guidance would need to be provided in relation to the meaning of fair and reasonable in a privacy context.
- 6.3 The proposal to introduce a due-diligence requirement on third-party collections needs more consideration to ensure that it does not interfere with reasonable and required business processes, such as credit checks or identity verification checks.
- 6.4 The ABA is not supportive of the proposal to redefine primary and secondary purposes in APP 3 and APP 6.
- 7.1 The ABA supports the proposed approach that entities engaged in certain high-risk activities should be required to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks in a flexible and scalable way.
- 7.2 The ABA submits that general direct marketing to an existing customer base that would reasonably expect their personal information to be used or disclosed for the purposes of such marketing, and that does not involve privacy-intrusive practices, should not be characterised as a restricted practice. If direct marketing is to be designated as a restricted practice, the Government should seek policy alignment between the relevant regulators as to how restricted practices are defined in the relevant Acts and regulations.
- 9.1 The ABA is not supportive of a broad approach that amends the Act to require consent to be provided by a parent or guardian where a child is under the age of 16.
- 9.2 The ABA believes that the current review should consider an amendment to the Privacy Act that permits 'good faith' disclosure of information to law enforcement or adult safeguarding authorities in circumstances when an individual's financial safety may be compromised, without a requirement to obtain express consent from such individuals.
- 10.1 If a right to object to the collection, use or disclosure of personal information is introduced, specific exceptions need to be considered where this right would not apply.
- 11.1 The right to erasure of personal information must be qualified by well-defined exceptions that allow APP entities to refuse to comply with a request (in whole or in part) in certain circumstances.
- 11.2 The right to erasure must be limited to a best endeavours obligation, with APP entities also allowed to comply with any erasure request by de-identifying the relevant personal information.
- 11.3 We would support detailed consultation and guidance on exceptions to the right of erasure, including in circumstances where erasure is technically impractical or an unreasonable burden to erase an individuals' personal information.
- 11.4 The ABA supports in principle the requirement for APP entities to respond to an erasure request within a reasonable period.
- 12.1 We strongly advocate for alignment between the existing legislation and Australian regulators to ensure consistency in requirements for direct marketing activities.
- 12.2 Implementing a global opt-out process will result in a significant and adverse impact on user experience and may be impossible to achieve in certain situations.
- 13.1 The ABA supports this proposal to require privacy policies to include information on whether personal information will be used in relevant automated decision-making
- 14.1 Instead of including a list of factors in the Act that indicate what reasonable steps may be required to protect information, the OAIC should update its existing guidance 'Guide to securing personal information.
- 14.2 The ABA does not support amending APP 11.2 to require APP entities to take all reasonable steps to destroy or anonymise relevant information.
- 15.1 The ABA is supportive of the inclusion of SCCs provided they are not mandatory, nor the only means by which to provide for overseas data flows.



15.2 Notice requirements do not need to be strengthened in relation to potential overseas disclosures.

15.3 The circumstances relevant to determining what 'reasonable steps' are for the purpose of APP 8.1 should be contained in OAIC guidelines.

16.1 The ABA conditionally supports the implementation of a voluntary domestic privacy certification scheme and welcomes alignment with the CBPR system and other established schemes worldwide.

*Regulation and enforcement*

18.1 Subsections 26WK(3) and 26WR(4) of the Notifiable Data Breaches scheme should not be amended.

19.1 The ABA supports in principle the recommendations to strengthen privacy harmonisation across State and Commonwealth agencies.



## Appendix B: Scope and application of the Act

### 1. Objects of the Act

#### AGD proposal:

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

- ...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*.

The Privacy Act is currently based on the notion that the privacy of an individual is not absolute and that its protection must be balanced against an entity's legitimate interest in the collection, use and disclosure of personal information. Although the discussion paper makes brief reference to the 'public interest' as extending to the 'economic wellbeing of the country,' the ABA considers that the proposed insertion of a public interest test would disrupt this longstanding balance.

It would tip the scales towards the privacy interests of an individual where APP entities<sup>2</sup> collect, use, and disclose personal information for their own legitimate commercial purposes. Instead, the ABA submits that the current iteration of the Act's objects strikes a better balance between the privacy of individuals and the legitimate commercial interest of APP entities in the collection, use and disclosure of personal information.

Information is the driving force of the modern economy. The Government's approach to privacy of information therefore affects the ease, costs, and risks of developing innovative technologies and services. If the Government is not minded to retain the current wording in section 2A, then it is our view that the Act should not seek to impose a standard of 'public interest' that is too burdensome for the average company to develop new products and services. Rather, the Objects of the Act should allow for innovators and entrepreneurs to use data responsibly and securely, without undue regulatory uncertainty or risk, to drive growth across the economy.

#### ABA recommendation:

1.1 The ABA does not support inserting 'undertaken in the public interest' into the Objects of Act.

### 2. Personal information, de-identification, and sensitive information

#### 2.1 Personal information

#### AGD proposal:

2.1-2.3 Amend the definition of personal information to make clear that it includes technical and inferred personal information. This definition would be supported by the following amendments to the Act:

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information
- a list of objective factors to assist APP entities to determine when an individual is reasonably identifiable, and
- a definition of 'collection' that expressly covers inferred information.

##### 2.1.1. Inferred and technical personal information

The ABA is supportive of the proposals to:

- amend the definition of personal information to clarify that it may include technical and inferred information depending on whether the information reasonably identifies an individual<sup>3</sup>, and

<sup>2</sup> An APP entity is either a government agency or an organization that must comply with the Privacy Act.

<sup>3</sup> Inferred personal information being information collated from a number of sources which reveals something new about an individual.



- to expand the definition of collection to expressly cover inferred information.

Indeed, we interpret the current definition as including technical and inferred information, to the extent it is information or an opinion about an identified individual or an individual who is reasonably identifiable. As outlined in the Discussion Paper, information is ‘inferred’ and enlivened as personal information under the Privacy Act at the point the entity collects it for inclusion in a record or generally available publication.

**ABA recommendation:**

2.1 The ABA is supportive of the proposals to amend the definition of personal information to clarify that it includes technical and inferred information, and to expand the definition of collection to expressly cover inferred information.

