Australian Banking Association

04 December 2020

Australian Attorney-General's Department
Via email: PrivacyActReview@ag.gov.au

Dear Colleague,

Privacy Act 1988 (Cth) Review

The Australian Banking Association (**ABA**) welcomes the opportunity to make a submission to the review by the Attorney-General's Department (**AGD**) of the *Privacy Act 1988* (Cth) (**Privacy Act**).

Since the *Privacy Act* came into force the data economy has become mainstream. For the banking industry, the data economy has enabled real-time and online banking services; it has created a vast number of new data points – information which, when used appropriately will facilitate better outcomes for Australians and drive jobs and innovation. The ABA supports a review of the *Privacy Act* and the stated goals to ensure privacy settings empower consumers, protect consumer data, and best serve the Australian economy. The right reforms will facilitate innovation and new products and services for confident Australian consumers as we emerge from the economic consequences of the COVID-19 pandemic.

Achieving the balance between Personal Information (**PI**) protection, innovation and economic growth will require considerable time and effort from the AGD to get these reforms right.

In support of these reforms, in the annexure to this letter the ABA has provided response to a number of the questions raised in the AGD issues paper. Additionally, the ABA highlights the following three points.

The Government's policy agenda

It is prudent for the AGD to first consider the multitude of live policy/legislative consultations and other government initiatives which overlap and will have significant impact on the Australian privacy framework. These include (to name a few), Open Banking; the Consumer Data Right (**CDR**); Treasury's Inquiry Into the Future of the CDR (read/write access); the ACCC consultation on Version 2 of the CDR Rules (including consumer consent); the Office of the National Data Commissioner proposed Data Availability and Transparency Bill; the Australian Government Department of Industry, Science, Energy and Resources consultation on an AI Action Plan for all Australians; the Digital Transformation Agency's consultation on Digital Identity; the Reserve Bank of Australia Review of Retail Payments; the Digital Transformation Agency's updated Trusted Digital Identity Framework; the Treasury's review of the Australian Payments System (announced as part of the Digital Business Package contained in the 2020-21 Budget); the Office of the Australian Information Commissioner (**OAIC**) work on Australia's third National Action Plan and the OAIC implementation of the eight commitments in Australia's second Open Government National Action Plan.

Given the above, the ABA urges the government to first design an overarching blueprint and roadmap for data and information privacy. Without oversight and co-ordination, it is a risk that no reform will fully achieve the intended outcomes because siloed approaches will potentially conflict with or hinder the planned benefits of the other government initiatives.

Vulnerable Australians

The ABA's Banking Code of Practice (2020) includes commitments relating to the treatment of customers experiencing vulnerability, including the need to take extra care with such customers. There is also an expectation by some consumer advocates, Australian Financial Complains Authority (**AFCA**), and Australian Securities and Investments Commission (**ASIC**) that banks hold a significant volume of customer data and can use this information to support customers experiencing vulnerability. To further the commitment of the Code and to address stakeholder concerns, the banking industry is in the

process of developing an industry guideline that outlines how banks will take extra care with customers experiencing vulnerability. Several challenges exist in developing the guidelines in the context of more complex customer cases. The ABA would value the involvement of the OAIC in these discussions and, where appropriate, the issuance of guidance aimed at addressing the nuance and complexity of different vulnerability scenarios, in a way that legislative amendment could not. The ABA may seek to provide further detail on this matter during the next stage of consultation.

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.

The ABA looks forward to engaging further with the Attorney-General's Department in respect to the Review of the *Privacy Act*.

Regards

Emma Penzo
Policy Director
Emma.penzo@ausbanking.org.au

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.

Australian Banking Association

Objectives of the Privacy Act

Question 1: Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

The objects of the *Privacy Act* are appropriate and do not require substantive changes.

The ABA recommends consideration of a minor enhancement to the drafting at clause 2A(a). The word 'promote' suggests that outcomes lesser than the protection of privacy are acceptable to the government. The ABA suggests delete 'promote' and substitute 'provide for'.

Definition of Personal Information

Question 2: What approaches should be considered to ensure the Act protects an appropriate range of technical information?

Technological innovation will continue to and is likely to expand or introduce new data points and information from which an individual can be identified and/or develop new data categories which could be accurately described as being 'about' an identified or identifiable individual. For example, technology which supports the creation of 'deep-fakes' will enable individuals to develop and assume virtual alter-personas from which virtual lives can be experienced. In another example, advances in medical technology may result in detailed medical information, which currently is not accessible, being gathered from a person as they walk through their daily routines. In other advances, a person's gait, keyboard typing pattern, handwriting, and other information may be used to identify them. For this reason, it is not possible for the *Privacy Act* to pre-empt all future-technology generated PI. As a principle, the *Privacy Act* should encompass any form of information which can identify an individual or from which an individual who is reasonably identifiable.

