10 January 2022

Privacy Act Review
Attorney-General's Dept.
Canberra ACT

By email: privacyactreview@ag.gov.au

Review of the Privacy Act – Discussion Paper

The Australian Financial Markets Association (AFMA) welcomes the opportunity to respond to the *Review of the Privacy Act – Discussion Paper* (Review). AFMA represents the interests of over 120 participants in Australia's wholesale banking and financial markets. Our members include Australian and foreign-owned banks, securities companies, treasury corporations, traders across a wide range of markets and industry service providers. Our members are the major providers of services to Australian businesses and retail investors who use the financial markets.

At a general policy level, AFMA supports a principled approach to individual privacy and recognises that given the substantial growth in personal data collection and its commercialisation in recent years, a review and update of existing arrangements is appropriate. AFMA fully supports the reasonable and proportionate safeguarding of personal information and requirements around this aim must be kept up to date to respond to evolutions in the field. Financial services firms are centred on the protection and accurate processing of private data, so these updates are of particular relevance to this sector.

AFMA supports the view that where extensions to the current regime are made they should be done so in a way that is aligned with standard practices elsewhere, where those practices have proved to work well and are compatible with Australian values and policies.

Any changes to the Privacy Act will have complex flow on implications for other regimes including the Consumer Data Right (CDR). AFMA has previously raised concerns around the highly complex design of the CDR's extensions of the Privacy Act. Revisions to the Privacy Act would likely require significant systems reengineering to ensure compliance of these systems. Any redesign must ensure it is coordinated with integration into the CDR regime, and it may be appropriate to consider rationalisation of the CDR extensions.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7993 Email: secretariat@afma.com.au

AFMA's substantive comments on selected Review proposals are set in the Attachment.

Please contact David Love either on 02 9776 7995 or by email dlove@afma.com.au in regard to this letter.

Yours sincerely

David Love
General Counsel & International Adviser

Attachment

This submission is limited to addressing those Review questions which were deemed to be relevant to AFMA members in the financial services sector. It responds to eight topics of review, namely:

1. Personal Information – Chapter 2
2. Employee records exemption – Chapter 5
3. Notice and consent, and introducing a fair and reasonable requirement - Chapters 8-10
4. Direct marketing, targeted advertising and profiling – Chapter 16
5. Automated decision making and organisational accountability – Chapters 17 & 20
6. Organisational accountability - Chapter 20
7. Industry funding arrangements – Chapter 24
8. Overseas data flows – Chapter 22

9. Personal Information

2.1 Change the word 'about' in the definition PI to 'relates to'

Not supported -The current definition of personal information is fit for purpose. We are concerned with the uncertainty created by such a change. We do not consider this proposal would achieve its intended purpose and may have unintended consequences, such as capturing any information remotely related to an individual, or capturing commercial information of entities used to provide the individual a service or a product.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

Not in the law – Providing further examples is a welcome idea due to the changing nature of technology. There is a need for the examples to be relevant to current technology and for this reason we do not support examples being provided in the legislation itself but rather through the existing means of the OAIC guidance '*What is Personal Information*'.

AFMA supports the Office of the Australian Information Commissioner's (OAIC) view that the amending legislation's Explanatory Memorandum could provide certain types of technical information that would be captured as personal information in appropriate circumstances. (see OAIC submission in response to the Issues Paper, para 2.17).

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment of personal information.

Not in the law – In keeping with the response to Q2.2, guidance is welcome but given the dynamic nature of technology this can be provided in the OAIC guidance, not in the law. Technologies which allow identification are evolving and consideration should be given to not penalising an entity for the assessments made in the past which are overtaken by technology enabling retrospective identification.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

Not supported – This proposal is unbounded and would make compliance very difficult because of its vagueness. Inferred information is already included under the current definition of personal information under 'opinion'. In addition, the OAIC's guidance about 'What is personal information' already includes information or opinion 'inferred' about an individual from their activities.

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

Not supported - OAIC's view is 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.' (OAIC's submission to the Issues paper, para. 2.39). Consistent with this view personal information with a low re-identification risk should be treated as anonymised information, given the challenge of being absolutely certain about the anonymisation of information in a data point rich environment.

More generally, due to existing the lack of clarity between the definitions of 'de-identified' and 'anonymised', further guidance is needed to assist entities in implementing the anonymisation standard.

10. Employee records exemption – Chapter 5

5 What would be the benefits and limitations of providing enhanced protections for employees' privacy in workplace relations laws?

Not supported - If collection of employee data were to be subject to a consent requirement it is problematic to conceive how free consent could be obtained in the context of the employment relationship.

11. Notice and consent, and introducing a fair and reasonable requirement Chapters 8 -10

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

Not supported - 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' is a sensible recommendation in respect of this question. The OAIC wording

is less ambiguous than 'current' and 'understandable', and preferable to the Q8.1 formulation.