**2.1.2. Non-exhaustive list of technical information in the Act**

The ABA accepts that, due to the ever-changing nature of technology, further examples of the types of information captured under the definition of personal information is important to assist all APP entities. Technological innovation will continue to and is likely to expand or introduce new data points and information from which an individual can be identified.

However, it is our view that such guidance should be covered by updating the OAIC’s already existing guidance ‘*What is personal information*,’ rather than expanding the definition and providing examples under s 6(1). We submit that this is more appropriate, given the pace of technological change may create new forms of technical information faster than the Act can be updated.

The ABA also agrees with the OAIC’s view the explanatory memorandum could provide certain types of technical information that would be captured as personal information in appropriate circumstances.<sup>4</sup>

**ABA recommendation:**

2.2 Instead of including a list of technical information that is personal information within the Act:

- a. the OAIC should update its existing guidance ‘*What is personal information*’ to include an up-to-date list of technical information, and
- b. the explanatory memorandum should elaborate on the types of technical information that would be captured as personal information.

**2.1.3. Clarify the circumstances in which an individual is ‘reasonably identifiable’**

The ABA agrees with the fundamental principle that the Privacy Act should encompass any form of information which can identify an individual or from which an individual is reasonably identifiable. This is because it is not possible for the Privacy Act to pre-empt all future forms of personal information that may result from technological innovation.

However, the proposed addition that “an individual is ‘reasonably identifiable’ if they are capable of being identified, directly or indirectly” must be accompanied by clear regulatory guidance as to how this test is to be applied in practice. To preserve the principles-based scheme underpinning the Privacy Act and to ensure the Act remains technologically neutral, this guidance would most appropriately sit in OAIC guidelines rather than in the Act itself.

The Discussion paper noted that there is some inconsistency in the application of ‘identifiable’ across international jurisdictions. For example, in the UK, information is considered ‘identifiable’ if a motivated intruder could identify someone from it, including by linking it with other information.<sup>5</sup> In Canada, it has been held that information is ‘identifiable’ if there is a *serious possibility* of someone being identified from it.<sup>6</sup>

<sup>4</sup> OAIC submission in response to the Issues Paper, para 2.17.

<sup>5</sup> UK ICO, [Anonymisation: managing data protection risk code of practice](#), (Web Page, 2021), 22. Note this Code is still used as a guide to interpret the GDPR, despite being made under the [Data Protection Act 1998 \(UK\)](#) and [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data](#) [1995] OJ L 281.31, 23.11.1995.

<sup>6</sup> See, e.g., [Gordon v Canada \(Health\)](#) 2008 FC 258, [34]; See also for the EU approach, [Patrick Breyer v Bundesrepublik Deutschland](#) (European Court of Justice, C-582/14, 19 October 2016), ECLI:EU:C:2016:77.



The ABA suggests that Australian guidance should outline that information is 'identifiable' if there is a reasonably serious probability of a particular individual being identified from it (rather than a lower standard of individuation). In addition, the guidance should be clear that the definition would not capture information where there is only a remote or hypothetical risk of identification, e.g., linking data sets following a cyber hacking incident. This is important for the regime to protect information that could negatively impact society and individuals, while reducing barriers to access for data that could spur innovation.

## **ABA recommendation:**

- 2.3 It should be clarified that information is 'identifiable' if there is a reasonably serious probability of a particular individual being identified from it (rather than a lower standard of individuation).
- 2.4 Instead of including a list of objective factors relating to determining when an individual is reasonably identifiable within the Act, the OAIC should provide regulatory guidance on the matter after consultation with key stakeholders.

## 2.2 De-identified, anonymised and pseudonymised information

### **AGD proposal**

- a) Require personal information to be anonymous before it is no longer protected by the Act.

The Discussion Paper frames the proposal that information must be 'anonymous' rather than 'de-identified' as a continuation of the proposed changes in proposals 2.1 to 2.3. If the definition of personal information is expanded, then more types of information may need to be 'de-identified' before they fall outside the scope of the Act. The Government suggests the word 'anonymous' would more clearly signal to APP entities that they are required to meet the broader standard reflected by this term.

The ABA respectfully disagrees with the proposed terminology change. We submit that the current standard should be maintained; that data is no longer personal information once it has been de-identified. 'De-identification' is well understood by industry and data technologists, whereas a substitution of the term may create confusion for these participants as to the proposed policy intent. It is not clear to us why the terminology of de-identification would not remain fit-for-purpose if and when the scope of data that may reasonably identify an individual is broadened.

If the policy intent of the part of the Government is broader, such that the standard is raised to a higher requirement where the risk of re-identification is 'extremely remote' or 'hypothetical,' the industry does not support this change. We consider personal information with a very low re-identification risk should be treated as de-identified or anonymised information given the difficulties with true anonymisation. This aligns with the OAIC's view that 'Information will be anonymised where the risk of an individual being re-identified in the data is very low in the relevant context in which it is held or disclosed.'<sup>7</sup>

It is worth noting that whilst the European Union has applied the standard of anonymisation in its General Data Protection Regulation (GDPR) since 2018, there is substantial inconsistency between different Member State regulators on how the standard should be applied. Due to the lack of clarity between the definitions of 'de-identified' and 'anonymised,' further guidance would be required to assist entities in implementing the anonymised standard if it is adopted.

## **ABA recommendation:**

- 2.5 The current standard should remain that, once information is de-identified, it is no longer personal information.

## 2.3 Definition of sensitive information

The discussion paper questions whether the current scope of sensitive information is adequate, or whether it should be expanded to include other types of personal information. It posited that sensitive information can be easily inferred from financial data; for example, transaction history featuring clothing purchases may strongly indicate gender. One of the suggestions was that the definition of sensitive

<sup>7</sup> OAIC's submission to the Issues paper, para. 2.39

information should be amended to include information that ‘acts as proxies for sensitive information’ as they may be used as a basis for discrimination.

The ABA respectfully disagrees with this view, particularly regarding financial information. The ABA considers that such an expansion would not be appropriate and would significantly impede ordinary banking services (particularly where two or more individuals have equal access to the accounts).

Where transaction data is concerned, most transactions would not tie to any ‘sensitive information’, meaning that ‘sensitive information’ cannot be inferred from the data. For example, the mere fact that an account has made a payment for a medical procedure does not infer that it is the sensitive information of the account holder, or any of multiple account holders. Indeed, the account holder may be making payment on behalf of another individual not known to the bank.

