5 April 2023

Privacy Act Review Secretariat
Information Law Branch
Attorney-General's Department

Via email: PrivacyActReview@ag.gov.au

Dear Secretariat

Government Response to the Privacy Act Review Report

COBA appreciates the opportunity to contribute to the Government's consultation on its response to the Privacy Act Review Report (the Report) and its proposals.

COBA is the industry association for Australia's customer owned banks (mutual banks, credit unions and building societies). Collectively, our sector has over $160 billion in assets and is the fifth largest holder of household deposits. Customer owned banks account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

Key points

COBA supports updating the *Privacy Act 1988,* but we need to see more clarity on the proposals and ask the Attorney-General's Department (AGD) to balance the costs to businesses with the rights and needs of the individual when implementing the proposals.

The wide-ranging impacts of many of these proposals will require significant implementation and consultation periods on the draft laws and draft guidance from the Office of the Australian Information Commissioner (OAIC).

Implementing many of the proposals will result in considerable cost to industry, notably in terms of upgrading controls, processes, and technology systems. Easier, streamlined and more effective solutions should be considered in achieving the same policy outcomes, including regarding communicating clear and understandable information to individuals while preventing prohibitive costs on regulated entities.

COBA strongly opposes the adoption of an Industry Funding Model (IFM) for the OAIC.

Privacy Act Report Proposals

COBA supports modernising the *Privacy Act 1988* to reflect changes to the economy due to digitisation and on the principle of providing strong and secure privacy rights to all Australians. Many proposals made in the Report are, when taken individually, appropriate and reasonable. However, when taken as a whole, the changes proposed will have significant impact on our members and be potentially expensive to implement and, in some cases, provide little benefit to individuals.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

These significant privacy reforms and accompanying costs follow on from the extensive and intensive period of responding to escalating regulation imposed on the financial services sector following the Banking Royal Commission, Financial System Inquiry, and post-Global Financial Crisis reform agenda.

COBA's members are much smaller than their competitor listed banks and operate on a mutual model where the bank is owned by its customers instead of by a separate group of shareholders. This means that our members' businesses operate for the benefit of their customers rather than to maximise shareholder profits. Costs imposed on our members are ultimately borne by their retail customer-owners in the form of less favourable product pricing and less investment in digital capability. Increasing regulatory costs adversely impacts on our members' product and digital offerings thereby limiting the ability of our members to provide competitive options to Australian consumers.

On many proposals the 'devil will be in the detail' and it is difficult for our members to exactly understand the business impacts until they see the draft legislation. A few high-level comments from COBA for the AGD to consider as it approaches the drafting:

- New measures and changes must appropriately balance the costs to regulated entities with the rights and needs of the individual. The measures must not be excessively weighted towards the individual at the expense of business as doing so will reduce innovation and competition, resulting in poorer individual/consumer outcomes. Increased costs for smaller ADIs, including our members, will hinder their ability to continue providing choice through an offering of strong, competitive, and ethical products against the major banks.
- Clarity must be provided on whether changes are prospective or retrospective. Most measures should not be retrospectively applied as we believe it will be prohibitively expensive for our members to implement and will not necessarily deliver benefit to individuals. We strongly recommend, for example, that any data already held by APP entities is grandfathered into the new regime rather than requiring APP entities to retrospectively identify and document matters such as source of data, purpose of collection and that the collection was fair and reasonable.
- Exceptions need to be sufficiently wide and flexible that they are capable of being used by the varying industries that are subject to the Privacy Act. Each industry has its own unique situations which includes its size, structure, customer base and the complexity of its products. The banking industry generally collects personal information directly from the individual and therefore we would consider it appropriate that any principles-based approach is flexible enough to support appropriate outcomes across industries.
- The draft legislation and draft OAIC guidance need to clearly set out the level of detail that APP entities must provide or record to explain how an individual's personal information is being collected, used, or disclosed.

COBA has provided more detailed commentary addressing individual proposals in **Appendix A** to this submission.

Implementation of proposals and consultations

Implementation period

The complexity of the proposed changes and the wide-ranging impacts that they will have on our members' businesses will require extensive changes to policies and procedures, and key business processes. Our members will need to make system modifications and upgrades. Like many businesses these days our members utilise and rely on third party vendors, including offshore service providers, for operating key business processes. New obligations will require extensive engagement by our members with these vendors to achieve compliance with the revised Privacy Act and is likely to require changes to vendor contracts and Service Level Agreements (SLAs). There are a number of suppliers that are used across our membership and there is a risk of a single point failure or delays across multiple entities, that could occur if all the changes are brought in simultaneously.

