Ai GROUP SUBMISSION

Australian Government
Attorney-General's Department

Review of the Privacy Act 1988 – Discussion Paper

January 2022

Table of Contents

1. Introduction

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Discussion Paper for the Review of the *Privacy Act 1988* (Cth) by the Attorney-General's Department (AGD). This submission follows on from our previous submission on the Issues Paper to the AGD in November 2020.

We note that the Issues Paper stage provided the AGD with an opportunity to start the conversation regarding areas in which the Privacy Act Review could cover in a holistic way. The Discussion Paper has now been released which includes potential options to reform the Privacy Act.

However, at this time we have not yet been provided with a Regulation Impact Statement (RIS) and details of the proposed timeline for implementation of the proposed reforms. Given the extensive nature of the proposed reforms and wide-ranging impact on businesses, we submit that a significant transition period will be required should these reforms proceed.[1]

In reviewing the Discussion Paper, including various proposals and questions, we consider that the volume of material needs to be properly worked through with stakeholders.

Given the extensive review and wide implications that proposals arising from the review could have on many businesses, we propose that the AGD consider breaking down their proposals into a more digestible and manageable manner, to allow sufficient time to be considered practically. This will ensure that stakeholders are properly engaged.

For instance, we suggest the consultation could be structured and coordinated by the AGD along the following lines:

- Categorise the different areas in which the AGD considers should be prioritised in its review and consult in a more structured manner. This should also take account of appropriate sequencing of related proposed amendments including the Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (OP Bill) and associated OP Code.

- Develop a consultation schedule including timeline and action plan to address specific areas. This should include a clear statement detailing the proposed lead time for implementation by regulated entities. Timelines should recognise the continuing impact of COVID-19 on regulated businesses.

- Walk through the issues and associated proposals, which can be undertaken via stakeholder workshops for example. This should assist the AGD to properly categorise and prioritise the issues and their potential options, as noted above.

- Following proper stakeholder consultation, the AGD could provide a RIS and undertake targeted consultations focused on specific areas and proposals that arise from the Privacy Act Review.

As a matter of good policy and regulatory practice, this consultation should be based on proper identification, analysis and assessment of issues, underlying causes, options to address these issues, as well as a robust and considered cost-benefit assessment for any proposed regulatory or legislative change. We consider the above steps will be strongly contingent on these conditions. At this stage, we maintain that this work still needs to be done.

[1] As a comparison, we note that a two-year period was provided for the EU General Data Protection Regulation (GDPR).

In contrast, we do not consider that the concurrent Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (OP Bill) is an appropriate option at this stage. For various reasons stated in our submission to the AGD on the OP Bill, matters raised in the OP Bill should be considered as part of the broader umbrella of the Privacy Act Review, rather than in a separate and concurrent consultation.[2]

At this stage of the review, we maintain our positions in our previous submission to the Issues Paper. These are briefly discussed in our submission, as well as additional comments arising since our last submission in November 2020.

2. Issues and proposals for further consideration

The following is a list of key issues and considerations that Ai Group raised in our submission to the Issues Paper, which we continue to stand by, including with respect to:

- Definition of personal information:[3]
    - There should be caution against shifting emphasis of protecting consumers under the current regime to data protection under the EU GDPR. The EU GDPR is a complex scheme with qualifications and exceptions that operate to ensure that its requirements are capable of practical implementation. Adoption of definitions and other individual features of the EU GDPR risks over-inclusiveness and unworkability.
    - Consideration should be given to the impact of multiple forms of regulation in this area such as Consumer Data Right and industry specific regulations. Over-regulation has the potential to chill innovation and add costs to business.
    - Appropriate assistance should be provided for industry, including additional guidance and other ways to alleviate regulatory compliance burdens for businesses.
- Flexibility of the APPs:[4]
    - We consider the current principles-based privacy regime to be appropriate, given its flexibility to enable future proofing and therefore technology neutrality in a rapidly changing environment.
    - Government should be aware of various issues associated with adopting an EU GDPR approach. For instance, international experience suggests that the EU GDPR has been highly prescriptive, with certain provisions introducing significant burdens on regulated businesses without necessarily providing demonstrable benefit to individuals. Retaining the flexibility of the APPs would mitigate the risk of a similar outcome in Australia.
- Notice of collection of personal information:[5]
    - Government should be cognisant of the risk of cumulative increase of notifications and information overload for consumers associated with notice of collection requirements.