The current Australian Privacy Principles (**APP**) are fit for purpose. The APP guidelines state information may be captured as sensitive information where it *clearly implies* one of the matters specified as sensitive information under s 6(1). In practical terms, this may mean that transactional data may become sensitive information if a bank takes an action to record an inference or opinion, based on the data, that constitutes sensitive information for the purposes of the Act.

**ABA recommendation:**

2.6 The current definition of sensitive information is fit for purpose. It captures financial information or transaction data as sensitive information in circumstances where there is a clear implication the transaction relates to matters under the definition of sensitive information.

### 3. Employee records exemption

The ABA supports in principle modifying the employee exemption to allow better protection of employee records, while retaining the flexibility employers need to administer the relationship. Where changes are made to the law that result in greater reliance on consent, special provisions may be required to address the potential power imbalance between employees and employers.

We agree with the position in the Discussion paper that a standalone exception for employers could be introduced into APPs 3 and 6 that permits employers to collect, use and disclosure personal or sensitive information relating to a current or former employee for any act or practice directly related to the employment relationship.

The application of other APPs would require careful consideration of the unique nature of the employment context, to ensure that proper management of the employee relationship is not hindered. For example, complexities exist in managing privacy for records which may contain opinions and personal information of multiple employees and in transferring records when businesses are sold.

There are also concerns about employers’ ability to undertake sensitive and confidential processes. APPs 12 and 13 would need to be amended to balance employees’ ability to access and seek correction of their personal information with countervailing considerations, such as the protection of other individuals’ privacy and maintaining the integrity of sensitive processes (e.g., investigations into employee misconduct, performance management or sexual harassment, whistleblowing requirements and other confidential investigations and complaints). In addition, transitional provisions may be required.

We also submit that a new exception should be added to APP 11.2 enabling an employer to retain personal information where it is in their legitimate interests to do so. The OAIC would need to provide guidance on the scope of an entity’s legitimate interests.

**ABA recommendation:**

3.1 The ABA supports in principle modifying the employee exemption to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship.

## Appendix C: Protections

### 4. Notice of collection of personal information

#### 4.1 APP 5 notices to be clear, current, and understandable

##### AGD proposal

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current, and understandable.

The ABA supports this requirement in principle, subject to simplification of the matters outlined in proposal 8.2. However, we seek further clarification on the interpretation of 'current' (including in the context of long-term contractual arrangements), and whether this would impose a standard review period over privacy notices.

We also agree with the OAIC's recommendation 32 from its Issues Paper submission, that APP notices need to be 'concise, transparent, intelligible and written in clear and plain language.' This wording is less ambiguous than 'current' and 'understandable' and may be a more appropriate approach than proposal 8.1.

##### ABA recommendation:

4.1 We support in principle a requirement that privacy notices must be clear, current, and understandable.

#### 4.2 Clarifying the interaction between privacy notices and privacy policies

##### AGD proposal

8.2 APP 5 notices limited to the following matters under APP 5.2:

- the identity and contact details of the entity collecting the personal information
- the types of personal information collected
- the purpose(s) for which the entity is collecting and may use or disclose the personal information
- the types of third parties to whom the entity may disclose the personal information
- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection
- the fact that the individual may complain or lodge a privacy request (access, correction, objection, or erasure), and
- the location of the entity's privacy policy which sets out further information.

The ABA is supportive of the intent to reduce the scope of matters listed in APP 5 notices. In practice, it is often challenging for an organisation to ensure the standard of being clear and understandable is met due to the current requirements in the APPs. The need to address these requirements often results in transparent but lengthy notices which mean they are likely to be less clear or understandable. Further, individuals are less likely to try to read and comprehend how their personal information will be used or disclosed, which may undermine the very purpose of a privacy notice.

However, we submit that the terminology in the following phrase, "...if the collection occurred via a third party, *the entity* from which the personal information was received..." is changed to refer to '*the type of entity*.' This is because it is often not practical for large organisations to amend each individual notice to specify the particular entity from which the personal information originated (e.g., in the case of credit origination, the individual mortgage broker).



**ABA recommendation:**

4.2 The ABA is supportive of the intent to reduce the scope of matters listed in APP 5 notices.

**4.3 Standardisation of APP 5 notices**

**AGD proposal**

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

The provision of examples of standardised privacy notices that could be used would be helpful. However, standardisation would be challenging in practice and would benefit from consumer testing. In addition, standard templates should not be mandated for an initial period so that effectiveness can be gauged over that period.

Key issues related to the development of the notices will include, amongst other things:

- the desirable length of content contained in the given template
- how information can be presented clearly and in an understandable way
- what aspects can be standardised across all APP entities, and which may require industry specific customisation.
- whether the templates can be optimised and made accessible across different technologies
- whether standardisation is intended to be mandatory and in what form (e.g., is it a requirement that notices be 'substantially in the form of...').

**ABA recommendation:**

4.3 The provision of examples of standardised privacy notices that could be used would be helpful, subject to extensive consumer testing and a transition period.

**4.4 Expanding the situations where notice is required**

**AGD proposal**

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, 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.

The ABA is supportive of the need to ensure transparency and consistency around the collection of personal information by APP entities. However, we are concerned that the proposed obligation is not clear and may result in inconsistent application.

We seek further guidance as to:

- what is meant by 'as soon as possible' and whether this would include a potential period, e.g., within 30 calendar days
- under what circumstances it would be acceptable for the prior notice to be considered adequate.

In addition, we caution against the introduction of subjective concepts that would cause confusion or inconsistency in approach. For example, it is difficult to understand what exactly is meant by 'disproportionate effort,' even with EU Article 29 Working Party Guidelines on Transparency that covers this specific exception. According to those Guidelines, each data controller must assess whether there is a proportionate balance between the effort involved to provide privacy information, and the effect that any use of such information would have on the data subject. Recital 62 of the GDPR points to three



factors that should be taken into account when making this assessment (i.e., number of data subjects, their age, and any appropriate safeguards); however, it is not clear how those factors would assist in a proportionality assessment.

In addition, 'impossible' would seem to be an onerous and impracticably high bar to meet and should be substituted for a term that provides protection balanced with the practicality of complying with the requirement (e.g., 'reasonably impracticable').