The wide-ranging impacts of the proposed changes across industries and different sectors will see a strong demand for the limited resources of SME consultants, legal advisers, and IT service providers

to understand the changes, update internal policies and procedures, and upgrade systems to be compliant. This will create a significant bottleneck and greatly hinder the ability of smaller APP entities to adapt to any changes in a timely manner, as they operate on very lean resource models.

Based on these costs and difficulties, COBA requests at least a two-year implementation period for our sector that only commences once the Bill and OAIC guidance has been finalised.

Some additional implementation options that the AGD could consider are:

- **Phased implementation based on business size**: larger businesses will have more resources and ability to make these changes. Providing longer lead times for smaller businesses, like our members, and other regulated entities would allow for the implementation costs to be spread over time thereby allowing our members to seek the advice and assistance they need without having to confront the bottleneck for resources we mentioned above. This would support outcomes for individuals by prioritising effort where it would have the greatest impact, with large businesses and their large customer bases.
- **Phased implementation of proposals by tranches**: if the AGD sought to introduce all the legislative proposals in a single Bill, this would result in a large and a very complex Bill that would be difficult to implement. The AGD should consider the benefit of implementing differing aspects of the proposals in tranches with like measures grouped together. This would allow regulated entities to implement and respond to changes in a piecemeal way and would help spread out costs over time. If this approach is adopted, we recommend that AGD outline from the beginning what is being implemented in each tranche and to provide a timeline of when each tranche would come into force. Effort would need to be made to ensure that later tranches do not result in rework of earlier implemented technical solutions.

Consultations

COBA recommends that the draft Bills implementing the legislative proposals and the draft OAIC guidance all be subject to extensive public consultation.

COBA wishes to be included in any future industry consultations or roundtables held by the AGD or the OAIC as part of the implementation of the proposals in the Report. In particular, this includes the targeted consultations undertaken to implement proposal 17.3 on identifying options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.

COBA is also happy to be directly contacted or consulted on any comments expressed in our submission and would be happy to facilitate discussions between the AGD and/or OAIC with our members on any issues as part of implementation.

Clear, streamlined, and effective ways of communicating personal information management

The Report makes many proposals requiring that APP entities better document how they collect, use, and disclose personal information. COBA supports this approach and proposes that the right balance between individual benefit and industry cost could be achieved by documenting these matters in a single policy document, either within or separate to the APP 1 Privacy Policy. This approach would ensure that APP entities consider whether the purpose, collection and use is lawful, fair, and reasonable before collecting or using personal information. It would also ensure that APP entities could be held accountable if their practices deviated from these requirements.

This document would outline:

- the personal information the entity collects, uses or discloses,
- where the data is sourced from,
- the purpose for holding the data, and
- the rationale as to why the collection, use, or disclosure is fair and reasonable.

A more granular approach, requiring purpose, source, reasonableness, and fairness to attach to each data element held would be excessively onerous without producing any material uplift in individual protection.

Imposing such a burden on business would require smaller APP entities to divert significant resources away from higher value initiatives. This is reinforced by the proposed removal of the small business exemption, which we believe would result in many smaller regulated entities being unable to achieve compliance.

COBA suggests that the AGD consider this approach when implementing various proposals (for example, proposals 12, 13 and 15) as it appropriately balances individual protection with business costs, improved competition, and innovation.

Industry Funding Model for the OAIC

COBA strongly opposes the introduction of an IFM for the OAIC. The OAIC is an economy-wide regulator and not a sector specific regulator or agency, such as APRA, ASIC, and the Financial Services Compensation Scheme of Last Resort. The single industry role of those agencies is not analogous with the economy-wide role of the OAIC.

The OAIC and its regulatory remit is far broader than these other agencies. Collection, use and disclosure of personal information permeates all businesses, industries, and government agencies. This would result in an extremely complex funding model that would not be efficient or effective in equitably raising funds. While COBA recognises that OAIC functions will be expanded under these proposals we believe that the funding of the OAIC should continue to come from general revenue. The privacy protections and cost of regulating this regime should be borne by every Australian individual and entity and the most effective way to raise these funds is through general taxation.