[2] We refer the AGD to our separate submission on the Online Privacy Bill for further information: https://www.aigroup.com.au/news/submissions/2021/online-privacy-bill-exposure-draft/.

[3] Ai Group submission to AGD (November 2020), pp. 5-6, https://www.ag.gov.au/sites/default/files/2020-12/ai-group.PDF.

[4] Ai Group submission to AGD (November 2020), pp. 7-9.

[5] Ai Group submission to AGD (November 2020), pp. 14-16.

- Government should properly assess whether there are material consumer benefits from expanding the range of requirements for giving of notice of collection requirements, and as to the content of these notices.

- Government should consider alternative options and assess their relative costs and benefits. A RIS would be of assistance in this regard.

- Consent to the collection, use and disclosure of personal information:[6]

  - Similar to the issue of notice of collection requirements, Government should be cognisant of the risk of creating information overload or consent fatigue for consumers with consent requirements.

  - There are practical implementation issues for businesses if the statute expands the range of requirements for obtaining of consent, or the form of requests for consent.

  - Opt-in consent should only be required where this has a real identified benefit to individuals and does not materially impact on the ability of businesses to continue to provide innovative services to the benefit of consumers and the broader Australian economy.

  - Government needs to properly understand the EU GDPR approach to consent. This includes the many exceptions and limitations to those consent requirements, including the legitimate interest exceptions.

  - Government should be cautious to not add a costly regulatory burden to businesses by requiring the retrospective operation of consent requirements in relation to already obtained data.

  - A proper assessment (including cost-benefit) of material consumer benefits should be undertaken with respect to any proposed consent requirements. A RIS would be welcome.

- Right to erasure or be forgotten:[7]

  - There is no evidence of consumer need for this right (over and above existing disposal requirements under APP 11), or that any need outweighs the significant regulatory burden, technical implementation issues, and substantial costs for entities that would be required to implement such a scheme.

  - Consideration should also be given to how erasure rights would impact insights that businesses develop through their own methods (e.g. inferences).

  - Proper consideration of public interest exemptions should be given to the right to erasure to ensure proper consumer safeguards are factored in and not inadvertently impacted such as in terms of ensuring privacy and security, preventing fraudulent activity and resolving later complaints or litigation.

  - Introducing this right could create a conflict with providing incentives to entities to ensure effective anonymisation of personal information to better protect against privacy risks.

  - Introducing this right could also conflict with mandatory regulatory requirements for retention of personal data.

[6] Ai Group submission to AGD (November 2020), pp. 16-18.

[7] Ai Group submission to AGD (November 2020), pp. 18-19.

- Unlike under the EU GDPR, the proposed right is not qualified through judicial oversight and ability to make public interest considerations. This should be taken into account and amended.

The above matters were discussed more comprehensively in our previous submission to the Issues Paper. We strongly encourage Government to review our previous submission regarding the above matters.

In addition, we would also like to build further in this submission on our previous views regarding:

- Definition of personal information;
- Notice of collection, use and disclosure of personal information;
- Consent of collection, use and disclosure of personal information;
- Employee records exemption;[8]
- A direct right of action;[9]
- A statutory tort of privacy;[10]
- Notifiable Data Breaches (NDB) Scheme;[11] and
- Interactions with other schemes.[12]

There are also other matters which we would like to discuss further relating to:

- The small business exemption;
- Direct marketing, targeted advertising and profiling;
- Automated decision-making; and
- Enforcement.

These matters are discussed in further detail in the remainder of this submission.

We would welcome discussing these issues and associated proposals in further detail as these matters progress further as part of the consultation process.

3. Definition of personal information

3.1 Scope

The Discussion Paper proposes various ways in which the definition of personal information in the Privacy Act could be potentially amended under Proposals 2.1 to 2.4 by:

- changing the word "about" in the definition of personal information to "relates to";

[8] Ai Group submission to AGD (November 2020), pp. 10-14.

[9] Ai Group submission to AGD (November 2020), pp. 19-23.

[10] Ai Group submission to AGD (November 2020), pp. 23-25.

[11] Ai Group submission to AGD (November 2020), pp. 25-30.

[12] Ai Group submission to AGD (November 2020), pp. 30-32.