Therefore, the ABA supports the recommendation of the Australian Competition and Consumer Commission (**ACCC**) to update 'the definition of PI in line with current and likely future technological developments to capture any technical data relating to an identifiable individual.'[1]

Question 3: Should the definition of personal information be updated to expressly include inferred personal information?

Inferred PI, to the extent it is information or an opinion about an identified individual or an individual who is reasonably identifiable, would already by captured by the existing definition of in the *Privacy Act*. On the basis that inferred PI may be PI, and for the benefit of clarity, the ABA recommends that the *Privacy Act* could expressly include reference to the fact that inferred PI may constitute PI and the OAIC could provide further guidance on this topic.

Question 4: Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

De-identification is a privacy enhancing tool. It is an important data governance measure which enables innovation and drives the data economy while protecting the privacy of individuals. The ABA notes the OAIC has issued clear guidance in respect to de-identified data[2] confirming that where de-identification is undertaken, such that the risk of re-identification is very low, that that information is not PI.

The ABA notes the OAIC's guidance, that the state of data being 'de-identified' is temporal and context specific, it is not a fixed or end-state. Therefore, de-identified data involves an ongoing process of monitoring and re-assessment for the risk of re-identification in different release contexts. Given this requirement for organisations to continually monitor the status of de-identified data, in the ABA's view further protections are not required. Extending the application of the APPs (such as APP 6, 8 and 11) to de-identified data will present practical challenges and inhibit innovation.

The OAIC has noted that eliminating any risk of re-identification is unachievable. ABA does not support a move from a standard of de-identification (that requires re-identification to be very low) to a standard

[1] ACCC, 2019, Digital Platforms Inquiry, p24
[2] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

which eliminates all risk of re-identification (where data is treated so that no individual can be identified irreversibly).

Therefore, the ABA supports the current position where de-identified data is excluded from the definition of PI and that de-identified data continue to not be subject to the APPs. Additionally, the existing standard of de-identification, should continue to apply. If there is an issue with the practice or quality of de-identification of data, the ABA suggests that this issue can be resolved through additional OAIC guidance.

Question 5: Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

The ABA notes that there is a broader discussion in the community regarding the memorialisation of a deceased person and any enduring rights that their next of kin or estate may have to their personal and digital data including their digital persona which has yet to be settled. There does not appear to be a general community consensus on this issue. Further, any consent requirements need to provide appropriate accommodation for banks to give account information to next of kin, representatives of an estate, or those applying for letters of administration in accordance with existing obligations, and practical needs. Therefore, the ABA submits that it would not be appropriate to extend the definition of PI to include PI of the deceased until there is an established community expectation.

Flexibility of the APPs in regulating and protecting privacy

Question 6: Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

The ABA notes that the APPs are sufficiently flexible and would not recommend including prescriptive rules which may serve to impede innovation and would likely not be resilient to advancements in technologies. Greater clarity could be provided through updated guidance from the OAIC.

There are clear benefits of principle-based regulatory frameworks for consumers and businesses alike. In practice, the principle-based framework can be applied and adapted across various scenarios and in relation to different technologies.

For a regime that would impact a wide range of industries, seeking to include more prescription would likely result in a high degree of complexity. This is particularly in the banking industry where banks are subject to many existing legislative regimes, the addition of greater prescription in the privacy regime would add to compliance costs and should take into account the operation of those regimes.

Notice of collection of personal information

Improving awareness of relevant matters

Question 20: Does notice help people to understand and manage their personal information?

Notice is an appropriate method for ensuring that individuals can make an informed decision regarding sharing their PI with an entity. The ABA recognises the challenges of striking a balance between providing individuals with sufficient detail regarding data usage and sharing versus overloading individuals with lengthy collection statements which may not be read or understood. The ABA is supportive of the position on a layered approach to notification and communicating with individuals in a user-friendly and comprehensible way.

Limiting the information burden

Question 24: What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

The ABA notes that APP 5 'Notification of the collection of PI' requires extensive notification which may duplicate the information required to be present in the Privacy Policy. The objective for privacy notices

should be to inform individuals written in a style and length that is easy to read and understand. For example, the Privacy Policy should contain generic information and that the notice could be more specific with clear link to the intended collection and use of PI. The ABA suggests that the OAIC provide guidance on what good practice looks like for privacy notices for different contexts.