If an IFM is adopted for the OAIC then proportionality and equity would require all government agencies, and all employers, to be included in the funding model. As above, we note that an IFM is likely to be so administratively inefficient that it belies the purported benefit that will be gained from adopting the model.

We look forward to engaging with the Department on this issue and thank you for taking our views into account. Please do not hesitate to contact Robert Thomas, Senior Policy Adviser (rthomas@coba.asn.au) if you have any questions about our submission.

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer

Appendix A: COBA Comments on Specific Proposals of the Privacy Act Review Report

Number	Proposal	COBA Comment
Personal Information, de-identification and sensitive information		
4.1	Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.	When combined with proposal 18.1 on access rights this could lead to unreasonably wide and burdensome requests for blanket searches. COBA is not necessarily opposed to the definition being changed to provide clarity, especially with proposed OAIC guidance to ensure that the connection is not too tenuous and remote. COBA asks AGD to be mindful of potential flow on risks and impacts of this change in definition will have during the drafting of the Bills.
4.5	Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.	COBA suggests that the 'use' aspects of APP 6 are not applied to 'de-identified' information. This will ensure that businesses can use de-identified data to help develop solutions, products and services that provide improve consumer outcomes and experiences. We support the application of other APPs, including APP 11 and the disclosure elements of APP 6, to de-identified data that is reasonably re-identifiable.
Flexibility of the APPs		
5.2	Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.	The circumstances of these temporary APP codes should be limited to account for the fact that they will not be subject to consultation. COBA suggests AGD consider adopting a model like New Zealand where the temporary APP code making powers can only operate after a state of emergency or national emergency has been declared.

Number	Proposal	COBA Comment
		There should also be a consideration given to the impact of the temporary APP code and the need for adopting a significant implementation period where the code requires changes to information handling processes or systems.
5.4	Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.	An emergency is by its nature temporary. Rolling powers granted to the Executive Government are not appropriate and the use of emergency declarations should continue to be of limited time duration. If there is an ongoing emergency then there needs to be safeguards, such as only allowing a one-off extension of six months beyond the original 12 months. There should also be an option for disallowance by either House of Parliament on the original declaration or on the extension of the declaration.
Small business exemption		
6.1	Remove the small business exemption, but only after: (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations.	COBA is cautious on this proposal as it is not clear that the additional costs imposed on small businesses and to the economy will deliver meaningful benefit to individual's privacy. Note that COBA's members are subject to the Privacy Act irrespective of this exemption remaining or being removed. Many small businesses do not have the resources to comply with the obligations of the Privacy Act and are likely to find it extremely onerous. The additional burden would likely have a detrimental impact on these entities and the inclusion of millions of additional businesses into the regime would also likely overwhelm the OAIC and result in lopsided or ineffective regulation. This also raises questions when considered in combination with the IFM in proposal 25.7. Due to the sheer complexity and inefficiency of including small business in the proposed IFM it seems likely that the model would exclude small businesses

Number	Proposal	COBA Comment
		from having to contribute. This raises questions about what purpose proposal 6.1 seeks to achieve as it will likely result in an unreasonable increase of costs on small businesses who mostly pose low privacy risks and is unlikely to deliver much benefit to the privacy of individuals. As an alternative, there is opportunity to expand the exceptions to the small business exemption to include certain higher risk small businesses. For example, real estate agents would be an appropriate exception as they handle significant amounts of personal information and should be held to a higher standard compared to other small businesses.
Employee records exemption		
7.1	Enhanced privacy protections should be extended to private sector employees, with the aim of: (a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for (b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information (c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and (d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.	These changes will have time and cost impacts on our members. We request that sufficient time periods be provided for implementing these. AGD should ensure that there is consistency and clarity in how these obligations are implemented and in how they interact with obligations under workplace relations laws.