**ABA recommendation:**

4.4 Regarding the proposed requirement to strengthen and expand the situations where an APP 5 collection notice is required, the ABA suggests that the terms 'impossible' and 'disproportionate effect' should be substituted with meaningful alternatives, (e.g., impracticable in the circumstances).

## 5. Consent to the collection, use and disclosure of personal information

### 5.1 Strengthening what is required to demonstrate consent

**AGD proposal**

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

The ABA supports this in principle. We note that consent is a valuable method to permit the collection, use and disclosure of personal information in certain prescribed circumstances.

We also agree with OAIC's Issues Paper submission that it is important to preserve the use of consent for situations which have the greatest privacy impact, and not require consent for routine personal information handling or situations where the individual reasonably expects the use or disclosure of their personal information or considers it reasonable in the circumstances.

We note that any amendments to how consent is required under the Privacy Act should align with relevant domestic legislation and requirements and other international omnibus privacy legislation. In particular, the ABA submits that consideration should be given to harmonising the consent models set out in the *Privacy Act*, *Spam Act*, the Do Not Call Register and the Consumer Data Right regime. This would provide greater simplicity and certainty for both business and consumers.

We would like further guidance on:

- renewing or refreshing consent. The ABA considers that consent should be current so long as the individual remains an active customer, and the purpose for the collection, use, or disclosure of their personal information remains the same. Periodic renewal of consent should not be required where individuals can exercise a clear and simple opt-out mechanism at any time in respect of the use or disclosure of personal information for the purpose of direct marketing. In such cases, the individual can exercise control over the continued use and disclosure of their personal information, rendering the need for renewal of consent unnecessary.
- the application of the elements of consent in practice, including what is meant by the term, 'specific'. For example, what constitutes an unambiguous indication of consent?

**ABA recommendation:**

5.1 The ABA supports in principle consent being defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

### 5.2 Standardisation of consent requests

**AGD proposal**

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons, or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.



The standardisation of consent taxonomies, icons or phrases in consent requests can be useful tools in simplifying consent practices and ensuring consumers understand what they are consenting to. Standardisation of such tools is occurring as part of the development of the Consumer Data Rights Standards.

However, as the Discussion Paper notes, care will need to be taken that the use of such tools does not oversimplify consent requests and the proposed handling of personal information. Further, any standardisation should occur most appropriately on a sector-specific basis.

**ABA recommendation:**

5.2 The standardisation of consent taxonomies, icons or phrases in consent requests could be useful. However, care will need to be taken that the use of such tools does not oversimplify consent requests.

## 6. Additional protections for collection, use and disclosure of personal information

### 6.1 Collection, use and disclosure of personal information must be fair and reasonable

**AGD proposal**

6.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

The ABA is supportive of the principle that the collection, use and disclosure of personal information is fair, within individuals' reasonable expectations, and that it does not cause them harm. However, we consider that this fairness principle already underlies many of the existing provisions of the Privacy Act, alongside the other proposals put forward in the Discussion Paper.

The use and disclosure exceptions in the Privacy Act strike a balance between the privacy interests of an individual, and the use or disclosure of personal information for legitimate public or commercial purposes. If a fair and reasonable test were to apply in addition to the exceptions, it is not clear what further consideration would need to be given to ensure that a use or disclosure of personal information, that falls within the scope of one of the stated exceptions, is fair and reasonable.

We ask the Government to clarify how it would envisage the new provision would operate alongside the other provisions of the Act (such as general permitted situations or other exceptions that apply under APP 6).

**ABA recommendation:**

6.1 We seek further information to explain the intended operation of the fair and reasonable test under APPs 3 and 6.

### 6.2 Factors relevant to the fair and reasonable requirement

**AGD proposal**

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used, or disclosed in the circumstances
- The sensitivity and amount of personal information being collected, used, or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm because of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity



- Whether the individual's loss of privacy is proportionate to the benefits
- The transparency of the collection, use or disclosure of the personal information, and
- 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.

If requirements of collection and handling being fair and reasonable are introduced, we agree that greater guidance would need to be provided in relation to the meaning of fair and reasonable in a privacy context. Use cases should be provided, particularly in the data analytics space where it is not always clear whether an individual would reasonably expect information to be used for data analytics. It should also be clarified whether a given use would be fair and reasonable if it is sufficiently disclosed via a privacy notice or policy.

In relation to the factor of 'whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity,' this may inadvertently constrain commercial innovation. For example, where an entity is designing better ways of providing its services through innovative technologies which involve the collection of new types of personal information, there is a potential argument that this collection of personal information is not reasonably necessary to achieve its functions and activities. The interaction between the reasonably necessary requirement and the need for innovation should be considered in further detail potentially in OAIC guidance.

#### **ABA recommendation:**

6.2 If requirements of collection and handling being fair and reasonable are introduced, we agree that greater guidance would need to be provided in relation to the meaning of fair and reasonable in a privacy context.

### **6.3 Additional requirements in APPs 3 and 6 - requirement on third party collections**

#### **AGD proposal**

10.3 Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

The ABA understands this proposal's intention goes to introducing a 'due diligence' standard to online entities, where the scraping of enormous amounts of personal information including from publicly available websites occur and is potentially shared with third parties (such as data brokers).

However, this may also capture any third-party collection of personal information. We note that full oversight of third-party collection is not always possible. For example, where a financial entity has a credit card distribution arrangement with another financial corporation in the same sector, the effects of competition may prevent the purchasing entity from accessing the records of the supplier.

Further guidance is required as to what type of circumstances this proposal intends to capture, and whether it would also capture legitimate business processes and procedures such as credit checks or identity verification checks. Additionally, we seek clarity on its interaction with Part IIIA of the Privacy Act, and whether credit information will be specifically excluded.

We also note that this proposal is out of step with international practices. For example, under the GDPR a data recipient (whether a processor or independent controller) is not required to satisfy itself that the personal data was originally collected from the individual in accordance with applicable law. The ABA suggests that further consideration should be given to whether this proposal is necessary.



**ABA recommendation:**

6.3 The proposal to introduce a due-diligence requirement on third-party collections needs more consideration to ensure that it does not interfere with reasonable and required business processes, such as credit checks or identity verification checks.

**6.4 Additional requirements in APPs 3 and 6 - define primary and secondary purposes**

**AGD proposal**

10.4 Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

We understand this proposal seeks to encourage entities to advise individuals at the time personal information is collected of all primary purposes for which the information will be used and/or disclosed.