Question 25: Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

The ABA considers caution and further consultation is required on the use of standardised icons or language. There is potential for consumer benefit by virtue of standardised icons as in certain circumstances this may assist in reducing content in a notice and removing duplication. For example, a symbol of the 'world' might indicate that information will be disclosed outside of Australia; or another symbol might indicate that PI is shared with third party service providers. That being said, the ABA is also conscious that mandating 'standard icons' may have the effect of limiting innovation or may result in consumer detriment and confusion if used inconsistently by different organisations or sectors.

As such, if standard icons were to be developed, the ABA considers that should involve wide consultation to test for consistent application across sectors. Further, such changes should be durable to accommodate developments in technologies and data handling practices.

Consent to the collect, use, disclose Personal Information

Consent effectiveness

Question 26: Is consent an effective way for people to manage their personal information?

Consent is an effective way to manage PI. The ABA supports the existing position of APP 6 where consent should only need to be sought for secondary uses of PI that are unrelated to the primary purpose of the transaction which are not reasonably expected, and in relation to the collection of Sensitive Information (**SI**). This position reduces regulatory burden and consent-fatigue.

Question 27: What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

If consent is required to be obtained, the *Privacy Act* should prescribe the principle that consent to the collection, use, and disclosure of information is to be freely given and informed. The *Privacy Act* should not prescribe how this is to be achieved. As per the current regime, the ABA's view is that it should be the remit of the OAIC to issue appropriate guidance and the responsibility of entities to undertake testing with customers to determine the optimal approach for consent given the context in which the PI will be collected, used, and disclosed.

Question 28: Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

Where the provision of the primary good or service requires multiple uses of PI such that the primary good or service cannot be delivered without the entirety of the consent, consent should not be required.

Where the PI will be used for multiple secondary purposes, which are unrelated to the primary purpose, consideration should be given to the practicalities of seeking separate individual consent for each purpose, particularly given individuals commonly sign up or provide data over small devices (e.g. smartphones).

The ABA does not believe obtaining unbundled separate consents to every secondary purpose is practical, or helpful for customers, in all circumstances and it should be available to organisations to delineate how those consents operate and the extent to which consents for similar uses may be bundled together.

Exceptions to the requirement to obtain consent

Question 31: Are the current general permitted situations and general health situation appropriate and fit-for purpose? Should any additional situations be included?

During the pandemic, some ABA members relied upon clause 16A of the *Privacy Act* in releasing transactional data (to the extent that it contained PI) to the state based COVOD-19 contact tracing teams. For this particular situation, clause 16A was fit-for-purpose but requires updated and detailed guidance to be issued by the OAIC.

Pro-consumer defaults

Question 32: Should entities collecting, using, and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Due to the evolving nature of information, a principle of pro-privacy defaults may be reflected in the *Privacy Act* however, context-specific, and current guidance should be left to the OAIC to provide. The industry would require further information on what such pro-privacy defaults may look like to fully consider the implications. Current pro-privacy defaults applied by the banking sector include:

- Products, services, and customer interactions are constructed with privacy by design.
- Check boxes remain unchecked.

The ABA suggests that further consultation is required if the *Privacy Act* were to require pro-privacy defaults.

Inferred sensitive information

Question 35: Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

As per the response to Question 3, the definition of PI could be clarified to include inferred PI, thereby extending the concept of inferred SI to the definition of SI as well.

Question 36: Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

The ABA suggests that specific consent should still be required for the collection of SI. However, flow-on impacts will need to be considered. For example, in the context of employees and if the employee records exemption is removed, there is a question over whether employees can provide consent given the nature of the employee/employer relationship. In this context, consideration should be given to how the collection of SI (e.g.: sick leave) will be managed.

Direct marketing

Question 37: Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

The position of whether explicit consent is required or not (and clarification on the standard of consent including granularity) for direct marketing circumstances needs to be clearer, including consistency with the *Spam Act 2003* (Cth).

The operation and interpretation of APP 7.6 and 7.7 is also unclear and would benefit from reconsideration and further clarity by the OAIC. In particular, APP 7.6(b) is not clear on the extent of what 'facilitating' would capture, including whether this is designed to capture engaging other organisations to perform direct marketing for the first organisation (akin to a service provider) or sharing data for the second organisation to use for its own direct marketing purposes. Following that, in 7.6(d) it is not clear whether 'the organisation' refers to the 'first organisation' or the 'other organisation' (i.e. the second organisation who was provided with the information by the first organisation). APP 7.6(e) is also unclear in a scenario where the first organisation is disclosing PI for a second organisation to use for

direct marketing – given the individual would presumably want to know where the second organisation (who is marketing to them) received their information.

Refreshing of consent

Question 38: Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

This depends on the context, including the subject matter and the way the consent is scripted. For example, a consent could be stated to 'continue for the life of the product or service' or 'on an ongoing basis until you withdraw your consent'.