- including a non-exhaustive list of the types of information capable of being covered by the definition of personal information;

- defining "reasonably identifiable" to cover circumstances in which an individual could be identified, directly or indirectly, and including a list of factors to support this assessment; and

- amending the definition of "collection" to expressly cover information obtained from any source and by any means, including inferred or generated information.

There is a real risk that these proposals would create a significant and inadvertent negative regulatory impact on entities and the possibilities of innovation, without necessarily providing material benefit to consumers. We note similar issues could arise if the definition of sensitive information were to be amended. These will also depend on the context and it will be important that proper consideration be given to such circumstances. For instance, it would be concerning if a changed definition unintentionally interfered with the normal operation of critical infrastructure, as well as any other service or system, that required access to such information.

Proposed amendments that expand the definition also pose risks, including information saturation where meaningful information would be lost through increased notice obligations, the inability to conduct meaningful analytics that would stifle innovation, and generally practical difficulties with notifying individuals when technical identifiers alone are collected and no further attributes are known.

As noted in our previous submission, the current definition of personal information provides for flexibility to include things like IP addresses, for example, in situations where they can reasonably identify someone (or are associated with other information that is about someone or which could reasonably identify someone). The OAIC has also pointed out in their own guidance, whether a person is reasonably identifiable "is an objective test" which depends on the "context in which the issue arises".[13] If the information could reasonably identify someone, it is already covered by the definition; and if it cannot reasonably identify someone (for example, an IP address taken in isolation), then it does not require the same level of protection as personal information.

Therefore, contextual evaluation will be critical and cannot be avoided with any proposed amendment in the definition of personal information. Such an evaluation may entail consideration of the particular circumstances of that entity, that entity's reasonable access to other information, the nature of the relevant information, and the data situation in which that relevant information is collected and handled.

It is also unclear how some of the APPs would apply to technical information. For example, data quality obligations (APP 10) and correction rights (APP 13) may not make sense in the case of technical information.

3.2 De-identification, anonymisation and pseudonymisation

Under the Privacy Act, de-identified information is not regarded as personal information and therefore not subject to the legislation. Proposal 2.5 in the Discussion Paper proposes to differentiate between de-identified information and anonymised information by requiring personal information to be anonymous before it is no longer protected by the Act. This proposal effectively means that de-identified information could become subject to the legislation.

We note that the AGD suggests that this proposal "would not impose an absolute or unworkably high standard on APP entities that use data for research or service delivery".[14] However, members

[13] OAIC, Australian Privacy Principles Guidelines, Chapter B: Key Concepts (July 2019), p. 20.

[14] AGD Discussion Paper, p. 31.

suggest that a goal to achieve complete anonymisation of consumer data is not possible in practice. For instance, the uniqueness of every individual would not preclude an individual ultimately being re-identified if other datasets (from other sources) were combined, not to mention the impact of technological advances that could enable re-identification. This issue will be further compounded if the definition of personal information were to be broadened, leading to a greater compliance burden for managing such information and inhibiting innovation. A significant investment will be required from businesses to ensure that the risk of de-identification remains unrealised.

If there were to be a delineation between de-identified and anonymised personal information, as proposed in the Discussion Paper, this also raises the question as to whether there should be a distinction made with pseudonymisation. Pseudonymisation is another safeguard for protecting personal information that we discussed in our previous submission in relation to issues associated with the AGD's proposal for a right to erasure or be forgotten.

We suggest that further assessment is needed for the practical considerations that such a proposal would introduce. We welcome further consultation for the technical standards if the Government wishes to proceed with this proposal.

4. Notice of collection, use and disclosure of personal information

4.1 Reducing matters to be notified under APP 5.2

Proposal 8.2 of the Discussion Paper proposes that APP 5 notices be limited to the following matters under APP 5.2:

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

In principle, we support the policy objective of providing consumers with transparency to better inform them regarding their privacy. Such an objective should avoid creating consent and notice fatigue on consumers. We would also support this proposal if it were to deliver such an objective, while providing entities with sufficient flexibility, simplicity and reduced burden and costs, especially those with complex operations. This could be achieved in part by limiting the amount of information provided to consumers under this proposal. However, this could be complicated if the definition of personal information were to be broadened under the proposals in the Discussion Paper, as discussed above. A proper assessment, including a cost benefit assessment, will also need to be undertaken.