Number	Proposal	COBA Comment
Privacy policies and collection notices		
10.1	Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.	COBA supports the intention of making Collection Notices (CN) useful and understandable to customers. However, there is inconsistency between proposals made in this Report. Proposal 10.1 wants CNs to be clear, up-to-date, concise, and understandable while proposal 10.2 wants more detail added and proposal 18.7 requires that entities advise of the rights of the individual at the point of collection, so assumedly would need to include more detail in the CNs. The Report wants more information in CNs but also wants existing CNs to be simplified but these could conflict as entities would be trying to simplify while also adding additional complex information. AGD needs to carefully consider the situations where proposals conflict as each on its own has merit but when taken as a whole actually add complexity and do not necessarily deliver the value purported to be created. Clarity is also needed on the level of granularity of information that is to be required by proposal 10.2. OAIC guidance on this would be helpful. Applying these changes to CNs retrospectively to all former customers in addition to providing updated CNs to all existing customers would likely impose a significant cost on regulated entities. These changes to CNs should only be applied prospectively to current and future customers.
10.2	The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice: (a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.	
10.3	Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency	Development and increased use of standardised privacy policies and collection could be beneficial in helping to reduce costs. For this to be of benefit to our members there would

Number	Proposal	COBA Comment
	across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	need to be tailored options for banking industry requirements as banking obligations are not the same as those that apply to other sectors. COBA welcomes being consulted in the development of these standardised documents especially if they can be made of use to the banking sector.
Consent and privacy default settings		
11.1	Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.	Inferred consent needs to be included in any change to the definition.
11.2	The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.	Guidance on consents and progressing to standardised consents are welcome assuming that they are usable by our members. We ask to be included in any consultation on the development of any OAIC guidance.
11.3	Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	COBA has concerns with how this would operate in practice. The issues are similar to our concerns with the right to erasure (proposal 18.3) and are expressed more fully below.
Fair and reasonable personal information handling		
12.1	Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.	The mutual model of our members and their focus on delivering good outcomes for their customer-owners means that our members already take a strong ethical approach in their decision making and would likely be compliant with the proposed test. Additionally, obligations imposed under their banking licences ensures that they are already subject to similar tests (for example, acting 'efficiently, honestly and fairly' in accordance with *Corporations Act 2001*, s 912 and *National*
12.2	In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances	

Number	Proposal	COBA Comment
	(b) the kind, sensitivity and amount of personal information being collected, used or disclosed (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) 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, and (g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and (c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.	*Consumer Credit Protection Act 2009*, s 47). We believe the test is an appropriate control to impose on regulated entities. It would also be beneficial if the OAIC could create guidance on how to practically apply the test. COBA suggests that the test be made as easy as possible to comply with. We provide two possible approaches. <u>Privacy Impact Assessments (PIA)</u> As part of completing a PIA for high privacy risk activities, as provided for in proposal 13.1, we suggest that the fair and reasonableness test could be explicitly included in the assessment process. <u>Policy document on management of personal information</u> Alternatively, COBA suggests that for complying with this proposal (and other proposals relating to purpose and source of collection) that the information be recorded in a single policy document that builds on the APP entities Privacy Policies and CNs. We believe that such an approach would require APP entities and agencies to consider the matters outlined in this proposal and to document the rationale as to how they meet their obligations. This approach would ensure that regulated entities and agencies would not be subject to an absolute requirement to demonstrate these objectives on a data element by data element basis. Any requirement for regulated entities to build and maintain separate data fields for purpose, source, and fair and reasonable would lead to significant complexity and create unnecessary costs with very limited benefits to individuals. These costs would be so significant that it likely to require smaller regulated entities to divert significant resources from
12.3	The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.	

Number	Proposal	COBA Comment
		other higher value customer-facing initiatives. If this is combined with the proposed removal of the small business exemption, we believe that it would result in many of those small businesses that were newly brought into the regime being non-compliant.
Additional protections		
13.1	APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.	COBA supports the proposal but believes a clear definition and examples are needed for 'high privacy risks'. We welcome the release of OAIC guidance and wish to be included in any consultation during its development. Clarity is needed on whether the change would require PIAs be made retrospectively and apply to decisions and products that have already been made. Our view is that this obligation should only apply prospectively as the cost to our members to review and revisit all existing products and decisions and complete PIAs would likely be prohibitively expensive without necessarily providing benefit to the individual.
Organisational Accountability		
15.1	An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.	COBA supports this proposal only where it is applied prospectively. A retrospective application would be difficult and costly for our members to adopt and unlikely to deliver significant benefit to individuals. Additionally, this obligation should be able to be satisfied by recording this information at a general level.
Children		
16.2	Existing OAIC guidance on children and young people and capacity should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.	COBA is supportive of strong measures to protect the personal information of children, but we have concerns with interpreting a best interest duty in a banking environment. We would like to