In our view, this proposal will not achieve its intended purpose of improving transparency and could have unintended consequences. For example, an unintended consequence may include entities adopting vague and broad descriptions for each primary purpose to capture potential or unclear future uses or disclosures. Alternatively, entities may circumvent the requirements by providing a large list of potential primary purposes (however remote they may be) – an outcome which would be detrimental from a consumer perspective.

**ABA recommendation:**

6.4 The ABA is not supportive of the proposal to redefine primary and secondary purposes in APP 3 and APP 6.

**7. Restricted practices**

**AGD proposal**

11.1 **Option 1:** APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- Direct marketing, including online targeted advertising on a large scale
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software
- The sale of personal information on a large scale
- The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale
- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

**Option 2:** In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.



The ABA supports the proposed Option 1, that entities engaged in specified restricted practices should be required to undertake additional organisational accountability measures to identify and mitigate privacy risks in a flexible and scalable way. We support the focus on Privacy Impact Assessments (PIAs) as an appropriate risk management tool in assessing the privacy impacts of a particular change initiative (where the initiative also constitutes a restricted practice).

However, the ABA exhorts caution in delineating the scope of restricted practices. For example, the ABA submits that general direct marketing to an existing customer base that would reasonably expect their personal information to be used or disclosed for the purposes of such marketing, and that does not involve privacy-intrusive practices, should not be characterised as a restricted practice. Individuals can also control the use and disclosure of their personal information by opting out of the receipt of further marketing, or by altering their marketing preferences. We would recommend that the Government seek to align its definition of restricted practices with other international privacy regimes, such as GDPR Article 35.

Additionally, as with the other proposals related to direct marketing and online targeted advertising, the Government should seek policy alignment between the relevant regulators (i.e., OAIC and ACMA) as to how these activities are defined in the relevant Acts and regulations. We note that this proposal is broader than the OAIC's recommendation 40 in its Issues Paper submission, which only applied to profiling, tracking or behavioural monitoring of, or direct advertising targeted at children.

Finally, the ABA also submits as follows:

- It is not clear whether the purpose is to capture activities where the personal information is the product being sold, or whether this would also capture divestment or acquisition activities which involve the purchase of customer databases as well as other business assets.
- European experience has demonstrated that appropriate and detailed regulatory guidance must accompany any prohibition or restriction on the collection, use or disclosure of personal information for the purposes of automated decision making that has *legal or significant effects*. This will ensure that the vague concept of 'significant effects' can be properly assessed by APP entities.
- It is not clear what acts or practices are intended to be caught by *the collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale*. Not all influencing behaviour results in a high privacy risk or serious risk of harm to individuals. We suggest that this be limited to social media networks and operators, per the worked example on page 136 of the Discussion Paper.
- Any collection, use or disclosure that is likely to result in a high privacy risk *or risk of harm to an individual*. The italicised words are unclear and should be defined. They may set too low a bar for a restricted practice. We suggest instead that the wording be amended to cover serious harm to an individual, which is consistent with the level of harm underlying the notifiable data breach scheme in the Privacy Act.

### **ABA recommendation:**

7.1 The ABA supports the proposed approach that entities engaged in certain high-risk activities should be required to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks in a flexible and scalable way.

7.2 The ABA submits that general direct marketing to an existing customer base that would reasonably expect their personal information to be used or disclosed for the purposes of such marketing, and that does not involve privacy-intrusive practices, should not be characterised as a restricted practice. If direct marketing is to be designated as a restricted practice, the Government should seek policy alignment between the relevant regulators as to how restricted practices are defined in the relevant Acts and regulations.

## 8. Pro-privacy default settings

### AGD proposal

11.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

#### **Option 1 – Pro-privacy settings enabled by default**

Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.

#### **Option 2 – Require easily accessible privacy settings**

Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

The ABA supports the intention of enabling users to have control over their privacy settings. We suggest that if Option 1 is pursued, the Government allow for the use of a neutral design approach where there is no default (for example, when an individual is presented with “yes” or “no”). Under such an approach, a customer could not proceed with using the product or service unless they select one of the options presented to them. The neutral approach allows for clear customer choice while enabling privacy protection.

## 9. Children and vulnerable individuals

### 9.1 Children’s privacy

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so.

The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1 – All collections of personal information**

Parent or guardian consent to be required before collecting, using, or disclosing personal information of the child under the age of 16.

- **Option 2 – Where consent is currently required under the Act**

Parent or guardian consent to be required in respect of a child under the age of 16 in situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction, or erasure requests.

The ABA is supportive of enhanced privacy protections for children considering their vulnerability. Children are increasingly engaging with technology, online platforms, mobile applications, and social media but may lack the technical, critical, and social skills to do so in a safe and beneficial manner.

However, we note caution in applying a new definition of a child to the banking and finance industry. It is important for children to be able to build their financial literacy skills as they develop cognitively. As ASIC advises through MoneySmart, opening a savings account is an effective way to introduce kids to banking, saving and interest in a safe and low-risk manner where they can have a degree of autonomy.

The ABA considers that the current approach specified under the OAIC’s guidelines works well in the banking context. Banks determine consent on a case-by-case basis, with the presumption that an individual aged 15 and over has the capacity to consent (unless there is reason to suggest otherwise).



This approach allows for adolescents to be gradually introduced to the banking services they will need in adulthood.

For example, it allows for a parent to open a basic bank account on behalf of their 13-year-old child, without the need for the parent to provide consent each time the child withdraws the pocket money available. This approach can assist parents in teaching their children a practical lesson about the scarcity and value of money management in a safe and contained environment. It is significant that it may be preferable for the child's physical safety to transact electronically than to carry cash.

If the Government proceeds with its proposal, we suggest further consideration be given to the practical effect of imposing a specific age threshold for consent. This is to ensure minors do not experience adverse and unintended detriment due to these changes. Any age threshold will also need to accommodate obligations banks have in relation to:

- collection, use and disclosure of customer personal information (including those that are children and vulnerable individuals) in connection with their obligations under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- other legal obligations to the minor, for example in cases involving family court
- the banker's duty of confidentiality, which is generally managed by obtaining customer consent to typical disclosures of customer information to third parties (including disclosures that do not require consent under the Privacy Act).