8.2 APP 5 notices limited to specific matters under APP 5.2.

Reserved support – Regarding the following matter in APP 5.2

- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection

This requirement would be hard to meet if it requires naming all third parties disclosing personal information to the entity (especially in large corporate groups). As a suggestion it would be sufficient to list the types of third parties the entity may receive personal information from as indicated in the dot point.

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.

Not supported – The experience in the financial services sector is that such standardised format notices are more trouble to the regulator, regulated entity and consumer than they are worth and have resulted in wording which is overly long and incomprehensible to the consumer despite the testing. The diverse range of businesses covered by this legislation means they will have a better understanding of how to communicate effectively with the target audience. For the financial services sector, in particular, businesses are required to communicate a large volume of statutorily mandated information and privacy notices form part of a large suite of information that needs to be combined and presented in a consumer-friendly form.

OAIC guidelines are the preferred way to assist business in preparing their privacy notices.

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.

Reserved support – This proposal would on the positive side provide greater compliance certainty. In this context guidance is desired on what the standard would be for 'as soon as possible', and whether this would include a potential time period, e.g. within 30 calendar days.

However, the collection notice process is already burdensome when personal data is collected in the B2B/institutional business context (personal data of other company employees, such as the individual contacts of a corporate client/counterparty); when business cards are provided by executives of corporate clients or prospective institutional clients; or when it is necessary to obtain information about a corporate institutional client to meet both Australian and offshore regulatory requirements. An

exemption for such business contacts and where collection is required by law (whether Australian or otherwise) such as that available in other jurisdictions is needed especially if the requirement is to be strengthened.

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

Supported – We agree with the 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 expects or considers reasonable in the circumstances.

The statutory formulation should also be consistent with international norms for consent giving.

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.

Not supported – Consistent with the response to Q8.3, standardisation is not desirable. The financial services sector has a large number of systems and client onboarding statutory requirements into which privacy consents need to be integrated in a clear manner. Standardisation militates against this objective and could conflict with other statutory requirements.

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

Supported - subject to comments in 10.2 below.

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 as a result 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.*

Reserved support - Legislated factors can assist with compliance certainty. However, cross-border compliance concerns arise, especially in relation to consistency with the General Data Protection Regulation [European Union] (GDPR) 'legitimate interests'

assessment test in respect of having a lawful basis. In addition we note that the balancing of individual interests is not required where there is a legal obligation to collect and handle personal information in a particular way (for example, disclosures to AUSTRAC), or where the collection is necessary to fulfil a contract (to which other legal and precedential tests apply).

In regard to a child, it would be more practicable for the test to be whether the collection, use or disclosure of the personal information has been consented to by the child's parent or guardian having done so considering the best interests of the child. It would be hard for the entity to determine whether the collection, use or disclosure of personal information is in the best interests of the child.

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.

Reserved support - This proposal amounts to a form of 'due diligence' standard for online entities, where the scraping of large amounts of personal information from publicly available websites occur and is potentially shared with third parties (such as data brokers).

However, it appears this may also capture any third-party collection of personal information. Further guidance is required as to what type of circumstances this proposal intends to capture, and whether it would also capture legitimate processes and procedures such as credit checks or identity verification checks, or whether it extends to a contract between the APP entity and a third party who has been engaged for a service. Additionally, we seek clarity on its interaction with Part IIIA of the Privacy Act, and whether credit information will be specifically excluded.

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.

Not supported - This introduces a significant change to the current approach where clear purposes are stated. It may have a counterproductive effect of encouraging vague and broad descriptions for each primary purpose in order to capture potential or unclear future uses or disclosures or providing a large list of potential primary purposes. By introducing the requirement that a secondary use or disclosure must be 'directly' related to the primary purpose for all personal information (rather than sensitive information alone), this would require a significant shift across all APP entities with established practices to reassess secondary purposes that may not be 'directly' related to the primary purpose. For example, the use of personal information for a legitimate business purpose the individual would reasonably expect such as quality assurance or auditing.

12. Direct marketing, targeted advertising and profiling – Chapter 16

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.

Query - From a financial services perspective this presumably would include the analysis of whether a client should receive product ideas / content aligned to their preferences / current portfolio when receiving financial service advice?

16.3 APP entities would be required to include the following additional information in their privacy policy on whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

Query - Would this reasonably include the analysis of whether a client should receive centralised product ideas / content aligned to their preferences / current portfolio? How would this interact with other obligations regarding financial services advice under the Corporations Act?

13. Automated decision making and organisational accountability – Chapters 17 & 20

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.

Reserved support – On the basis that further information and guidance will be needed to explain:

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

14. Organisational accountability -Chapter 20

20.1 Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk.