Number	Proposal	COBA Comment
	The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).	work with AGD/OAIC on the development of these proposals and OAIC guidance. The need to consider an individual child's maturity, while appropriate, does rely heavily on OAIC guidance and consideration needs to be given to specific issues regarding children and their interactions with banking. While banking products are financial products of relatively low complexity, they may still be too complex for many children to understand. If a best interest duty is adopted, we believe that OAIC guidance will be necessary to assist in how this duty should be managed in the banking sector, and in other sectors where the collection and disclosure is often to or from a parent or guardian responsible for the child. A particular concern in banking is determining the best interest of the child vis a vis the rights of parents or guardians to information on their child. Clear guidance, with examples, are needed to ensure that ADIs are appropriately balancing the rights of children and the rights of their parents/guardian. There are also concerns with determining the rights of each parent/guardian versus the other parent/guardian, particularly where there is a known relationship breakdown. In practice, the best interests of the child can conflict with the interests and rights of one or both parents/guardians. Potential solutions could include: • OAIC guidance to regulated entities in how to manage these kinds of situations, including example scenarios on how to apply the best interest duty. • A defence for regulated entities to protect them when it is not clear what the best interests of the child are, but they act reasonably and appropriately in the circumstances.
16.4	Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.	

Number	Proposal	COBA Comment
		• A specific exemption from the obligation be provided for basic banking products, for example, transaction and deposit accounts. More complex banking products should be kept within the regime. Further consultation will be necessary with industry before any new obligations are introduced and COBA welcomes the opportunity to engage further with AGD on this issue.
People experiencing vulnerability		
17.3	Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.	COBA supports the views expressed by the ABA and consumer groups in their joint submission of 16 September 2022. We agree that there needs to be consideration of how financial institutions can act appropriately in the interests of customers experiencing financial abuse or no longer have capacity to consent. As COBA represents two thirds of domestic ADIs in Australia we expect to be included in these consultations regarding customers who may be experiencing financial abuse.
Rights of the individual		
18.1	***Access and Explanation*** Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features: (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act) (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying	The implementation of the proposals on the Rights of the Individual will be time consuming and bear significant cost. Implementing these proposals will require an increase in data maturity across many sectors and we agree that this uplift is appropriate. We believe the rights of the individual in relation to these proposals should be subject to similar restrictions that are currently set out in APP 12. Further clarity must be provided to

Number	Proposal	COBA Comment
	purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual	ensure that the request for information is not absolute, and that APP entities may decline (or charge for) such a request to the extent that the cost of complying with the request is disproportionately excessive relative to the benefit the individual is seeking to derive. See discussion below on proposal 18.6 for more detail. Clarity will be needed on how these rights, particularly the right to erasure, applies to data collected and held before the right commences. Significant work will be required by our members to review their existing vendor contracts, services, and SLAs and accordingly a longer lead time would be recommended before introducing new individual rights in these areas. As part of this work, clarity will need to be provided on exactly what kinds of personal information needs to be provided and in what form. COBA would like to see limitations on the extent of information or detail that needs to be provided as conducting searches of all systems and records could be unreasonable and overly burdensome.
18.3	***Erasure*** Introduce a right to erasure with the following features: (a) An individual may seek to exercise the right to erasure for any of their personal information. (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.	
18.4	***Correction*** Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.	
18.6	***Exceptions*** Introduce relevant exceptions to all rights of the individual based on the following categories: (a) **Competing public interests:** such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. (b) **Relationships with a legal character:** such as where complying with the request would be inconsistent with another law or a contract with the individual. (c) **Technical exceptions:** such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.	COBA supports the exceptions provided but requests that the drafting of these exceptions be made sufficiently broad and flexible to capture the many types of industries regulated by the Act. <u>Relationships with a legal character</u> We support this exception as our members are already subject to many overlapping and complicated laws, which could conflict with the Privacy Act and the changes proposed in the Report.