### **ABA recommendation:**

9.1 The ABA is not supportive of a broad approach that amends the Act to require consent to be provided by a parent or guardian where a child is under the age of 16.

### **9.2 Vulnerable individuals' privacy**

ABA member banks have obligations under the Banking Code of Practice to take extra care with customers who are experiencing vulnerability.<sup>8</sup> This means that, when we are providing a banking service to a customer experiencing vulnerability, we will:

- be respectful of the need for confidentiality
- try and make it easier for them to communicate with us
- provide appropriate guidance and referrals to help them to maintain, or regain, control of their finances, and
- refer them to external support, if appropriate.

The ABA has spent considerable time working with the OAIC to map rules to assist banks when they are handling the personal information of customers experiencing vulnerability. We have concluded there are limited circumstances when banks can use or disclose personal information for the purposes of taking extra care of customers without express and informed consent.

### **Case study<sup>9</sup>**

Edith Black is 83 years old and lives with her daughter and son-in-law, Henrietta, and Tom Swan. Edith has an account with the bank where her age pension is deposited. The account has a balance of \$202,430.

Edith has appointed Henrietta as her attorney. One day, Henrietta attempts to transfer \$120,000 from Edith's account to a building contractor. The transaction description lists 'Henrietta Swan – Renovation.' The Bank notices the transaction and is concerned that this payment may not be for Edith's benefit. It

<sup>8</sup> Chapter 14, Banking Code of Practice, accessible at: <https://www.ausbanking.org.au/wp-content/uploads/2021/10/2021-5-Oct-Banking-Code-WEB.pdf>

<sup>9</sup> This is a fictional case study for the purposes of illustrating privacy concerns.



places a block on Edith's account while further enquiries are made about the purposes of the transaction.

The bank tries to speak directly with Edith to confirm she is aware of the transaction and to raise its concerns. However, the contact details listed for the account are managed by Henrietta, who does not allow the bank to speak with Edith over the phone. Henrietta also refuses to bring Edith to the branch to discuss the transaction.

The bank has genuine concerns for Edith's financial welfare. It has no basis to conclude that Edith has diminished capacity and would like to refer the matter to the State police force for a welfare check. The bank can't rely on the 'permitted general situation' under s 16A of the Privacy Act as this exemption does not ordinarily extend to a threat to an individual's finances.

The above case study is a useful example of the privacy challenges faced in circumstances where the financial safety of an individual may be compromised. The ABA believes that the current review should consider an amendment to the Privacy Act that allows for 'good faith' disclosure of information to law enforcement or adult safeguarding authorities in circumstances where an individual's financial safety may be compromised. This would be in line with the operation of the UK regime.

The *UK Data Protection Act 2018* includes a provision that can be relied on for processing special category data in limited circumstances where there is a substantial public interest in safeguarding an individual's economic well-being. An individual is 'at economic risk' when they are less able to protect their economic well-being by reason of physical or mental injury, illness, or disability.<sup>10</sup> The exemption can be used in the following situations:

- the customer cannot give consent
- the entity cannot reasonably be expected to obtain consent
- obtaining consent would expose the customer to harm to their economic wellbeing.

It is important to note that, under UK law, firms cannot rely on this exemption if they have asked for express consent from the customer and the individual has declined to provide consent. The ABA proposes that a similar provision exist in Australia.

#### **ABA recommendation:**

9.2 The ABA believes that the current review should consider an amendment to the Privacy Act that permits 'good faith' disclosure of information to law enforcement or adult safeguarding authorities in circumstances when an individual's financial safety may be compromised, without a requirement to obtain express consent from such individuals.

## **10. Right to object and portability**

#### **AGD proposal:**

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using, or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

In other jurisdictions the withdrawal of consent and the right to object to processing are considered separately. We support the right of an individual to withdraw their consent, noting in certain circumstances this may have consequences that mean a product or service can no longer be provided or tailored to the individual's preferences or needs. An individual's broad right to objection needs to be balanced with regards to the other legitimate and lawful purposes for which APP entities collect and handle personal information which an individual cannot reasonably object to.

For example, the right to object under GDPR is not absolute and only applies to particular activities that are contingent on the lawful basis for processing (such as direct marketing, a task carried out in the public interest, or for an entity's legitimate interest). Any introduction of a similar right in Australia would

<sup>10</sup> *UK Data Protection Act 2018*, Schedule 1, Part A, section 19(3).



need to consider exceptions where this right would not apply. These exceptions should include, amongst others:

- Where the collection, use and disclosure of personal information is reasonably necessary for the administration of an employee's employment or to maintain records relating to a former employee's employment.
- Where the collection, use or disclosure is reasonably necessary for the performance of a contract, or to complete a transaction.
- Where the collection, use or disclosure of the personal information is reasonably necessary for a credit provider to comply with its responsible lending obligations.

The Privacy Act should also make it clear that any request by an individual not to collect, use or disclose personal information will not apply to their personal information to the extent it has already been de-identified.

#### **ABA recommendation:**

10.1 If a right to object to the collection, use or disclosure of personal information is introduced, specific exceptions need to be considered where this right would not apply. The Privacy Act should also make it clear that any request by an individual not to collect, use or disclose personal information will not apply to their personal information to the extent it has already been de-identified.

## 11. Right to erasure of personal information

### 11.1 Introduce a right to erasure on certain grounds

#### **AGD proposal:**

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Chapter 14)
- the personal information has been collected, used, or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent, or authorised guardian.

The ABA supports the right to erasure in a defined manner. However, consistent with the approach applied under GDPR, this right should not be absolute.

The Act should allow an APP entity to refuse a request in whole or in part in circumstances in which the interests or obligations of the APP entity, or the public interest, outweigh an individual's privacy interests. The introduction of clear principles outlining when an individual can request the erasure or destruction of their personal information should balance customer fairness with business requirements.

We note the possibility that there may be circumstances where erasing an individual's information may not impair the performance of obligations; however, if enough individuals exercise this right, the cumulative effect may be that of impairment. For example, this may be the case with back-office functions such as audits or portfolio risk assessments.

In addition, technology systems and data architecture make erasing data at an individual level practically difficult. We believe that the erasure right must be limited to a best endeavours obligation, for



example where low risk legacy systems are involved or where data owners may have to overcome technological challenges such as removing data piecemeal from back-ups.