The ABA may be supportive of periodic consent refresh in relation to certain marketing or personal information commercialisation activities. The method for refreshing a consent should not be prescriptive. For example, an organisation may choose to periodically notify the individual that their consent for the entity to do [X] or [Y] continues and that they can change their consent preferences by contacting [Z]. Requiring individuals to expressly opt-in on a regular basis is likely to result in consent and/or notice fatigue on the part of individuals, as well as create unnecessary administrative burdens for organisations.

Control and security of personal information

Security and retention

Question 43: Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

The security requirements under the *Privacy Act* are appropriate to protect the PI of individuals. Risk assessments need to be able to be calibrated to a range of situations. It is difficult to prescribe appropriate security obligations covering all practices, particularly given security requirements change overtime and adapt to changing technology and risks.

Right to erasure

Question 46: Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

Question 47: What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

Any right to erasure needs to operate in concert with obligations of banks to maintain PI and banking data of individuals for specified periods for legal and risk management purposes.

Further, the complex nature of banking systems means that a right to erasure will introduce an operational and compliance burden for backed-up records which may be duplicated across multiple systems.

Overseas data flows and third-party certification

Question 48: What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information? a. Are APP 8 and section 16C still appropriately framed?

The APP's are broadly suitable for the transfer of data overseas. However, the ABA notes that an alignment of the APPs to international standards would reduce friction when establishing data transfers internationally. The ABA recommends that it would assist Australian entities if the OAIC were to provide a 'whitelist' of countries/jurisdictions which were considered to fit within APP8.2(a) in a similar manner to GDPR's adequacy findings.

Australian Banking Association

Secondly, the ABA notes the long history of the OAIC's Public Interest Determinations (**PID**) relating to International Money Transfers (**IMTs**) in February 2020[3], in 2015[4], and in 2014[5]. PIDs are self-repealing with the current one to be repealed on 17 February 2025. The ABA notes the PID consultation and submission process is not an efficient way to manage the privacy requirements for IMTs. Additionally, the temporary nature of PIDs make it an insecure mechanism on which to build international funds transfer service offerings.

The ABA submission to the OAIC consultation on *Public Interest Determinations on International Money Transfers* also noted the inability of ADIs to rely upon the APP8.2 exceptions:

> 'Given the nature of the IMT process… an ADI is unable to rely upon any APP 8.2 exceptions. Specifically, under APP 8.2(a) it would be impractical for every ADI to obtain current and ongoing legal advice in relation to the privacy regimes of all jurisdictions to which IMT initiated by that ADIs customers are sent. Even if such legal advice was obtained, those jurisdictions with inferior privacy schemes would fall outside the APP 8.2(a) exception.[6]

Therefore, the ABA recommends a review of APP8 to provide permanent relief to IMT remitting ADIs.

Enforcement powers under the Privacy Act and role of the OAIC

Question 53. Is the current enforcement framework for interferences with privacy working effectively?

The ABA notes the presence of multiple and overlapping regulatory bodies or instruments which can take enforcement concurrent action in the event of a breach. These include: APRA's CPS234; ASIC's licensing requirements; the CDR Rules and Standards; ACMA's Spam Act and Do Not Call Register, as well as APP11.1 and the Notifiable Data Breach (NDB) under the *Privacy Act*. Therefore, the ABA notes that the enforcement framework for interferences with privacy is complex.

Notifiable Data Breaches scheme – impact and effectiveness

Question 64: Has the NDB Scheme raised awareness about the importance of effective data security?

The ABA agrees that the NDB scheme has been effective in raising awareness.

Question 65: Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

The ABA notes the extensive guidance[7] of the OAIC in respect to NDB however considers that further reform of the NDB would be helpful. There is opportunity for the NDB scheme to align with other mandatory data breach notification schemes globally in respect of joint party data breaches. Other schemes manage the notification of joint party data breaches (where the data breach involves PI held by more than one entity) by assigning different responsibilities to the controller and processor entities. This reduces time and negotiation involved in notification where one party disagrees with the assessment of the data breach under the NDB scheme. As the Australian scheme is currently interpreted, the decision to notify is left for the parties involved to determine, which can lead to delays and complexity in notifying affected individuals.

[3] https://www.legislation.gov.au/Details/F2020L00145
[4] https://www.legislation.gov.au/Details/F2015L00199
[5] https://www.legislation.gov.au/Series/F2014L00241
[6] https://www.oaic.gov.au/assets/engage-with-us/consultations/applications-for-new-pids-regarding-international-money-transfers/submission-aba.pdf
[7] https://www.oaic.gov.au/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf