Insurance Council of Australia

10 July 2023

Tasmania Law Reform Institute
Private Bag 89
Hobart

Tasmania 7001

By email: Law.Reform@utas.edu.au

Review of Privacy Laws in Tasmania

Thank you for the opportunity to provide feedback to this inquiry. The Insurance Council of Australia (Insurance Council) is the representative body for the general insurance industry in Australia.

As outlined in the Tasmanian Law Reform Institute Discussion paper (the Discussion Paper), the Commonwealth Attorney General's Department is currently undertaking a broad review of the *Privacy Act 1988 (Cth).*

The Insurance Council has provided a detailed submission to the Commonwealth review (attached) and we continue to engage with the Commonwealth Attorney-General's Department in relation to the proposed Federal reforms.

As referenced in the Discussion Paper, consistency and harmonisation across jurisdictions should be a key goal when designing laws to address privacy issues.

Similarly, unnecessary duplication of existing Commonwealth laws and regulations should also be a key consideration in any state and territory reforms.

We note that the proposals of the Commonwealth Privacy Review report will be considered in the drafting of the Tasmanian Law Reform Institute Final Report. However, many of these proposals will require further consultation before any changes to the *Privacy Act 1988 (Cth)* are made.

We also note the Federal Government is yet to provide a response to the Commonwealth Privacy Review report. There also remains uncertainty over the breadth of reforms that the Federal government will take forward, that could then be replicated at state and territory level.

Therefore, given the importance of ensuring national consistency and avoiding unnecessary duplication, the Insurance Council request no changes be made to privacy law settings in Tasmania until the completion of the Commonwealth review and any changes to the *Privacy Act 1988 (Cth)* are complete.

Thank you for the opportunity to provide feedback. If you have any queries, please contact Tom Lunn, Senior Policy Manager, Regulatory Affairs at tlunn@insurancecouncil.com.au or on 0418 251 326.

Kind regards,

Andrew Hall
Executive Director and CEO

Insurance Council of Australia

06 April 2023

Hon Mark Dreyfus KC MP
Attorney General
Attorney General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

By Email: privacyactreview@ag.gov.au

Dear Attorney-General

Consultation on the Privacy Act Review Report 2022

The Insurance Council of Australia (ICA)[1] represents general insurers. We support the protection of privacy and alignment of privacy law with global standards, and particularly welcome the attention given to privacy in the online environment.

Executive Summary

The privacy environment has changed significantly since the 2014 changes to the Privacy Act, seeing an increase in the volume of data handled by businesses and organisations; greater reliance on data; and concurrent increased threats from cyberattacks and identity theft. These trends increase the risk of disclosure and misuse of personal information.

In advance of a more detailed response to the proposals we highlight the following contextual matters.

1. Adoption of Digital IDs and other secure technologies will improve personal information security.

The government should enable the adoption of Digital IDs by amending legislation to allow acceptance of Digital IDs as an alternative to the 100-point check and other identification processes. While the development of means of storage and access to personal information has made personal information more accessible than ever before, the process for providing proof of identity still relies on original documents. Digital IDs and other technological innovations can transform proof of identity by reducing the requirement for businesses and organisations to collect and hold documents containing personal information. By limiting collection and retention of such documents to the Digital ID provider, the number of places where personal information is held would reduce, as would the risk of disclosure and misuse.

[1] The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 89% of private sector general insurers. As a foundational component of the Australian economy the general insurance industry employs approximately 60,000 people, generates gross written premium of $59.2 billion per annum and on average pays out $148.7 million in claims each working day ($38.8 billion per year).

We note that the Digital ID will not completely solve the problem of collecting identification documents as the insurance industry may still have a legitimate reason to collect this information, for example, to validate that a person was a legal driver when processing a motor claim.

2. Review data retention laws, simplify obligations and enable management of collected data.

The government should focus on timely destruction of redundant data including reforming data retention laws that add complexity and constraints on entities and delay destruction of redundant data.

3. Time and resources will be required to transition to the new legislation.

Significant time and resources will be required to implement any changes to operations and processes, products, governance, and technology systems. Entities should be given sufficient time to adjust to the new legislation. Implementation should be phased over at least 2 years from when the legislation is passed and anticipated guidance from the Office of the Australian Information Commissioner (OAIC) is made available. This would be consistent with the implementation of the General Data Protection Regulation (European Union) (GDPR) as suggested throughout the Report.

Key points

This section provides a summary of the more detailed responses to the proposals contained in Attachment A to this submission and should be read in conjunction with that attachment.

1. Further clarification, guidance and consultation is required on several the practical implications of the proposed changes, including but not limited to proposals 4.3, 4.4, 4.5, 4.6, and 21.4. The importation of GDPR style rights into our existing privacy legislation also requires careful consideration, to ensure the outcome aligns with public expectations. We suggest further consultation is required on proposals 18.1, 18.2, 18.3, 18.5, 19.1, 19.3, the whole of chapter 20, and proposal 21.8. Further work is also required to inform how entities can identify people experiencing vulnerabilities under proposals 17.1 to 17.3.

   We welcome the opportunity to participate in further consultations on these and other matters. We also suggest any proposed regulatory reform impacting small business should be carefully considered and should take into account a range of factors including the risk profile of these businesses, potential increases in compliance burden and costs and expected benefits in terms of increased privacy protections. Regardless of the application to small business, greater transition support will be required for various entities, including small business, to improve data security in advance of the potential removal of the small business exemption. The proposal to remove the small business exemption may also increase the risk of personal data breaches occurring, potentially adding to claims related costs.

2. Changes which could cause confusion for consumers should be avoided. For example, entities should be able to continue to use their privacy policies as their APP 5 notice (chapter 10) and the up to date requirement should be reserved for significant changes only (Proposal 10.1). Proposal 21.8 and 28 will also require careful consideration to ensure customers are not adversely affected.

3. OAIC guidance should be provided on the content of privacy policies and collection notices in preference to the imposition of standardised templates. Guidance should also be provided by the OAIC on the proposed activities contained within proposals 13.1, 13.3, and 13.4.

4. Some proposals have a risk of causing delays in claims processing, stalling of an insured's claim or legal proceedings, or otherwise delay or overly complicate insurance activities. Proposal 11.1, 11.3, 15.1 should be carefully considered to avoid negative unintended consequences. Further, ensuring a child consents (chapter 16) should be a matter for entities to set their own risk-based approach.

5. There are areas where express insurance permissions should be included, for example to help prevent fraud and protect vulnerable people and the public.

6. Careful consideration needs to be given to changes to the domestic legal framework flowing from these proposals. In particular:
   - Civil penalty provisions should be limited to mid-tier civil penalty provisions to preserve OAIC resources and reduce costs to small business (Proposal 25.1);
   - Additional OAIC funding would be most appropriately sourced from general taxation rather than an inefficient business tax (proposal 27.5);
   - The direct right of action should only be commenced with thorough investigation and just cause, and following exhaustion of all OAIC conciliation processes; and
   - If intending to adopt aspects of international law, there should be consistency with international law across both permissive and restrictive elements.

We trust that our submission is of assistance. If you have any questions or comments in relation to our submission please contact Alexandra Hordern, General Manager, Regulatory and Policy, on 0411 281 790 or ahordern@insurancecouncil.com.au

Yours sincerely

Alexandra Hordern
General Manager, Regulatory and Policy
Insurance Council of Australia

Attachment A

4. Personal information, de-identification, and sensitive information

Proposal 4.2: Non-exhaustive list of information which may be personal information

It would benefit APP entities to include in the proposed non-exhaustive list specific examples of technical information, inferred information and generated information. We ask that for all types of information defined in the Act, there is a non-exhaustive list of information that could fall within the definition.

If examples are not in legislation, we ask that that they are provided in guidance in a timely fashion to allow for implementation. Ideally, we would like the draft guidance at the same time as when the draft law is published. The guidance should also specify the types of scenarios in which such information could be present. This would also be beneficial for small businesses, some of which will need to implement these privacy obligations and privacy risk management practices for the first time.

We appreciate data may be personal information given context. Equally beneficial would be a list of examples of personal information that would not be considered reasonably identifiable and the type of indicators to look for to test identifiability.

Proposal 4.3: Definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

It would benefit APP entities to define the terms "inferred" and "generated" information or provide examples of how inferred or generated information can be collected. If the intention behind this proposal is to make clear that personal information that is created by an APP entity is personal information, we suggest this is not included in the definition of collection as it is confusing, even for an individual. We recommend that the data that results from processes of collecting, inferring, and generating information is information that can be "collected, inferred or generated".

An alternative recommendation would be to move towards a definition of personal information that encompasses all activities that "process" personal information which would move the Privacy Act closer to the GDPR and cover all activities that include personal information. The proposal seems to be attempting to identify and define the activities that can be done with personal information which makes understanding when personal information is protected both for individuals and organisations more complicated.

Proposal 4.4: 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances

In the recent 7-Eleven determination, the OAIC found that a record pertaining to an individual that is unique to that individual, would constitute data that is reasonably identifiable. This interpretation may however not work in all cases. Records may be distinguished from others but not be re-identifiable. For example, a record could contain ranges instead of the data itself, such as an age range rather than an age or date of birth. Guidance on what type of records with examples that would be considered unique and distinguishable and hence reasonably identifiable would be useful. For example, would using a cookie identifier that can link data across devices without knowing whether an individual is a customer or not be considered reasonably identifiable?

Background on 7-Eleven determination

7-Eleven rolled out facial recognition technology supplied by a third party to collect customer feedback in stores across Australia. The tablets took facial images and converted it into a

faceprint when a customer first interacted with the survey, and after completing the survey, in order to match survey results to understand customer demographics. 7-Eleven claimed the faceprints were not personal information as they were not used to identify, monitor or track individuals and the third party's system was independent of 7-Eleven's and that none of the information collected by the facial recognition technology was matched with any other personal information.

The OAIC indicated in the determination:

> *"...customers' facial images were analysed to generate faceprints. These faceprints were compared to other faceprints to identify faceprints that were sufficiently similar. The Facial Recognition Tool also directly linked individuals' faceprints with survey responses, by using each faceprint as an 'identifier' to detect if the same individual was leaving multiple survey responses. These processes enabled an individual depicted in a faceprint to be distinguished from other individuals whose faceprints were held on the Server. Accordingly, I am satisfied that individuals depicted in faceprints were reasonably identifiable."*

Proposal 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.

This definition implies de-identified data could be personal information at any point in the de-identification process. The ICA believes that adding this definition would mean that the definition of both personal information and de-identified could apply to the same information at some points of the de-identification process. For example, there are three possible scenarios:

(a) Data which is only personal information and has not been de-identified

(b) Data which is both personal information and de-identified information (e.g., de-identified but re-identifiable).

(c) Data which is only de-identified information and is no longer personal information (e.g., data that has been aggregated such that it cannot reasonably be re-identified).

Scenario (b) would mean that the definition and obligations of both personal information and de-identified information would apply. An example could be a table of the number of people that own a type of car in a postcode in Australia, with one record showing that only one person in a particular postcode owns a particular car. While the data is derived from personal information it may be reasonably identifiable depending on the context and may be de-identified, again depending on the context. Two different individuals could have the same access to the data, and only one has ability to re-identify the data.

It would be simpler if the definition of personal information included *data that is reasonably likely to be linked with other personal information to reveal the identity or reasonably reveal the identity of an individual.* This is because not all de-identified information can be re-identified. For example, it would not be possible to identify individuals from a table of one hundred records containing two columns with a postcode and two brands of car. There is useful guidance in other jurisdictions which can be considered, for example the UK ICO Anonymisation Code, which contains useful concepts in establishing when de-identified information is reasonably likely to be reidentified.

Further, we believe that with the evolution of privacy enhancing technologies, it can be possible for data to remain de-identified without it ever posing a risk to individuals. For example, identifying values

could be replaced with random text or scrambled data and the remaining unscrambled data records may not be distinguishable.

Nevertheless, we believe further guidance is required on what distinguishes de-identified information from personal information and from anonymised information, as well as standards that APP entities can refer to, to manage re-identification risk.

The definition of "anonymisation" as stated in section 4.4.1: "which may only be achievable by aggregating individuals' data together" provides clarity that aggregated data is not de-identified or personal information.

Proposal 4.6 states: Some APP 11.1 and APP 8 protections to apply to de-identified information

We suggest that if de-identified data needs the same protections as personal information, then it should be included in the definition of personal information. This would remove the need for overlapping requirements as data used as part of the de-identification process may already be considered personal information and truly de-identified data would not require unnecessary protections.

It is unclear how APP entities are expected to know whether third parties have the means to re-identify the data. Some APP entities interact with hundreds or thousands of suppliers who may receive personal or de-identified information. We would welcome guidance on how to practically fulfil such an obligation with a large volume of suppliers. Standard Contractual Clauses recommended under Proposal 23.3 could include this provision to make contractual negotiations easier.

Another challenge for the insurance industry is that it is often required by law to share data with third parties that is de-identified. An example of this is insurers would be mandated to share data with the Australian Reinsurance Pool Corporation an Australian Government entity which then has a broader privilege to use and share data under the *Data Availability and Transparency Bill* 2022. We believe that as we are already required to protect personal information, the same protections should apply to the sharing of de-identified information with third parties that is required by law. We would welcome clarification on whether these obligations should apply to organisations that are required by law to share de-identified data with third parties.

Proposal 4.6: Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice

We would welcome clarity on how de-identified information could be used to target individuals that are not identifiable or reasonably identifiable. The determination by the OAIC for 7 Eleven would treat such information used to target individuals as reasonably identifiable.

Proposal 4.10: Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent.

Whilst we agree in principle with this proposal, we note that obtaining an individual's consent may not be possible in all circumstances. For example, geolocation tracking data may be collected by an insurer for the purposes of providing discounts to customers based on driving behaviour. Under this scenario, the driver of the car may not always be known to the insurer, for example, under a policy insuring a corporate vehicle. There should be sufficient flexibility in this requirement so that an APP entity would not be non-compliant if obtaining consent was not practicable.

5. Flexibility of the APPs

Proposals 5.1 & 5.2 – Making of APP Codes

The ICA suggest that further guidance should be provided regarding the steps that the Attorney-General should be required to take in determining that 'there is unlikely to be an appropriate industry representative.

As recognised in the Report (at 5.1), any APP Code is likely to have impacts across multiple sectors of the economy, where there are multiple appropriate industry representatives (e.g., different industry associations). Greater clarification is required regarding the process that the OAIC would use to seek to identify an appropriate lead organisation (or organisations) before the A-G determined that no appropriate industry representative could develop a code.

Further, we suggest that a period of public consultation for as little as 40 days may be insufficient to ensure broader and detailed consultation on any proposed APP Code, especially if there is only one period of consultation.

We also note that the introduction of any APP Code would require reasonable transition and implementation periods (and potentially enforcement grace-periods), as resulting changes would likely require changes to systems and processes (which can take significant time). Depending on the nature and extent of changes required to give effect to any temporary code (as outlined in 5.2), there may be a tension between the urgent nature of the need for the temporary code and the necessary transition and commencement periods required to give effect to those changes.

Section 5.3 – Emergency Declarations

The ICA and its members welcome the proposals outlined in section 5.3 of the report, particularly the focus on ensuring that information can be shared between the private sector and state/territory governments following disaster events (Proposal 5.5). This was sought by the ICA in its submission to the previous Discussion Paper.

Insurers note that Emergency Declarations under the *Privacy Act* have only been issued on three occasions – in relation to the 2009 Black Saturday bushfires (Victoria), 2011 floods (QLD/NSW) and 2020-21 Black Summer bushfires (QLD/NSW/VIC/SA). The absence of a declaration made in relation to the 2022 East Coast Floods – Australia's largest ever natural disaster, by insured losses, indicates the high bar that is required for such a declaration.

The infrequent nature of Emergency Declarations risks undermining the benefits of information-sharing that are intended to be created by this process. Acknowledging the need for a balance between preserving privacy and efficiency in response and recovery processes, we consider that greater consideration should be given to the standard required for a declaration to be made.

Insurers are also concerned that Proposal 5.5 would not result in practical changes that enable the Emergency Declaration process to operate as intended.

The different approaches to privacy legislation adopted by the states and territories mean that the possibility for information sharing under Emergency Declarations would be inconsistently applied in different Australian jurisdictions. Further, the uplift in the Commonwealth Privacy Act that may result from these proposals could mean that the requirement for 'comparable' privacy legislation at state and

territory level is in practice unachievable, at least until the states and territories embark on their own privacy reforms.

The ICA and insurers are concerned that the benefits of information sharing for Australians impacted by disaster events may not be realised unless a pragmatic approach is taken to determining equivalence of legislation. We do not consider that it would be a good public policy outcome for Australians impacted by disaster events to receive different standards of response and support through their recovery based on different jurisdictions' approach to privacy legislation.

We suggest that any reforms to implement Proposal 5.5 should be accompanied by guidance on the level of comparability required to enable the intended information-sharing, including a view on which states and territories have 'comparable' privacy legislation. This would provide insurers, government departments and other organisations involved in disaster response and recovery with greater certainty over their capacity to exchange information with state and territory agencies as soon as any reforms commence, rather than potentially delaying assistance to Australians in their time of need.

6. Small business exemption

Proposal 6.1 Remove the small business exemption

The ICA agrees with the observations about the increasing privacy risks associated with the small business sector and the associated benefits of uplifting protections to personal information held by small businesses. We note that applying the Privacy Act obligations to small businesses has the potential to increase demand for insurance, and claims related costs, for information technology, digital-environment, or personal information-related loss events, including cyber insurance.

In conjunction with the other proposals in the report, small businesses may confront significantly increased liability or regulatory exposures. We welcome the report's recognition that reform in this area will significantly increase the compliance burden on the small business sector, and the recommendation for further impact assessment before the exemption is removed. This impact assessment should also take into consideration insurance related issues. The ICA would welcome being part of this important consultation.

7. Employee records exemption

Proposal 7.1 Enhanced privacy protections should be extended to private sector employees

The ICA agrees with the report's conclusion that enhanced transparency for employees around the personal information collected and used by their employers should be balanced against an employer's flexibility to collect and use information critical to the employment relationship, and that further consultation on this issue is required.

We note that even for existing APP entities, reform in this area is likely to entail substantive changes to organisational policies and processes, as existing processes for the protection of customer privacy are adapted to be fit-for-purpose for employee records. This is further complicated by the interaction between the proposed enhanced privacy protections and existing workplace law. As such, any reform must be accompanied by an adequate transition period.

Below are several examples that demonstrate the need for balance between enhanced protection of employees' personal information and flexibility in administering the employment relationship. We would welcome the opportunity to be involved in further consultation on specific proposals regarding amendment of the existing exemption.

Specificity of collection notice to employees

We anticipate 'enhanced transparency' regarding what employees' personal and sensitive information is being collected and used for could be achieved by requiring employers to issue an appropriately drafted 'collection notice' (or similar) to employees. Such a notice might detail that information may be shared/disclosed with certain third parties to support administration of the employment relationship (eg to facilitate payroll processing / payment of wages to employees, to an external rehabilitation provider to support with an injured employee's return to work etc). The identity of these third parties may change from time to time or otherwise may not be specifically known at the time the notice is issued.

For example, an employer may be required to share personal information about an employee with an external investigator subsequently engaged to support with an investigation into alleged concerns raised during the employee's employment. This may result in a scenario where updated collection notices would need to be issued to employees each time a further party became involved in that process, creating the potential for 'notice fatigue'.

Employee not consenting to collection

Situations may arise where employees do not specifically consent to the collection, use or disclosure of sensitive information which is necessary to administer the employment relationship. For example, an employee may refuse consent to the collection of sensitive health or medical information that is needed to assess the employee's fitness for work or capacity to meet the inherent requirements of their role.

We suggest that further guidance is required in relation to the interaction between an employee's refusal to provide consent and an employer's right to issue a lawful and reasonable direction to their employees.

Destruction of employee records

Insurers already adopt reasonable steps to protect employees' personal information from misuse, loss or unauthorised access. However, legitimate concerns arise about any potential requirement to destroy employee records when they are 'no longer required' and the lack of clarity around this timeframe.

A strict obligation to destroy records after a certain period of time could be detrimental to employers in situations where access to such information may be needed some many years after an employee's employment has finished. For example:

- An employer may need to retain former employees' personal information to respond to workers' compensation or common law claims alleging mesothelioma from historical asbestos exposure.
- To discharge its obligations under the Corporations Act, an employer may need to investigate concerns raised via a whistleblower channel that relate to historical alleged incidents of reportable conduct involving former employees.

In addition to considerations as employers, the destruction of records may also hamper insurers' capacity to assess and manage claims on insurance policies that provide coverage to employers or employees (such as workers' compensation, industrial disputes, business interruption insurance, or employee dishonesty or fidelity cover).

We look forward to the opportunity to participate in further consultation on how to balance these competing interests.

Part 2: Protections

10. Privacy policies and collection notices

The ICA supports the general uplift in the quality and transparency of wording for privacy policies and collection notices. However, we are concerned about the potential practical implications of the Proposals in Chapter 10 of the Report, especially as they impact on the insurance sector.

We request that the practical implications noted below are considered in any amendments to the Privacy Act or APPs so as to avoid, in the insurance industry in particular, the unnecessary increase in the number of privacy documents (i.e. notices) needed to be provided to individuals (our insureds and potential insureds). In our view, this is counterproductive to the goal of transparency and being concise. In our members' experience, the increase in privacy related documentation (notices and policies) with insureds will in many cases overwhelm them and defeat the goal of providing choice via clearer, more concise and understandable privacy documentation.

Many of our members have recently sought to reduce the number of privacy related documents required to be read and understood by our insureds (and prospective insureds) by preparing and using, as the APP 5 notice, a single clear (and as concise as possible) privacy policy. The benefits of this are that it has in one place all of the relevant privacy information required by the Privacy Act in respect of any insurance product they are taking out at that time and any future insurance products that they may subsequently take out. That is, the individual has one document to read, understand and keep.

Of course, where insurers are providing speciality products or services that require additional personal information to be collected or have different processes to those referred to in the privacy policy, they will use a privacy notice or collection statement often referring to details (such as contact details, how to complain, exercise individual rights, etc) in the privacy policy and therefore limiting the contents of the privacy notice (or 'collection statement') to only that additional information actually required, thus avoiding duplication for duplication's sake.

Therefore, for all the Proposals for Chapter 10 (in addition to our specific comments below) the ICA recommends that entities still be able, where appropriate, to use the entity's privacy policy as its APP 5 notice, especially where this will lessen the burden on individual of multiple notices that simply repeat parts of the privacy policy.

Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise, and understandable.

As noted above, whether the privacy policy is used as the APP 5 notice or a separate collection notice is used, the ICA fully supports this goal. However, in addition to our concerns about the totality of the privacy documentation noted above, we also note that the suggested additions to collection statements (in Proposal 10.2) do threaten the aim of being concise.

The ICA also requests care be taken in the 'up-to-date' requirement to ensure it is proportionate. Given the multiple points by which personal information is collected in the insurance sector, we suggest that the 'up-to-date' obligation be triggered for significant changes to the processing rather than a review every 6 or 12 months, for example.

Proposal 10.2 List of matters in APP 5.2 should be retained.

We request this Proposal take account of our comments above and consider the goal of minimising the information in both a collection notice and in total (i.e. including the privacy notice) to that actually

required (i.e. in addition to the privacy policy of an entity). However, if a collection statement as proposed is enacted then, in our view, items 5(e) and (i) should be retained.

Proposal 10.3 Standardised templates and layouts for privacy policy 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 across the economy.

The ICA does not support the development of templates and terminology as attempts to impose uniformity can stifle competition and innovation. The ICA believes effort would be better applied to the development of the range of OAIC guidance contemplated in the Report that will be essential to implementation rather than attempting to develop standard templates that will not accommodate the myriad of products and variations, options and policy wordings offered in the insurance market.

Further there would be a risk of inadvertently minimising (a) the current obligations of entities and rights of individuals in the Privacy Act and APPs and (b) any of the Proposals in the Report should they be made law.

11. Consent and online privacy settings

Proposal 11.1 Amend definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

While the ICA welcomes the Report's desire in Chapter 11 to address current shortcomings in the implementation of the current consent obligations, our concern is that this is a significant move towards 'explicit consent' (especially as we anticipate how the 'unambiguous' element in the Proposal will be dealt with in practice).

In the insurance context of ‘explicit consent’ is not in the public interest. In fact, explicit consent (even in practice) will prejudice individual insureds by holding up claims processing as has been recognised in the UK and several EU member states, such as the Republic of Ireland (ROI), which have passed derogations and exemptions specifically related to insurance. In this regard, it may be worth noting that while most of Europe is governed under civil law systems, the UK and the ROI, the only 2 common law countries in Europe, have both elected to grant special derogations to the insurance industry.

The United Kingdom, for example, has implemented an 'insurance purpose' exemption (which is the basis for a derogation adopted in various guises in several the EU member states) and we urge consideration of a similar exemption in Australia to avoid unnecessary impacts. The 'insurance purposes' for this UK exemption to 'explicit consent' (and which we believe are relevant to avoid unintended consequences of the 'unambiguous' standard) are:

- advising on, arranging, underwriting, or administering an insurance contract.
- administering a claim under an insurance contract; and/or
- exercising a right or complying with an obligation arising in connection with insurance contract.

The ICA is concerned that a lack of clarity as to the application of 'unambiguous' in practice (without an insurance purpose exemption) will cause significant difficulty in implementing it in the insurance sector. Further we believe that the 'insurance purpose' exemption noted above is uncontroversial, in the public interest and will avoid significant disruption by avoiding complex, vague and time consuming procedures to obtain 'explicit consent' (which we anticipate will be the default in insurance for the 'unambiguous' standard), rather than risk a finding that in any specific case the implied consent relied on by the insurer to write insurance or process a claim was, in fact, ambiguous. This will also prevent, for example, third parties against whom a claim is made from using this to delay or impede processing

of a claim (or the taking of legal action) by raising technical privacy challenges around whether their consent is unambiguous. Without the exemption, this may ultimately add significantly to claims related costs and the time to process claims.

The ICA therefore recommends that an "insurance purpose exemption" (like that implemented in the UK) be included in any change arising in respect of this Proposal to make it clear and unambiguous that consent is inferred in the specific circumstances of the 'insurance purpose'.

Proposal 11.2 OAIC guidance on how online services should design consent requests….

The ICA supports this proposal requiring more guidance and, where required, detailed specific guidance on particular areas and/or for specific sectors. However, we urge that due consideration be given both to (a) the requirements of different sectors and (b) in the case of insurance, the myriad of variations, differences and options in products and services provided by different insurers on different policy terms. Care should be taken to avoid negatively impacting the amendments in Proposal 11.1, for example, by providing a 'one size fits all' template when, in insurance there are multiple products offered with an almost limitless range of alternatives, options and extras (and where no two policies by different insurers even for a similar product are the same). A standardised template/layout may be counterproductive and limit, in practice, the obligations otherwise introduced by the Proposals (and those under the current law).

Proposal 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 would not affect the lawfulness of how the personal information was handled before the consent was withdrawn.

The ICA broadly supports this Proposal but believes that, any change to the privacy should also clearly note that in certain circumstances, such as insurance, consent cannot be withdrawn without impacting the ability of the insurer to provide the relevant insurance services, such as claim processing.

Consideration should also be given to ensure that the withdrawal of consent of a party to an insurance claim or proceedings, for example, should not be able to negatively impact or prevent the exercise of a right, compliance with an obligation or pursuit of an insurance claim or legal claim by the insurer. The ICA recommends that either (a) there be a specific exemption from the right to withdraw consent for the 'insurance purpose' or (b) it generally be noted that the right to withdraw consent may be limited in relevant circumstances where it impacts (i.e. voids, in the insurance context) a legitimate claim on the insurance policy itself. That is, that withdrawal of consent should not be able to be used to avoid the processing of an insured's claim or relevant legal proceedings against that person.

13. Additional protections

13.1 – Privacy Impact Assessment for high privacy risks

The ICA and its members agree that conducting a Privacy Impact Assessment for activities with high privacy risks is a reasonable requirement, and forms part of good privacy management and governance. We also welcome the proposal for the OAIC to consult with APP entities and develop guidance on what may represent high privacy risks.

With factors relevant to assessment of high privacy risk activities to be provided in OAIC guidance, not the Act, we do not consider that it would be appropriate to include examples of high privacy risk activities in the Act itself. This approach would preserve the flexibility of the regulated privacy environment and facilitate changing community and regulator expectations.

13.3 – Guidance for new technologies and emerging privacy risks

Insurers would welcome the development of OAIC guidance regarding new technologies and emerging privacy risks.

When developing guidance on this important topic, the ICA and its members would encourage the OAIC to consult widely and to adopt an approach that seeks to achieve an appropriate balance that promotes the protection of privacy but does not inhibit innovation and development of new technologies.

13.4 – Additional requirement for APP 3.6

For organisations with complex supply chains and that utilise or obtain information from various sources to develop and provide their products or services, there may be challenges in obtaining necessary satisfaction that the information has been collected in accordance with APP 3 – particularly if (as is common) information may not have been personal information at the point it is obtained by an insurer, but becomes personal information when combined with other information provided (such as by a customer).

For example, insurers may obtain information regarding specific motor vehicles, drivers, properties or businesses from third party sources, using that information as part of determining the price of an insurance policy. Similarly, customers and others may provide information to smash repairers, builders or other parties involved in claim fulfilment, who then relay that information to an insurer.

While contractual requirements to comply with APP requirements are common, and the need to comply with privacy obligations is set out in training for insurers' suppliers regarding obligations under the *General Insurance Code of Practice*, OAIC guidance on further or additional measures that may be required to have taken 'reasonable steps' would be welcome.

15. Organisational accountability

The ICA broadly supports the Proposals in Chapter 15 of the Report but seeks consideration when drafting any changes to the Privacy Act or APPs, for both the different requirements of and modes of engagement with individuals in different sectors. For the insurance industry, given the myriad of variations and options, different service delivery models and policy wordings, we request that consideration be given to the difficulty and cost impacts of implementing these Proposals. As noted earlier, highlighting that a 'one size' is unlikely to fit all.

Proposal 15.1 An APP entity must determine and record the purpose 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.

While broadly supportive of this Proposal, the ICA requests that any change to the Privacy Act or APPs be clear and detailed as to what this requirement involves. This may be similar to Article 30 of GDPR requiring 'records of processing activities'. At this point in the evolution of the privacy law in Australia, this will be a significant impost on business economy-wide (but in particular SMEs) as shown by the experience in the EU where there were significant costs in replacement of technology (crippling in some cases) to implement the 'records of processing activities' obligations.

We therefore urge precision and clarity in wording in prescribing the relevant requirements and that appropriate exemptions be included in sectors, such as insurance, where in order to efficiently and cost effectively implement the 'insurance purpose' (see our comments in relation to Chapter 11 above).

An insurer should be entitled to process the relevant personal information (including sensitive information) without having to stop and record any secondary purposes that arises prior to finalising the claim or making payment, For example, if secondary purposes should be recorded, we suggest that leeway be given as to the timing in certain contexts, where recording secondary purposes would result in undue delay in insurance claims.

Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

The ICA supports this proposal but it is concerned that it may impose an undue financial burden on small business if the exemption is removed. We therefore recommend that some consideration be given as to whether this obligation should only apply to businesses of a certain turnover or with a certain volume or type of personal/sensitive information that they process, rather than applying it economy-wide.

Section 15.4 Privacy by design

The ICA suggests that if there is any change to the law to include mandatory PIAs, this be considered both (a) in terms of its application economy-wide or only to certain businesses – not including small business – or for particular types of information, and (b) specifically as to when a PIA is required. It should be clear when a PIA is mandated (and we suggest that this should be for high-risk processing or for specific types of sensitive information being handled) and whether, for example, it applies to small businesses or businesses with minimal personal information processing.

16. Children's privacy

Proposal 16.1: Define a child as an individual who has not reached 18 years of age.

Proposal 16.2: 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.

The ICA supports the strengthening of privacy protections for children and recognises the potential vulnerability of children to online privacy harms. Robust protections for children should recognise that young people can become active participants in the economy, and there should be sufficient flexibility for APP entities to comply with the strengthened protections for children in a way that is appropriate and context-specific.

From an insurance perspective, young people may be exposed to life experiences or events (such as learning to drive, owning a car, working, owning valuable portable assets) which introduces independent risks or liabilities which are insurable. Privacy protections should not operate to restrict or impede a young person's access to services or products which they may need to address personal interests where they are inherently separate of their parent/carers, or in the absence of either parent/carers.

We note that proposals 20.5 and 20.6 seek to introduce protections for children specific to direct marketing and targeting activities. While we agree in principle with the objectives of these proposals, a strict prohibition on direct marketing and targeting to children may negatively impact young people's choice and ability to be fully informed in making decisions about their insurance needs. There may need to be a lower age threshold for specific activities.

17. People experiencing vulnerability

People experiencing vulnerability

The ICA supports the Review Report's proposals for how Federal Privacy laws might better consider consumer vulnerability. We welcome the opportunity to participate in further consultations towards the development of OAIC guidance and policy options as suggested by the Review Report's proposals 17.1-17.3.

Consumers experiencing vulnerability

We support proposal 17.1 on development of OAIC guidance to assist with a non-exhaustive list of factors to indicate when individuals might be experiencing vulnerability.

We note the Review Report at page 161, mentions the *2020 General Insurance Code of Practice* (2020 Code)[2]. And especially calls out paragraphs 91-92 in Part 9 *Supporting customers experiencing vulnerability* of the 2020 Code, including the non-exhaustive list of factors that might contribute to a customer's vulnerability.

The Review Report also mentions the 2020 Code encourages customers to self-identify as vulnerable. This is because it might not always be possible for a general insurer to identify the customer might be experiencing vulnerability if the customer does not tell them. This may especially be the case for survivors of family and domestic violence.

We appreciate that understanding and awareness of consumer vulnerability is an evolving area and best practice approaches may change over time. We are aware a new international consumer vulnerability standard has been developed[3] and it may helpfully inform the development of OAIC guidance.

Options for supporting customers who may be experiencing financial abuse

We support proposal 17.3 for the Attorney General to further consult on clarifying the issues and identifying the options for how customers experiencing financial or economic abuse may be better supported by the Privacy Act.

As important context, we highlight the *National Plan to End Violence Against Women and Children 2022-2032*[4] which calls out the role of general insurers and other private sector businesses as workplaces and providers of consumer products. The National Plan also identifies as an action, the need to consider the impact of domestic and family violence and financial abuse in the context of the Privacy Act [5].

To complement the National Plan, Federal, State and Territory Attorneys-General are in the process of developing *National Principles to Address Coercive Control* which identifies 'financial abuse' as a possible common feature of coercive control for *National Principle 1*[6]. We suggest it may be desirable to have regard to the National Plan and Principles and the possible issues and actions they suggest if proposal 17.3 proceeds.

Through the introduction of the 2020 Code and new commitments in Part 9 *Supporting Customers Experiencing Vulnerability*, including supporting survivors, many of our members have restructured their

[2] 2020 *General Insurance Code of Practice*
[3] ISO Standard ISO 22458 *Consumer vulnerability – Requirements and guidelines for the design and delivery of inclusive service*; CFA, *Standard for responding to vulnerability* (10 June 2022); SOCAP, *Standard for responding to vulnerability*
[4] Department of Social Services, *National Plan to End Violence against Women and Children 2022-2032*
[5] See above note 2, page 118
[6] Attorney-General's Department, *consultation draft National Principles to Address Coercive Control*

businesses to set up specialist 'high care' customer support teams, trained customer-facing staff to identify and support survivors and changed systems and processes to have in place a Family Violence Policy about how the business will support survivors. ICA has also published a *Guide to helping customers affected by family violence*[7] to assist Code subscribers.

Together with our members, the ICA is looking at what more might be done by the general insurance industry to advance the National Plan. The National Principles will assist the ICA and members with continuing to build on the work already undertaken to support survivors.

As general insurers focus on supporting vulnerable customers and inclusion, their preference is for any changes to the privacy framework to support, and not inhibit, their ability to provide appropriate responses to vulnerable customers.

18. Rights of the individual

Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

(b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual

We recommend that the requirement for an APP entity to identify the source of personal information that it has collected indirectly applies to personal information collected and held from the effective date of the updated Privacy Act.

The insurance industry can have longer retention periods than most APP entities, particularly when some types of insurance is involved, which would add complexity to such requests. In certain circumstances it would be impossible to determine the source of information collected indirectly as it has not been a requirement to collect this information under the Privacy Act. This requirement will require APP entities to build processes to allow for the capture of details regarding indirect sources of information. Until now, the Privacy Act has not required APP entities to collect the metadata relating to personal information.

We would also like clarity as to the level of detail that APP entities would be required to supply to individuals about indirect sources of information and when such level of detail would need to be provided. We also recommend there are exceptions to respect the privacy of individuals. For example, a witness may provide information to an insurer regarding a claim. We recommend that for an access request, there is a clear exception not to provide information that would disclose the personal information of another individual. In such cases we recommend that APP entities should only provide access to the type of source that provided the information, in this case, a witness.

Proposal 18.2: Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

We are supportive of individuals having rights to their personal information and would welcome clarity on the purpose of the right to object in the Privacy Act. While this right appears to be drawn from the General Data Protection Regulation (GDPR), it does not appear to fulfil the same purpose and seems to be applicable in a very narrow set of circumstances.

[7] Insurance Council of Australia, *Guide to helping customers affected by family violence*

Under GDPR, individuals have a right to object to personal information in a broad set of circumstances including where the processing of personal information is: in the public interest, for a legitimate interest, for direct marketing purposes or for specific research purposes. With the exceptions outlined in Proposal 18.6, the right to object could potentially be exercised in very limited circumstances and it is unclear when the right to object could be used. This may lead individuals to incorrectly believe they have a real right to object, causing an unnecessary operational burden on APP entities in answering requests by outlining the valid reasons for retaining the personal information, rather than accepting the right to object.

Proposal 18.3 states: Introduce a right to erasure

Similar to the right to object this right appears to be drawn from the GDPR. We note that this right is likely to be misunderstood by individuals as it would only apply in a very narrow set of circumstances. Individuals may be misled into believing they have a right to seek erasure more generally, however the circumstances will be limited to data that is no longer needed. This could impose an unnecessary operational burden on APP entities in responding to individuals on why their request for erasure will not be fulfilled. We expect multiple erasure requests given the high profile this right has been given in the media in Australia since the General Data Protection Regulation came into effect in Europe.

The full report also notes: “the right would be limited to where the information should be destroyed for example by court order or under APP 11.2 as it is no longer needed.” However, the exceptions proposed in Proposal 18.6 could also apply to this right. We suggest a consistent approach is taken so that it is clear to individuals how the rights will apply (and only in limited circumstances).

In relation to the requirement to inform third parties of the erasure request, we note that third parties may share personal information with other parties, and it is not clear when the requirement ends. We suggest that extending the right beyond third parties where there is a direct contractual arrangement in place would be disproportionate, or impossible.

Proposal 18.5: Introduce a right to de-index online search results containing personal information

We would welcome clarity on the intention behind this proposal, specifically whether “online search results” refers to online search engines such as Google or Bing, or whether it also includes search results on APP entity websites or internal intranet sites. For example:

- Should the employee record exemption be removed, this requirement could also apply to any board members, CEO, leadership team members or employees mentioned on any APP entity website. We therefore suggest that an exception is introduced where individuals sit in specific roles that are publicly known or are on other public registers.
- APP entities have internal directories on intranets to facilitate searching for employees. We recommend that if the employee exemption is removed, that an exception is added to this right to allow employers to provide a directory on their intranets for staff.

In addition, the Australian Link definition now being much broader, that is data does not need to be held or collected within Australia. We would also welcome clarity as to whether this would apply to entities with websites overseas that may produce search results containing personal information of Australians.

It is also suggested that within the legislation there is further clarity to confirm that the individual must make the request to de-index to the APP entity publishing the personal information, not the APP entity that may be associated with the data, For example, a customer of an APP entity should contact the

search engine publishing the link to a news article mentioning the customer's name along with the APP entity, especially if the APP entity has provided comment to the media.

Proposal 18.6: Introduce relevant exceptions to all rights of the individual

We presume that these exceptions are intended to bring the Privacy Act in line with the GDPR. Further clarity is required on which right the relevant exceptions would apply to. Read broadly this section could imply that there would be very few requests that would not fall within one of these exceptions. Again, this would create an illusion of individuals possessing rights that they do not have and increasing the operational burden on APP entities in responding to rights requests and complaints that may arise following the refusal.

We would also recommend clarity on what "contract with the individual" means. Specifically, whether it also includes:

- Purposes outlined in a Privacy Policy or APP 5 Notice which are referred to in legal agreements with a customer, such as Terms and Conditions or Product Disclosure Statements.
- Employment contracts, policies referred to in these contracts, and/or purposes outlined in a Privacy Policy or APP 5 Notice.

*Proposal 18.7: 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 indi*vidual.

We note that there are circumstances in which notification of rights and obtaining disclosure is not practicable at the point of collection. For example, when an insurance claim is lodged, an insurer may collect information related to third parties prior to the insurer having any direct contact with that third party.

The ICA suggests that the proposal to require an APP entity's procedures for responding to the rights of individuals within privacy policies be reconsidered. Currently, privacy policies contain information about an individual's rights and how these rights can be accessed. Extending this disclosure to include an APP's procedures would significantly increase the volume of information required to be disclosed and is inconsistent with the report's competing objective to keep privacy policies concise. From a consumer perspective, our experience is that action-oriented disclosure around how individuals can access their rights is more valuable than information on an APP entity's procedures.

19. Automated decision-making

The ICA supports the proposals in Chapter 19 of the Report relating to more transparency and clearer disclosure of what personal information is involved in automated decision making (ADM) as proposed in Proposal 19.1. However, we urge care to ensure that this does not inadvertently include the release of intellectual property or proprietary information as to the workings of the ADM technology.

As noted above in respect of Chapter 11 and 'explicit consent', the ICA suggests that any 'insurance purpose' exemption also be included in (and not inadvertently overridden by) the Proposals in Chapter 19. We note the issues around sensitive information and information which might otherwise require consent under the Report Proposals would also be relevant in respect of automated processes and ADM in insurance too. The ability to 'opt out' of ADM and/or the ability to withdraw consent for processing generally would significantly disrupt the insurance industry and lead to significant claims processing delays.

Proposal 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.

Whilst supporting this Proposal in principle, the ICA urges caution to ensure that any changes to the Privacy Act or APPs are proportionate to the proposed goal. In accordance with Proposal 19.2, it should be clear that the types of decisions subject to the obligation in Proposal 19.1 are decisions that have a legal or significant effect on an individual's rights and not every automated process. There are significant levels of automation in the insurance sector, and we are concerned that a lack of clarity and precision to limit this scope to the intended objective will expose insurers to an unintended and significant burden.

In addition, while it may be appropriate for privacy policies to provide information about the broad subject matters in relation to which ADM occurs, it would be more practical for more specific disclosure to be contained in a privacy/collection notice.

Proposal 19.3 introduces a right for individuals to request meaningful information about how substantially an automated decision 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.

We note that the second sentence of the first paragraph of Proposal 19.3 is effectively a duplication of Proposal 19.1. We suggest that this duplication may cause confusion and ambiguity and therefore should be deleted (and only dealt with in Proposal 19.1).

We urge consideration of precise wording so this does not require the disclosure of any intellectual property, proprietary information or processes in respect of each business. We note our concern that this may lead to abuse and misuse.

We reiterate that this be limited to only those substantially automated decisions that truly have a legal or similarly significant effect on individuals' rights and that such be clearly defined. In insurance, this will help avoid significant unintended negative impacts on insurers and costs to address numerous requests on automated processes generally that do not impact an individual’s rights.

Proposal 19.3 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.

The ICA notes that insurance is a sector with significant automated processes including ADM. We urge that consideration be given to the economic impacts and disruption that may be caused, for example, by a right to 'opt out' of ADM. While we acknowledge that this is not a current proposal, we note that consideration should be given to the impacts of opting out of ADM as this would cause slower claims processing and may have other unintended consequences. We are happy to address this in greater detail if you wish.

20. Direct marketing, targeting and trading

Insurers ensure that products are marketed to customers in a responsible manner and support appropriate measures to warrant that marketing activities occur in a way that involves appropriate management of information about customers.

However, we note that the discussion in the Report frequently suggests that digital forms of marketing, particularly targeted marketing activities, involve intent that is adverse to consumers’ interests.

In addition to advertising insurance products to potential customers, insurers use targeted advertising to provide support to customers – such as following natural disasters, where insurers promote claims processes, the presence of support teams on the ground in affected areas, the availability of support packages or services, etc. Geo-targeting or use of other customer information ensures messages are targeted to appropriate audiences, improving the efficiency and effectiveness of these communications. The ICA and its members suggest that further consultation is required to ensure that any proposals taken forward to not unnecessarily inhibit insurers capacity to target such messages to provide support for Australians at their time of need.

Regarding the proposals in section 20 generally, the ICA and its members are of the view that the proposals, when combined, will do little to deter or prevent 'bad actors' from using advertising for adverse purposes. Conversely, the combination of the proposed expansion of personal information to include online identifiers (many of which are dynamic, and shared across people), proposals regarding de-identified information, unambiguous consent and unqualified right to opt out, will inhibit organisations from efficient and effective marketing approaches. In addition to the potential for adverse impacts on consumer experience, any impact to efficient and effective marketing may result in increased costs to business, with broader impacts to costs of products and services.

The ICA suggests that detailed consumer research should be undertaken to understand whether the proposals would result in improved consumer experience, as well as further consultation to understand the potential impact of the proposals for businesses.

Further, we suggest that these proposals should be considered in the context of the ACCC's ongoing Digital Platforms Inquiry and cyber-security reforms, which may impact businesses' use of data (including for marketing purposes). As much as possible, co-ordination across government should ensure that the outcome of these consultations and reforms is a consistent and effective regulatory regime on the collection, storage, and use of personal information.

Comments on specific proposals are below.

Proposal 20.2: Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.

Whist we agree in principle with this proposal, we suggest further consultation as there are some practical challenges with implementing opt-out requests. Participants in the marketing value chain will hold varying amounts of data. If an individual requested to opt out, their identity and all their data points need to be reconciled to a single-view-of-customer to be effective. This may require the acquisition of more identifying data to be collected by more participants in a value chain to give effect to general opt out requests. True single view of a customer is complex and difficult to obtain, especially in legacy businesses or businesses that participate in intermediated distribution/acquisition or fulfilment/supply chains.

20.3: opt-out from targeted advertising

The proposal is unclear on whether the onus is on the advertiser or the publisher to facilitate and manage an opt-out request.

The right to opt out of targeted advertising may be best achieved by linking it to the act/practice of data matching in order to 'target' the intended consumer, as the identity of the consumer may not be known to an advertiser (who may have minimised collection of identification information, and but unable to identify a consumer beyond a data point such as mobile number or email address).

Proposal 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.

Proposal 20.6: Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Whilst we support robust protections for children, we note that these prohibitions would require all prospects for direct marketing to have age data collected or declared before marketing to ensure that the recipient is not a 'child', or where they are a 'child' their personal information has been collected directly from them and the direct marketing is in their best interests. If the best interests test cannot be satisfied at a general level, an APP entity may be required to collect additional personal information to determine whether the direct marketing/targeting is in a child's best interests.

21. Security, Destruction and Retention of Personal Information

Proposal 21.4: Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.

As indicated above, we suggest that information is classified as personal information throughout the de-identification process until it is de-identified. This would simplify the obligations for APP entities, address the risk around protecting data that is in the process of being de-identified, and remove the need to apply the same controls on de-identified information as personal information. For example, a de-identified data set containing age ranges and the number of customers in those age ranges for a product, should not need the same protection controls as personal information.

We suggest the wording could state:

> *Amend APP 11.1 so that APP entities must also take reasonable steps to protect personal information where there is a reasonable likelihood that it could be re-identified.*

We note this requirement places a large burden on organisations to protect information where it would be impossible to re-identify or would never be re-identified.

Proposal 21.8 Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.

The ICA recommends further consideration on this proposal, which could focus on information destruction rather than retention period disclosure. Further, legislation that requires data retention could be reviewed to enable more timely destruction of data that is no longer required for insurance purposes.

We query the usefulness of such disclosure to consumers, as specific periods of retention can vary significantly within a business and likely to be confusing to individuals. As periods of retention are designed to relate to business use cases, including for use cases internal to the business (such as retained evidence, controls assurance, due diligence, etc) the disclosure may not be meaningful to individuals in many cases.

The requirement to specify retention and deletion practices in privacy policies may disadvantage insurance, banking, superannuation and financial services businesses which provide long-term products and services to consumers. Publicising these longer periods of retention may, contrary to the objective of privacy protection, attract adverse attention by cyber-criminals.

In addition, we note that for general insurance, certain state-sponsored insurance schemes (e.g. Workers Compensation and CTP insurance) set specific legislative requirements around retention periods.

If the Government is minded to requiring additional transparency on retention periods, the ICA would suggest that a general description of the purposes personal information is retained and practices relating to disposal is sufficient to meet this objective.

Part 3 Enforcement

25. Enforcement

The ICA does not support proposal 25.1(b) for a low-level civil penalty provision supported by infringement notices. We believe this proposal would set the bar too low for the imposition of penalties. We believe that proposal 25.1(a) for mid-tier civil penalty provision is a more appropriate level for civil penalties.

Further, a low-level infringement notice-based system is not appropriate for the privacy regime as infringements are based on strict liability and typically involve administrative oversights such as a failure to maintain a register. To support an infringements system a range of strict liability offences would need to be legislated that would have little connection with the more complex harms the Privacy Act seeks to prevent. Further infringements reverse the onus of proof so that businesses, including small businesses, must decide between paying a fine that can be issued without due process or challenging the infringement in the courts. Finally, it would divert resources into low level compliance checking of a small proportion of businesses covered by the Privacy Act.

The ICA does not support proposal 27.5 to investigate an industry funding model. The Act has broad application across the Australian economy and under proposals in the report to private individuals. Existing funding through consolidated revenue aligns revenue raising (through general taxation) with the scope of application of the Act.

Insurers are highly regulated and contribute to the cost of industry specific regulation. For example, insurers are subject to APRA's CPS 234 (Information Security) which overlaps with other privacy regulatory obligations to a degree. General insurers are members of the Australian Financial Complaints Authority (AFCA), which provides an avenue for external dispute resolution and can hear cases involving privacy breaches.

26. A direct right of action

The ICA does not support a direct right of action on the premise that additional channels outside the OAIC are needed to support compliance with the Privacy Act. The ICA notes the proposed direct right of action model is designed to limit cases using the direct right of action to those where OAIC conciliation has been undertaken and proven to be unsuccessful or cases where conciliation is not suitable and that the OAIC will have a role in advising the courts on the suitability of cases that seek leave from the courts.

The ICA is concerned that the large number of cyberattacks and associated personal data breaches could lead to a proliferation of actions, including representative actions and class actions under the proposal.

27. A statutory tort for serious invasions of privacy

We note the recommendation is to introduce a tort for *serious invasions of privacy*, drawing on the ALRC 123 model that includes, *that invasion must have been committed intentionally or recklessly*. The recommendation then broadly aligns with the ICA submission to the review, that should a statutory tort be introduced; it should be confined to *intentional or reckless invasions of privacy*.

If the government proceeds with a statutory tort of privacy, further consultations around the level of statutory damages should be undertaken.

Finally, with respect to the direct right of action, the ICA notes that this needs to be considered in conjunction with the statutory tort. The ICA recommends that the direct right of action and statutory tort should be mutually exclusive.

28. Notifiable data breaches scheme

Proposal 28.1 Facilitating reporting for notifiable data breaches (NDB)

The recommendation that the OAIC streamline reporting is supported. An uplift in the notifiable data breach form itself, in addition to the supporting tools is required. For example. The draft NDB training version of the reporting form on the OAIC website has not been uplifted to match the live NDB form.

It is noted that the NZ Privacy Commissioner has a useful self-assessment tool to help understand whether a particular incident is considered reportable under the Privacy Act 2020 (NZ). The OAIC could develop a similar tool to help entities assess and report eligible data breaches in a timely manner.

Proposal 28.2 Eligible data breach notification – 72 hours

Notification to the OAIC

The proposal to reduce the time taken to notify the OAIC of an eligible data breach is not supported.

The significant reduction in time may increase the overall number of reports, providing an inaccurate reflection of the total number of breaches occurring as APP entities prepare 'holding' statements, rather than adequately informed notifications to the OAIC. It may also result in increased administration as some notifications may be withdrawn when the entity concludes its investigations and determines that the initial assessment was incorrect. The quality of reports to the OAIC will be significantly degraded, as many facts surrounding the breach are only determined after appropriate investigation occurs.

Per the July - December 2022 NDB Report[8], it is noted that 29% of entities took longer than the 30 days to report eligible data breaches. 23% were unable to identify the breach within the 30 days, indicating some entities are struggling to comply with the existing 30-day reporting requirement.

It also will be a challenge for APP entities to carry out an investigation, gather all required information and report to the OAIC within 72 hours. Particularly if a data breach occurs on a Friday, which would trigger reporting by Monday morning. This will require internal investigations, assessment and escalations over the weekend.

Further, if the incident involves a third-party vendor, contracts may mandate certain timeframes (for example 48 hours) for a third party to notify of a data breach. It may be challenging to get outsourced

[8] OAIC, Notifiable Data Breaches Report (July-December 2022)

providers to commit to a shorter timeframe and the organisation may need further time to work with the vendor to ensure compliance with its own reporting obligations.

The current requirement to take reasonable steps to complete an assessment within 30 days of the entity becoming aware of a suspected eligible data breach remains sufficient.

Notifying impacted individuals

The proposal to provide notification to the OAIC around steps the entity has taken or intends to take in response to the breach within 72 hours will be challenging when the context of the breach is not yet known. This may also increase 'notification fatigue' which will result in increased anxiety, or a degradation in effectiveness (particularly where notification is too broad or does not address how the individual can take steps to protect their personal information).

Whilst the OAIC notes that the rationale of the scheme should not be undermined by 'pursuing a tailored notification at the expense of timely reporting', the current regime strikes the right balance between reporting and notification. APP entities need to be mindful not to produce notifications to individuals that are misleading, alarmist and inappropriate, given the intention is to empower individuals to take steps to protect themselves in the event of a data breach.

It is difficult to foresee how an entity can properly investigate and identify the type of personal information compromised or impacted customers within 72 hours. For example, in a malware data breach, the entity may be unable to identify exactly what personal information has been encrypted by the malicious actor until a significant time post breach incident.

If the 72 hour notification requirement is pursued, we propose a separate notification timeframe for notifying the customer formally. This can be further supported by company holding statements where larger scale breaches mandate communication within a shorter timeframe. These should already form part of APP entities internal data breach response plans.

The recent Latitude Financial Services data breach highlights how complex data breaches can be and the need to balance community expectations with accurate dissemination of information. The best approach is to rely on sufficiently communicated, correct and helpful communication (e.g. holding statements placed on company websites with suggestions on immediate consumer actions). Formal data breach notifications to impacted individuals in compliance with Privacy Act requirements can follow investigations once details are confirmed (e.g. within a mandated time of 30 days).

Proposal 28.3 Statements about eligible data breaches to include mitigation steps

Many APP entities already provide a statement to the OAIC indicating what steps they have taken (or intend to take) to mitigate the risk of serious harm to impacted individuals. This information is prompted in the NDB form under 'recommended steps' and again in 'breach details'. Any requirement included within the Privacy Act should be sufficiently flexible and not overly prescriptive, to allow entities to tailor appropriate responses to data breaches.

Further, entities regularly take reasonable steps in practice to prevent or reduce harm to individuals that is likely to arise as a result of data breaches. For example, adding fraud flags to compromised accounts. However, assistance is often best placed in supporting impacted customers to protect their own personal information, rather than imposing a requirement that organisations take active steps themselves.

Proposal 28.4 Attorney General to permit the sharing of information with entities in response to an eligible data breach event.

This proposal is supported in principle.

29. Interactions with other schemes

The ICA and its members support the intended outcomes of the Proposals in Section 29 of the Report, particularly the need for increased co-ordination across government to ensure consistent and efficient approach to regulation of privacy.

To the greatest extent possible, regulation of privacy should be harmonised – both at Commonwealth level, as well as between the Commonwealth and States and Territories. For example, private sector insurers who participate in state-based statutory injury insurance schemes (such as compulsory third-party motor vehicle insurance, or workers compensation insurance) face scenarios where the same piece of information could be subject to the Commonwealth Privacy Act, state-based health information legislation, and state-based privacy legislation applying to the public sector (given the state government involvement in the statutory insurance scheme).

Obligations under state/territory legislation, particularly regarding health information, can go beyond the requirements of the Privacy Act, increasing the complexity of compliance and creating uncertainty over applicable requirements.

We strongly support the recommendations for improvements in consistency of legislative design, co-operation between jurisdictions, and the proposed working group to examine options for harmonisation. The ICA would welcome opportunities to participate in future consultation on this issue.