In addition, APP entities should be permitted to either erase the relevant personal information or de-identify it. De-identifying the personal information will serve both to protect the privacy of an individual's personal information and enable APP entities to continue to extract value from the data they hold. This approach is consistent with APP 11.2.

### **ABA recommendation:**

- 11.1 The right to erasure of personal information must be qualified by well-defined exceptions that allow APP entities to refuse to comply with a request (in whole or in part) in certain circumstances.
- 11.2 The right to erasure must be limited to a best endeavours obligation, with APP entities also allowed to comply with any erasure request by de-identifying the relevant personal information.

### 11.2 Exceptions to a right of erasure

#### **AGD proposal:**

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.

We would support detailed consultation and guidance on exceptions to the right of erasure, including in circumstances where erasure is technically impractical or an unreasonable burden. For example, relevant circumstances could, at a minimum, include the following:

- Where the retention of the personal information is reasonably necessary for the performance of a contract to which the requesting individual is a party, or to complete a transaction.
- Where retention is required or authorised by law or a court/tribunal order.
- Where retention is otherwise required for an overriding public interest reason.
- Where compliance with the request would be technically impracticable, or the burden or expense of complying with the request would be excessive in all the circumstances.
- Where there is only an incidental link to an individual.
- Where an APP entity reasonably believes that erasure would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.
- Where a request for erasure is frivolous or vexatious.
- Where the information also includes the personal information of other individuals.
- Where erasure would pose a serious threat to the life health or safety of any individual, or to public health and safety.
- Where the information relates to existing or anticipated legal proceedings.
- If the employee records exemption is abolished or modified, where retention of the personal information is consistent with the legitimate interests of the employer.
- Where the retention of information is required for back-office functions, including security and fraud assessments, audits, portfolio credit risk assessments and model development (noting that there is a regulatory expectation that personal information used to meet compliance obligations is complete and accurate).
- Where the deletion of personal information would affect another customer, e.g., it relates to a joint account.



**ABA recommendation:**

11.3 We would support detailed consultation and guidance on exceptions to the right of erasure, including in circumstances where erasure is technically impractical or an unreasonable burden to erase an individuals' personal information.

**11.3 Include a process for responding to erasure requests**

**AGD proposal:**

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

We support this proposal in principle. If the right to erasure is enacted, APP entities should be permitted to respond and give effect to a request within a reasonable period, having regard to the following considerations:

- the complexity of the request and the volume and sensitivity of the personal information involved
- the extent to which an APP entity must work with other entities (e.g., the entity's service providers) to give effect to the request.

**ABA recommendation:**

11.4 The ABA supports in principle the requirement for APP entities to respond to an erasure request within a reasonable period.

## 12. Direct marketing, targeted advertising, and profiling

**12.1 Unqualified right to object to collection, use and disclosure for direct marketing**

**AGD proposal:**

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using, or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

The right to object (including for the purpose of direct marketing) overlaps with some of the key provisions already captured in the *Spam Act 2003* and the *Do Not Call Register Act 2006* for direct marketing activities undertaken in specific channels.

We would strongly advocate for alignment between the existing legislation and Australian regulators to ensure consistency in requirements for direct marketing activities. Alignment is particularly important concerning inclusion of objection requirements versus requirements for unsubscribing to commercial electronic messages under the *Spam Act*.

The ABA also seeks clarity as to whether the right to object:

- could be applied on a per brand basis, as opposed to all brands across an entity
- would extend to any underlying processing of an individual's personal information for the purpose of direct marketing, and



- would prevent the use of personal information where it is aggregated with the information of other individuals for marketing purposes.

In addition, we note that there may be situations where it is not possible for the entity to act in accordance with a right to object unless the individual provides further information (such as their email address, mobile number or device identification). For example, this may occur where an individual is not a customer of the organisation but has received targeted advertising. The ABA requests that an exemption is included for such situations.

## **ABA recommendation:**

12.1 We strongly advocate for alignment between the existing legislation and Australian regulators to ensure consistency in requirements for direct marketing activities.

## **12.2 Influencing an individual's behaviour or decisions must be a primary purpose**

### **AGD proposal:**

16.2 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.

The ABA seeks further clarification as to what is considered use and disclosure '*for the purpose of influencing an individual's behaviour or decisions*,' and any examples of such acts or practices. For example:

- would this capture benign or beneficial activities (such as using personal information to prompt a customer to update their contact details or offering emergency assistance during natural disasters)?
- is it intended that all marketing activity aimed at inducing acquisition or disposal of a new product or service is influencing behaviour or decisions? Is promoting a feature of a product or service already held caught, even if the feature was already available?

## **12.3 Remove APP 7 considering other proposals for reform**

### **AGD proposal:**

16.4 Repeal APP 7 considering existing protections in the Act and other proposals for reform.

The ABA is not opposed to the repeal of APP 7.

We note that the Government has asked for stakeholders to comment on the practical challenges of implementing a global opt-out process (i.e., to enable individuals to opt out of all online tracking in one click). The ABA understands that this is likely to be difficult to do without a significant and adverse impact on user experience. It may also be impossible where the individuals seeking to opt out have been delivered through third party channels, such as digital platforms.

## **ABA recommendation:**

12.2 Implementing a global opt-out process will result in a significant and adverse impact on user experience and may be impossible to achieve in certain situations.

## **13. Automated decision-making**

### **AGD proposal**

17.1 Require privacy policies to include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on people's rights.

The ABA supports this proposal in principle. However, further information and guidance will be required to explain:

- what the definition of 'automated decision making' would be, and whether this intends to align with the definition under the GDPR



- what is meant by ‘AI informed decision making,’ particularly if it will be used to form the basis of the definition of ‘automated decision making’
- a non-exhaustive list and examples of ‘similarly significant effect.’

**ABA recommendation:**

13.1 The ABA supports this proposal to require privacy policies to include information on whether personal information will be used in relevant automated decision-making processes.

## 14. Security and destruction of personal information

### 14.1 Clarify what reasonable steps may require

19.1 Amend APP 11.1 to state that ‘reasonable steps’ includes technical and organisational measures.

19.2 Include a list of factors that indicate what reasonable steps may be required.

The ABA supports further information on how reasonable steps to protect information can be achieved as this will assist APP entities in understanding their responsibilities under APP 11.1. However, we are of the view this proposal would be best achieved by providing the factors and information on reasonable steps under the OAIC’s existing ‘*Guide to securing personal information*’.