Not supported – APRA regulated entities are already subject to extensive accountability requirements under the *Financial Accountability Regime Act 2021*. Redundant accountability regulation should not be imposed on the financial services sector.

15. Industry funding arrangements – Chapter 24

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.***

Not supported - AFMA has been a long-time critic of the way industry funding arrangements have been implemented for financial services regulation, a subject on which we have made representations to government in recent years. Our views in regard to this proposal extend across to privacy regulation on a consistent basis. The following points set out AFMA's views relevant to consideration of policy on industry funding arrangements.

Moral hazard is a significant problem in the design of cost recovery arrangements. The structures for these arrangements present little incentive for government to keep costs low or efficient, as these costs are passed onto the invoiced entities. Moreover, governments have paid little attention to the cumulative burden of ad hoc increases in cost recovery levies and also have failed to recognise that the primary beneficiary of regulation is the public, whose interests can in effect only be reflected in a government contribution to regulator funding.

It is generally accepted, at least in principle, that cost recovery should be instituted for reasons of economic efficiency and good regulation and not to raise revenue. However, in practice, governments may impose cost recovery arrangements to improve the budget bottom line. In an environment in which the federal budget is under pressure from a number of sources, there is a realistic concern that further cost recovery arrangements will be imposed as revenue-raising measures at the expense of economic efficiency. There is also a danger that the revenue-raising motive leads to cost recovery arrangements being imposed in an ad hoc and uncoordinated fashion so that the full cost recovery burden of regulation being imposed on the regulated industry is not recognised by government. In the case of financial services, this regulatory cost burden is seen as hindering Australia's international competitiveness as a regional and global financial centre.

There is also the danger of regulatory creep if there is no direct cost to government from the introduction of new regulation. This may lead to regulation being over-supplied. Cost recovery arrangements should only be imposed as a result of a detailed assessment process that takes account of the full burden of regulation on the regulated industry, including compliance costs and the benefits to government from the industry's contribution to the implementation and continued operation of government regulation.

Cost recovery arrangements also ignore significant revenue benefits to government arising from regulation. Industry bears the considerable compliance costs of regulation, an additional cost burden over and above regulator's expenses. Cost recovery for new regulation typically generates new charges and compliance costs for the industry to bear. Little or no thought is given in this context to the full cost of such regulatory change for industry participants. In practice, their business units must incur the operational and compliance start-up costs associated with new regulation, deal with the (often dampening) impact of the new regulation of business activity and, at the same time, pay an additional charge for regulation. It is important to the efficiency of the financial system for cost recovery charges to be introduced in a manner that has regard to the broader costs of regulation being absorbed by a regulated entity, and its ability to pay.

More generally we see an opportunity to rationalise and streamline the current disjointed approach to privacy which currently sees four regulators in the financial services sector alone enforcing overlapping and inconsistent privacy related regulations.

16. Overseas data flows – Chapter 22

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

Not supported - AFMA members caution that the prime example of the APAC CBPR system has not proven to be helpful in practice with only five countries providing the certification possibility and limited number of companies that joined the system, missing some of the biggest companies in the personal data storage business such as Microsoft, Amazon or Google. Consequently the system cannot be leveraged for many data transfers by members with others such as financial institutions with whom they into business transactions and provide personal data to.

22.3 Remove the informed consent exception in APP 8.2(b).

Not supported - Removal of this exception may mean a reduction in services that will be available to AU individuals. In practice global organisations apply global minimum privacy protection standards to their related bodies corporate and to agreements with outsourced providers. Where information must be provided under foreign law (eg under tracing notices where an individual wants to trade / hold securities in a non-Australian jurisdiction) it may not be possible to ensure the third party recipient will meet the protections required under the Privacy Act and if there is no informed consent exception the business would need to block clients trading /holding securities from certain jurisdictions.

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.

Not supported - Large multinational entities regularly engage (and disengage) overseas third-party entities and are already required by APP 1 and APP 5 to provide transparency to individuals around these transfers. The implication of this proposal would mean the APP entity's privacy policy could contain a large list of countries with different types of personal information used for different purposes, and would be required to be regularly updated with each engaged or disengaged third party. This would not be efficient 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 most likely not apply to the individual in the circumstances.

It is noted that APP 8 already provides adequate safeguards for the individual, with any information regarding specific cross border disclosure or the types of personal information used/disclosed to third parties can be adequately captured under APP 5 notice requirements around the time of collection.

22.5 Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines

Supported - Legislative certainty around the definition of 'use' and 'disclosure'.

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

Reserved support- This would provide further clarity on transfers under 8.1. However, we seek further consultation on these factors/circumstances, in order to seek alignment with other privacy jurisdictions which have recently introduced similar requirements (for example, Data Transfer Risk Assessments under the GDPR).