Number	Proposal	COBA Comment
		<u>Possible additional exception or sub-exception – business needs</u> While we are supportive of the legal character exception, we do not believe it, nor the other two exceptions, are sufficiently scoped. We do not believe that the exceptions capture all the situations where our members may need to hold personal information even though an individual has requested its deletion. For example, our members may need to hold onto records that are not strictly provided for by law or by contract but are needed as proof that the member has satisfied contractual or other obligations. This information would need to be held to defend themselves in future complaints or legal action. Our members are particularly concerned with the risk of abuse these new rights could create. For example, where a customer requests the deletion of records under the new right of erasure in proposal 18.3 with the motivation of making a future complaint against the bank. The bank could then no longer defend itself due to the relevant records having been deleted. COBA believes that an additional exception could be drafted, or the legal character exception widened, to include business needs where the records or personal information is necessary to be held in order to prove the entity has complied with its legal and contractual obligations. An alternative to creating a new exception could be to extend the quarantining option provided in proposal 18.3. This would extend it beyond law enforcement to allow for information needed to be kept by entities for protection against future legal actions. This would ensure that the personal information is not being used by the entity but could be made available if a legal action is brought against it. The information could then be

Number	Proposal	COBA Comment
		deleted at the appropriate time when it is no longer needed for legal needs. <u>Technical exceptions</u> COBA is concerned that some of the rights in proposals 18.1, 18.3, and 18.4 being unfairly or unreasonably used against APP entities and agencies, for example, through excessive requests for information. We note the Report has already provided for an exception to address vexatious and unreasonable requests at proposal 18.6. We ask the AGD to consider providing guidance on what is an unreasonable request. For example, guidance could cover how large a request would have to be to be unreasonable, what would constitute an unreasonable search, and address how much effort must be undertaken. Freedom of Information laws that apply to government agencies will often provide a means to refuse to deal with an application for information if it is an unreasonable and substantial diversion of the agency's resources. A similar approach could be provided for unreasonable requests to access information from a regulated entity. However, like in those instances under Freedom of Information, the regulated entity should have an obligation to assist the applicant in making their request reasonable. As a further deterrent to vexatious requests the law could also allow an entity to charge a nominal fee to process the request. The Act or Regulation could prescribe the amount to prevent any misuse of this, such as setting at $25 or $50 per application. Additionally, consideration could be given to prescribing an hourly processing fee for applications for information that are above a certain size. For example, if processing the application

Number	Proposal	COBA Comment
		would take more than 10 hours for an APP entity to process. The collection of this fee would allow entities to partially recoup costs from the application and could encourage individuals to work with the entity to identify what information they actually want and how it can be reasonably provided. This process could work in a similar way to the processes provided for in Freedom of Information laws. The amount charged could also be prescribed in law to prevent misuse, with a suggested amount of $25-$50 per hour.
18.7	***Response*** Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.	COBA agrees that providing notice to individuals about their rights is appropriate. However, we would just note our comments on proposals 12.1-12.3 on the potentially conflicting obligations to both provide more information but also to simplify how it is provided.
18.9	An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.	Please note our comments for proposals 18.1, 18.3, 18.4.
18.10	An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding. An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	
Automated decision making		
19.1	Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.	COBA is concerned with the potential wide-ranging impact of these proposals. These proposals would likely see significant amounts of proprietary commercial information being made

Number	Proposal	COBA Comment
		publicly available and create a significant risk of abuse. This creates reputational risk and could potentially cause significant brand damage. Many of our members make use of automated decision-making, for example, as part of making assessments on and processing of credit applications or loan approvals. Information on how banks make decisions on credit applications is commercially sensitive and its release would be anti-competitive as the criteria of how an individual bank makes these decisions would be made available to its competitors. Additionally, there is a high risk that if this information is made publicly available it could be used by fraudsters and other bad actors to identify a bank's safeguards and assist these people in their 'gaming' of the bank's processes. Our member's automated decision-making systems are already subject to extensive internal and external auditing to ensure that they meet the relevant legislative and regulatory requirements. Customers of banks subject to automated decision-making already have access to existing and effective complaint mechanisms both within the bank and externally to AFCA. We would also suggest that the information that is to be provided to be limited to that which is actually helpful and understandable to individuals. Due to the complexity of these IT systems, it is likely that if all the detail of an individual were made available it would be too complex and provide a level of minutiae that is not helpful to the individual. Additionally, providing this level of detail would likely be burdensome as our members would need to conduct detailed searches. COBA's view is that these proposals need to have an exemption to refuse to release information where the
19.2	High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.	
19.3	Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	

Number	Proposal	COBA Comment
		information is commercially sensitive, or the information could facilitate fraud. Additionally, the information that is provided should be limited to that which can help the customer understand how their information is being managed. An approach similar to that provided in our comments to proposals 12.1-12.3 would be appropriate. COBA welcomes the opportunity to work with AGD and the OAIC in implementing these proposals and the development of any guidance.
Direct marketing, targeting and trading		
20.2	Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.	COBA requests more detail and clarity in how these would apply in practice. We suggest that an appropriate exception be provided where the direct marketing is providing the customer with an alternative product to their existing product or information that is in the customer's interest. This exception should be limited in the case of children to only apply to basic banking products, such as transaction and deposit accounts. For example, APP 7 currently prohibits our members from proactively offering customers better pricing when rolling out of fixed rate home loans if they have opted out of receiving marketing material. Such communication would be 'direct marketing' as defined, even though it is related to a contracted event. The ability for APP entities to achieve better customer outcomes should be considered by AGD as it approaches regulating or reviewing obligations in this area.
20.3	Provide individuals with an unqualified right to opt-out of receiving targeted advertising.	
20.5	Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.	
20.9	Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	
Security, retention and destruction		
21.6	The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions	COBA recommends as part of this review that the Commonwealth should also seek to identify and improve the

Number	Proposal	COBA Comment
	appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial. However, this review should not duplicate the recent independent review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979* and the independent reviews and holistic reform of electronic surveillance legislative powers.	clarity of those provisions on when an entity can destroy or de-identify personal information, noting the various overlapping retention and destruction obligations in various laws.
Overseas data flows		
23.2	Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).	COBA supports this proposal.
Enforcement		
25.7	Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.	COBA strongly opposes the introduction of an IFM for the OAIC. The OAIC is an economy-wide regulator and not a sector specific regulator or agency, such as APRA, ASIC, and the Financial Services Compensation Scheme of Last Resort. The single industry role of these agencies is not analogous with the economy-wide role of the OAIC. The OAIC and its regulatory remit is far broader than these other agencies. Collection, use and disclosure of personal information permeates all businesses, industries, and government agencies. This would result in an extremely complex funding model that would not be efficient or effective in equitably raising funds. While COBA recognises that OAIC functions will be expanded under these proposals we believe that the funding of the OAIC should continue to come from general revenue. The privacy protections and cost of

Number	Proposal	COBA Comment
		regulating this regime should be borne by every Australian individual and entity and the most effective way to raise these funds is through general taxation. If an IFM is adopted for the OAIC then proportionality and equity would require all government agencies, even all employers, to be included in the funding model. As above, we note that an IFM is likely to be so administratively inefficient and belies the purported benefit that will be gained from adopting the model. Government agencies and larger listed businesses create most of the regulatory risk and would attract most of the OAIC's attention. In our view it would be appropriate that they bore a significant proportion of the cost. This would help cover the cost of the likely exclusion of small businesses from the IFM regime due to complexity. Our members already participate in several IFMs and pay state and federal taxes, and due to their smaller size and privacy risk we would expect to see any fees imposed on our sector to reflect this.
Notifiable data breaches scheme		
28.2	(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.	COBA believes that the proposed 72 hours is too short a period to effectively respond and mitigate any activities that caused a breach. If the 72 hours is proceeded with then there should be consideration given to what information can be realistically confirmed or reasonably known within that period. This means that the information to be reported will be limited to a high-level understanding of what happened, an estimate of customers impacted, and known data fields compromised. Clarity is needed on when the 72 hours starts (e.g., when the breach occurs, or when the breach is originally identified, or when the scale of the breach has been determined) and clear guidance on when it will be necessary to make the report.

Number	Proposal	COBA Comment
	(c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.	Consideration should also be made to allowing reporting entities to provide the OAIC a follow-up report to notify it that the breach is no longer a notifiable data breach following its further investigation. It is also unclear if the 72 hours includes weekends and public holidays. This is an important consideration as breaches can happen late on a Friday or just before a public holiday and can be targeted to take advantage of the lower staffing numbers over the weekend or public holiday. If the 72 hours is not to be limited to business days, then we would suggest that there be some additional flexibility provided to regulated entities where the breach occurs immediately prior to a weekend or a public holiday to recognise the constrained resources the entity is operating under. Alternatively, COBA suggests that the 72 hours reporting period could be limited to those circumstances where there is an identified significant risk of harm. In other circumstances where there is not a significant risk of harm then a longer reporting period could apply, e.g., five days or a week.