We also support any alignment of reasonable steps requirements with Article 32 of the GDPR, and existing standards such as SOC, ISO and/or CPS234.

**ABA recommendation:**

14.1 Instead of including a list of factors in the Act that indicate what reasonable steps may be required to protect information, the OAIC should update its existing guidance ‘*Guide to securing personal information*.’

### 14.2 Strengthen destruction requirements

**AGD proposal:**

19.3 Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

This is a meaningful change from the existing requirements of APP 11.2. The ABA is concerned that this provision appears unbalanced relative to other requirements in the Privacy Act that refer to ‘reasonable steps.’ The destruction and de-identification obligation in the Privacy Act should continue to be qualified by a standard of reasonableness. As noted previously, we would seek further clarification of the definition and threshold for ‘anonymisation’ and what factors may be considered in determining whether an entity has taken all reasonable steps.

**ABA recommendation:**

14.2 The ABA does not support amending APP 11.2 to require APP entities to take all reasonable steps to destroy or anonymise relevant information.



## 15. Overseas data flows

### 15.1 Introduce standard contractual clauses (SCCs)

#### **AGD proposal:**

22.4 SCCs for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information

The ABA is supportive of the inclusion of SCCs provided they are not mandatory, nor the only means by which to provide for overseas data flows.

In addition, the ABA supports consideration being given to some prescribed statutory obligations for offshore processors, regardless of agreed terms, and with extraterritorial application. This may have the benefit of limiting the effort required to reach agreement on acceptable contractual terms and could improve the performance of offshore data processors as it relates to the personal information of Australians. The ABA also supports consideration being given to other international privacy regimes in developing a statutory test that would capture offshore processes to ensure alignment wherever possible.

#### **ABA recommendation:**

15.1 The ABA is supportive of the inclusion of SCCs provided they are not mandatory, nor the only means by which to provide for overseas data flows.

### 15.2 Strengthen notice requirements

#### **AGD proposal:**

22.4 Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

Large multinational entities regularly engage (and disengage) overseas third-party entities and are already required by APPs 1 and 5 to provide transparency to individuals around these transfers. These third-party entities assist in ensuring, amongst other things, availability and business continuity which is critical to financial services.

The ABA is concerned that the implication of this proposal is that an entity's privacy policy could contain a large list of countries with several types of personal information used for different purposes that would need to be regularly updated with each engaged or disengaged third party.

This would not be effective in achieving its purpose of transparency, relevant to the individual's interaction with the entity. Rather, it may confuse individuals by listing numerous countries, types of personal information and purposes of disclosure that would not apply to the individual in the circumstances.

The ABA's view is that APP 8 already provides adequate safeguards for the individual. Any information regarding specific cross border disclosure or the types of personal information used/disclosed to third parties can be captured under APP 5 notice requirements around the time of collection.

#### **ABA recommendation:**

15.2 Notice requirements do not need to be strengthened in relation to potential overseas disclosures. The qualification currently present in the Privacy Act, 'if it is practicable to specify those countries,' should be retained.



### 15.3 Obligations apply only to 'disclosures'

#### **AGD proposal:**

22.6 Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

While greater clarity around reasonable steps is welcome, the ABA is of the view that such clarification should take the form of non-binding guidance in the APP Guidelines.

#### **ABA recommendation:**

15.3 The circumstances relevant to determining what 'reasonable steps' are for the purpose of APP 8.1 should be contained in OAIC guidelines.

## 16. Cross Border Privacy Rules and domestic certification

#### **AGD proposal:**

23.1 Continue to progress implementation of the CBPR system.

23.2 Introduce a voluntary domestic privacy certification scheme that is based on and works alongside CBPR.

The ABA conditionally supports the implementation of a voluntary domestic privacy certification scheme and welcomes alignment with the CBPR system and other established schemes worldwide. Critical to the ABA's support is that some form of assurance is provided by the Government or the regulator that negative inferences would not be drawn, for example in enforcement action, from an absence of certification under a voluntary scheme. In addition, we agree with the OAIC's submission to the Issues paper that a certification scheme would provide consumers with evidence-based information about the privacy credentials of entities.

#### **ABA recommendation:**

16.1 The ABA conditionally supports the implementation of a voluntary domestic privacy certification scheme and welcomes alignment with the CBPR system and other established schemes worldwide.



## Appendix D: Regulation and enforcement

### 17. Enforcement

#### AGD proposal:

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- A cost recovery levy to help fund the OAIC's provision of guidance, advice, and assessments, and
- A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.

The ABA understands that several proposals contained in the Privacy review would require increased funding to the OAIC. However, we would request that further details be released about the operation and quantum of the proposed levies, and the meaning of 'operation in a high privacy risk environment' before we are able to make a further recommendation. Clarification is also needed as to how this model would work for public sector agencies.

### 18. Notifiable Data Breaches scheme

#### AGD proposal:

27.1 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

The ABA does not support this proposal, on the basis that including this information in the mandated statement without the option to provide information as commercial in confidence may complicate requests subject to the *Freedom of Information Act 1982 (Cth)* (FOI). This information is already routinely included in notifications to individuals by ABA members without this amendment.

It is important for such information to be provided in confidence so that the personal information of individuals is not disclosed under an FOI, or in circumstances where the information would reveal commercially sensitive activities in response to a data breach caused by a malicious or criminal attack. We submit that, if this proposal is intended to improve the quality of the information the OAIC receives from entities that have made an NDB, then it is more appropriately reflected in improvements to the OAIC's information gathering powers or fines for non-compliance.

#### ABA recommendation:

18.1 Subsections 26WK(3) and 26WR(4) of the Notifiable Data Breaches scheme should not be amended.

### 19. Interactions with other schemes

#### AGD proposal:

28.1 The Attorney General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

28.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

28.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Given regulatory overlap in matters involving the handling of personal information, the ABA would support a more cohesive framework around how regulatory enforcement will be prioritised and handled in these kinds of incidents and investigations.

**ABA recommendation:**

- 19.1 The ABA supports in principle the recommendations to strengthen privacy harmonisation across State and Commonwealth agencies.