We previously raised the issue of complexities and information overload for consumers associated with proposed notification obligations. For example, this could arise as a result of notifications from multiple APP and third party entities, which could be burdensome for the notifying entity as well as

providing limited value for affected individuals. Matters listed under Proposal 8.2 need to avoid creating such a scenario. For example, the items referring to third parties (fourth and fifth items) may need to be reviewed including on whether they should be removed if they do not offer any material consumer benefit. Similarly, if the purpose of personal information to be collected, used or disclosed is reasonably expected by the consumer, it may also provide no material benefit for them to be notified of such information.

In addition, standardised collection notices and templates under Proposal 8.3 may be difficult to implement for some entities and may not offer material benefit to consumers if they already have templates which are compliant.

Finally, further consideration should also be given to the practical value in treating the use of hyperlinks (as suggested in the Discussion Paper) as a potentially legitimate way for entities to provide individuals with sufficient notice to an entity's privacy policy including APP 5.[15]

4.2 Strengthening requirement for APP 5 notice

Proposal 8.4 in the Discussion Paper proposes to strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- the individual has already been made aware of the APP 5 matters; or
- notification would be *impossible* or would involve *disproportionate effort*.

For the sake of strengthening the requirement for notifications, we would be concerned if consumers were overloaded with information, such as a consequence of a cumulative increase in notifications (albeit reduced in matters under Proposal 8.2) from APP entities (including third parties). And if there were limited benefits to consumers in introducing such a new notification requirement, it would be inappropriate to create a new unreasonable regulatory burden on businesses. Therefore, regard needs to be given as to whether such a proposal will reduce information overload for consumers and be of material benefit to them. Associated with this, sufficient guidance will also be needed to clarify the meaning of "disproportionate effort", which should include a cost benefit assessment.

Setting aside this concern, we note that the exceptions under this Proposal appear to be limited and it may be worth expanding these to take into account other reasonable exceptions. For example, "lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety" is commonly referred to as a permitted general situation in several APPs that may warrant further consideration.[16]

5. Consent of collection, use and disclosure of personal information

In addition to matters that we have previously discussed regarding consent of collection, use and disclosure of personal information, we would be concerned if consent requirements were to be expanded or introduced without proper assessment of the problem, as well as material consumer benefit and cost impact on entities.

For instance, it is important to ensure that consent fatigue be avoided in a similar manner that it should be avoided through privacy notification fatigue. There may also be benefit in considering whether transparency measures such as through privacy disclosures and user empowerment can provide consumer benefit without creating unnecessary new regulatory obligations. There should

[15] AGD Discussion Paper, p. 69.

[16] Section 16A of Privacy Act.

also be an appreciation of the diversity of ways in which consent can be reasonably provided without needing to be overly prescriptive.

6. Direct marketing, targeted advertising and profiling

6.1 Definition of direct marketing

The Discussion Paper refers to OAIC guidance for the definition of "direct marketing", which "involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services".[17]

In contrast, Proposal 16.2 in the Discussion Paper applies a different definition for "direct marketing": "The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected". Associated with this, Proposal 10.4 proposes to: define a "primary purpose" as the purpose for the original collection, as notified to the individual; and define a "secondary purpose" as a purpose that is directly related to, and reasonably necessary to support the primary purpose. This expansion of the definition of "direct marketing" will have far reaching implications and lead to notification fatigue for individuals. If this proposal were to be adopted alongside Proposal 11.1, which concerns prohibited acts and practices, businesses will be less inclined to invest in innovative services that benefit customers through providing timely and targeted information (e.g. through location data).

Where entities must provide notices to individuals of the use or disclosure of personal information for the purpose of influencing their behaviour or decision as a primary purpose, additional risks emerge when coupled with Proposal 8.1, which provides that notices must be clear, current and understandable. Without further direction as to a reading comprehension threshold, businesses are at risk of failing to cater to a wide range of Australians. Further, providing concise explanations of technically complex information exposes regulated entities to risk. Guidance from the OAIC would greatly benefit businesses, or the inclusion of a legislative safe harbour would also address this risk.

Taken together, Proposal 16.2 effectively departs from the meaning of "direct marketing" provided in OAIC guidance and broadens its scope, which can lead to unintended consequences for entities. We therefore suggest applying a consistent definition, as provided by the OAIC.

6.2 Right to object to collection, use or disclosure for direct marketing

Proposal 16.1 in the Discussion Paper proposes that:

> *The right to object … would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.*
>
> *On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.*

We appreciate the intention behind the proposal is aimed to ultimately assist individuals in enhancing their awareness and understanding about the use of information for direct marketing. However, the proposal does not contemplate that such information is collected for other various legitimate reasons that would also be in the individual's interest. For instance, consumers could

[17] AGD Discussion Paper, p. 124.

reasonably expect information to be collected to enable better customer service, improve products or services, communication of targeted non-marketing information such as invoices, and protect against fraud. In this regard, loyalty schemes should benefit from being considered for exemption as an example. Such applications are not always completely known at the time of collection, which could evolve over time to meet consumer expectations.

If consumer benefit is the main objective, then allowing consumers the ability to opt-out of receiving direct marketing could be a better alternative to be considered further, as opposed to automatically adopting Proposal 16.1 and Proposal 10.4 more broadly. However, a global opt out of direct marketing with a single click mechanism as in Proposal 12.1 for example may not meet the needs of consumers and create confusion. An example of this would be a business with multiple products and services, and the consumer opts out of all direct marketing when the consumer would still like to receive offers on certain products and services. Even where a consumer may opt out of receiving direct marketing, ads may still be shown indirectly via other platforms. This could lead to blow-back on businesses even where opt outs are offered to consumers.

Careful consideration should be given to any opt out settings so that consumers and businesses can continue to benefit.

7. Automated decision-making

Proposal 17.1 in the Discussion Paper proposes that privacy policies be required to include information on whether personal information will be used in automated decision-making (ADM) which has a legal, or similarly significant effect on people's rights.

Should this proposal proceed further, clarification will be needed:

- Regarding the threshold of "legal, or similarly significant effect". The risk of non-compliance by entities due to unclear criterion should be addressed, particularly where entities will utilise artificial intelligence (AI) to support decision making in the realm of employment and recruitment.

- To ensure that both business and individuals understand the scope of information included. For instance, the language in Proposal 17.1 should be clarified and there is merit in considering that it applies only in those instances where personal information is inputted into ADM and that it does not apply more generally e.g. the use of anonymised information derived from personal information.

We note that the Discussion Paper particularly notes the use of AI for implementing ADM and also cites the AHRC's report on Home Rights and Technology, which included a number of recommendations on how Australia should regulate AI and other emerging technologies that can be used to make automated decisions.[18]

Overall, we agree that privacy is a relevant consideration in a discussion about AI and other emerging technologies, such as in Proposal 17.1. However, there are a range of dimensions and activities related to AI, not limited to privacy and human rights. We appreciate diversity of perspectives that need to be properly captured and would be concerned about the potential for fragmented and conflicting regulation or legislation that could arise in absence of proper coordination between multiple bodies on this subject. There would be benefit if privacy and other matters associated with AI were considered as part of coordinated discussion between the various Federal departments, agencies, authorities and stakeholders around policy issues that arise from new and emerging technologies such as AI. This will help to ensure that government's potential role in promoting AI

[18] AGD Discussion Paper, p. 137.

investment and uptake is not inadvertently stifled by other government activities that may inhibit it. This valuable coordinating role would also ensure consistent policy, efficient use of stakeholder resources, and helping to connect industry capability.

These are matters that we have previously raised in various submissions including to the AHRC and Department of Industry, Science, Energy and Resources (DISER).[19] Subsequent to this, we note that the Government released its AI Action Plan, and more recent Critical Technologies Blueprint and Action Plan. These and other government activities are also more broadly relevant to our point in this submission regarding the need for better coordination across Federal departments, agencies and authorities around interrelated reforms.

8. Controllers and processors of personal information

While not currently a proposal, the Discussion Paper discusses the concepts of data controllers and data processors. According to the Discussion Paper, there may be benefits in introducing such a concept in Australia, where it could clarify entities' accountability such as with the NDB Scheme, and align with international data protection and privacy regimes. However, the Discussion Paper also notes that there may be challenges in its implementation such as how it might apply to small businesses with an annual turnover of less than $3 million (which is in contrast to how these concepts have been adopted overseas).

As a general comment, to the extent that the Privacy Act review can assist with the facilitation of effective and efficient cross-border disclosure, this may be valuable for certain large entities, particularly given the nature of many of their services which require transfer of data. This is also important in terms of enabling regulatory coherence.

While we have noted caution needs to be given regarding a proposed adoption of the EU GDPR (discussed earlier in this submission), there may be benefit in reviewing further and consulting on the concept of data controllers and data processors, including a cost benefit assessment and whether they are appropriate in the Australian context. A RIS would be of assistance in this regard.

9. NDB Scheme

In our previous submission, we shared our views regarding the NDB Scheme since its commencement in February 2018.[20] Subsequent to this consultation, we provided updated views regarding the Scheme to Home Affairs in response to Home Affairs' Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives.[21]

Overall, while the Scheme may have been a useful source for analysing reasons for data breaches, more can be done to assist businesses in mitigating them from occurring in the first place.

[19] Ai Group submission to DISER (1 December 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/diser_ai_action_plan_dec2020.pdf; Ai Group submission to AHRC (26 March 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/ahrc_human_rights_and_technology_discussion_paper_26mar_2020.pdf.

[20] Ai Group submission to AGD (November 2020), pp. 25-30.

[21] Ai Group submission to Home Affairs (September 2021), pp. 16-21, https://www.aigroup.com.au/news/submissions/2021/home-affairs-discussion-paper-on-strengthening-australias-cyber-security-regulations--incentives/.

Of particular interest to the AGD's consultation, the NDB Scheme has highlighted a number of issues which we believe requires Government actions or assistance and we recommend the following:

- Address the source of malicious or criminal attacks that lead to data breaches
- Publish more frequent OAIC NDB Scheme insights reports (e.g. annually) that may help to better inform policymakers with respect to privacy and cyber security policy.
- Fund businesses with transition support to meet regulatory obligations associated with cyber security including NDB Scheme.[22]
- Develop policy options to assist businesses to mitigate data breaches from occurring in the first instance, including awareness and effective responses. This could entail further collaboration between industry and governments to co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs.
- Proper coordination between Government agencies to assist business victims of data breaches and cyber security incidents.
- Ensure the ACSC is sufficiently resourced to meet the cyber security demands of industry and the community.
- Undertake a public health approach through specific awareness campaigns targeted at industries that most often appear in the NDB Scheme reports.

10. Interactions with other schemes

In our previous submission to the AGD, we noted the various government consultations and initiatives that are relevant for consideration in relation to this review. Complexity of parallel and overlapping reform initiatives continues to be a problem and in fact appears to be increasing. In our most recent submission to the AGD on its OP Bill, we raised this issue again, noting further issues that have since arisen and wish to reiterate these points for the purposes of this consultation.

In addition to the Privacy Act Review, there are a range of other reforms, legislations and regulations that Government needs to be mindful of and avoid potential scope creep, overlap and duplication. And there is a larger impact on affected stakeholders that the RIS for the OP Bill may not fully appreciate, which is the cumulative impact of multiple forms of regulation in relation to online activities.

Without properly considering these other reforms more holistically, there will likely be similar problems as running concurrent privacy reforms as discussed above. It would also be an administratively inefficient outcome and inappropriate use of public resources if there were to be overlapping regulations and therefore overlapping responsibilities between regulators. Such complexities in overlapping regimes will also more likely lead to inadvertent non-compliance and confusion for consumers seeking to exercise their rights.

Given the interactions between these areas of reform, we also recommend that consideration be given to improved coordination within Government on these matters. It also raises the broader

[22] For example, this could include providing cyber security uplift such as education and training, compliance assessment, cyber security assessment, and cyber security investment. Such a cyber security support scheme could offer a range of security services and capabilities that can be accessed by businesses at a subsidised cost (i.e. either no or minimal cost).

question of how these fit under the Government's various strategies including the Digital Economy Strategy, Australian Data Strategy and Cyber Security Strategy.

We therefore recommend that:

- Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.

- Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations.

10.1 Online Privacy Bill

The AGD has acknowledged that there are interactions between its OP Bill and the Privacy Act Review. However, the AGD has suggested that the OP Bill "addresses the pressing privacy challenges posed by social media and other online platforms", while the Privacy Act Review "seeks to build on the outcomes of the OP Bill to ensure that Australia's privacy law framework empowers consumers, protects their data and best serves the whole of the Australian economy".[23]

However, we consider that the issues raised and solutions proposed in the OP Bill are intertwined with the wider Privacy Act Review. We are concerned if the Online Privacy Code (OP Code, arising from the OP Bill) were to be developed ahead of completion of the Privacy Act Review, without proper consideration of the practical challenges and other options including amending the Bill.

We strongly encourage the AGD to refer to our submission on its OP Bill, which goes into comprehensive detail regarding the overlap between its OP Bill and the Privacy Act Review, including practical challenges with the concurrent consultations and recommendations.

Below is a summary of our issues and recommendations in response to the OP Bill.

Issues	**Recommendations**
1. Problem and rationale for regulation	• A more detailed analysis of the problem statement should occur before proceeding with the OP Bill. The Privacy Act Review provides the perfect platform for this.
2. Interactions with Privacy Act Review	• The Privacy Act Review should take precedence over the OP Bill to ensure proper analysis, assessment and consultation of the issues and underlying causes (if any), as well as options to address these. • Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the AGD's concurrent privacy reform consultations, including the proposed approach for development of the OP Code. • If it were not possible to pause the OP Bill to allow for the Privacy Act Review to take precedence, the scope of the OP Bill should be limited to those aspects requiring Government's critical attention and subject to further consultation.
3. Interactions with other interrelated reforms	• Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.

[23] See: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.

Issues	Recommendations
	• Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations. • Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape. • Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap. • An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.[24]
4. Overly broad and disproportionality in scope of targeted businesses	• Subject to properly assessing the issues and underlying causes, Government should further clarify the businesses that it intends to target under the OP Bill. • Based on clearly defined targeted businesses under the OP Bill, Government should undertake a proper assessment of the impact on targeted businesses including cost-benefit assessment and other relevant implementation considerations (e.g. compliance time and assistance).
5. Lack of consideration of other options and solutions	• Government should explore other options to the OP Bill and these should be considered as part of the Privacy Act Review, including: ○ Providing sufficient resources to the OAIC funded by Government in the first instance; ○ Reviewing the effectiveness of the APPs; and ○ Providing businesses with transition assistance such as an industry engagement plan for enabling business privacy capability uplift, Government funding to support business uplift, and providing industry with a reasonable timeframe to meet any new compliance requirements.

10.2 Consumer Data Right

In our submission to Treasury on its Consumer Data Right (CDR) Strategic Assessment Consultation Paper, we suggested that it would be prudent for Treasury to consider integrating or aligning its CDR Review with the Privacy Act Review, especially as there are interrelated privacy and data protection regulation considerations.[25] This would benefit consumers and industry by ensuring a more integrated approach – as opposed to creating multiple and overlapping privacy regimes.

In this regard, we welcome the AGD's consideration of the potential overlap between the OP Code (as proposed in the OP Bill) and the CDR regime, with the AGD having consulted with other Government Departments on these reforms, according to the RIS.[26]

However, we would like to see more integration and coordination between Treasury and the AGD to ensure there is proper alignment of activities associated with the CDR and Privacy Act more generally. For example, as we previously raised with Treasury and the AGD, the CDR has effectively created a dual privacy regime with regulatory oversight of the CDR Privacy Safeguards by the ACCC

[24] The UK Centre for Data Ethics and Innovation is an example of a coordinating central body, https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about.

[25] Ai Group submission to Treasury (September 2021), https://www.aigroup.com.au/news/submissions/2021/treasury-consultation-paper--strategic-assessment-on-implementation-of-an-economy-wide-consumer-data-right/.

[26] AGD RIS for the OP Bill (October 2021), p. 25.

and OAIC for sectors subject to the CDR. Such an outcome creates complexity and compliance costs for businesses that have to comply with both regimes, and also for small businesses that may not currently be subject to the Privacy Act and therefore not familiar with privacy regulatory regimes. Here, there would be benefit in reducing regulatory duplication and associated red tape.

We therefore recommend that Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape.

10.3 Landscape of regulatory processes relating to online activities

We note that there are several concurrent regulatory processes initiated by government agencies and departments with a focus on online activities where these processes appear to be targeting so-called digital or online platforms. However, as noted earlier, many businesses have the capability of having an online business or platform, with online services delivered via various digital media (e.g. websites, social media, apps and other digital or online platforms) which are B2C or B2B in nature, and affect businesses of all sizes. In fact, there are only low barriers to an online presence and it is common for even small businesses today to have any online presence.

For example, in addition to the proposed OP Code:

- The eSafety Commissioner is currently overseeing industry codes being developed under the *Online Safety Act 2021* (Cth);[27]
- The eSafety Commissioner is also consulting with industry on a roadmap for the introduction of mandatory age verification and the Restricted Access Systems Declaration;[28]
- The Department of Infrastructure, Transport, Regional Development and Communications is currently consulting on the Basic Online Safety Expectations;[29]
- Home Affairs has put forward a proposal for a new cyber security code under the Privacy Act as part of its Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper;[30] and
- Most recently, the AGD has initiated consultation on its Exposure Draft of the Social Media (Anti-Trolling) Bill 2021.[31]

These concurrent activities suggest a lack of coordination across Federal departments, agencies and authorities, and a lack of appreciation by at least some of them of the potential negative cumulative impact that this could have for a wide range of businesses, not just for large technology companies.

To reiterate, there would be a greater benefit if there could be better coordination between Federal departments, agencies and authorities in relation to multiple industry codes and regulations relating to online activities that are becoming an overcrowded landscape of regulation for a wider range of businesses.

---

[27] See: https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper.

[28] See: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification; https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system.

[29] See: https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.

[30] Ai Group submission to Home Affairs (August 2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-industry-group.pdf.

[31] See: https://www.ag.gov.au/legal-system/publications/exposure-draft-social-media-anti-trolling-bill-2021.

10.4 Overlapping regulatory bodies and functions

In addition to concurrent interrelated government activities with respect to the online domain, there is a consequential risk of overlapping regulatory bodies and functions in regulating this area.

An option that has been put forward in the OP Bill is to empower the eSafety Commissioner to be an alternative complaints body to the OAIC. The rationale provided in the Explanatory Paper is to "allow information sharing to occur in the event of overlap between privacy complaints and complaints to the eSafety Commissioner – such as cyberbullying, cyber abuse and image-based abuse complaints".[32]

Another example of overlap with questionable public benefit relates to the section 52A(1)(c) of the Bill, whereby the Commissioner can require the publication or communication of a statement in those cases where there has been an interference with the privacy of an individual. This overlaps with the NDB Scheme and may cause information that is harmful to the relevant entity to be published e.g. notification of weaknesses in systems may be exploited by malicious actors if made public.

In principle, we support administrative efficiency that enables information sharing between government bodies (subject to appropriate regulatory safeguards) and reduces regulatory red tape for businesses. However, we would be concerned if the eSafety Commissioner were to be given powers that extended beyond its remit of promoting online safety and duplicating the regulatory responsibilities and functions of the OAIC with respect to privacy related matters. There should be other options explored, without necessarily expanding the eSafety Commissioner's powers that could risk creating regulatory uncertainty, overreach and duplication. It should be made clear that the eSafety Commissioner will only deal with online safety matters and the OAIC deal with privacy matters.

For instance, where privacy related complaints are determined by one regulator, the complainant should not be able to make the same or similar complaint to another regulator. This protects against regulatory double dipping and forum shopping. Anecdotal feedback from an industry member indicates that they have experienced this problem with two regulators (namely, the Telecommunications Industry Ombudsman (TIO) and OAIC). This can arise where a complainant is unhappy with a TIO decision regarding their complaint so they subsequently file that same complaint with the OAIC.

Further exploration of other options through proper stakeholder consultation could include assessing the merits of establishing a central regulatory body (under a central government department such as the Department of the Prime Minister and Cabinet (PM&C)) that can properly coordinate between the various regulators responsible for developing codes and regulations. This could enable a more holistic consideration including understanding the cumulative regulatory impacts and costs on affected stakeholders who may be subject to multiple regulations related to online activities. The PM&C also plays an important role, providing oversight of the Digital Economy Strategy, Australian Data Strategy and most recently Critical Technologies Blueprint and Action Plan, so this coordinating approach could be another advantage.

We therefore recommend that:

- Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap.

[32] AGD Explanatory Paper for the OP Bill (October 2021), p. 22.

- An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.

- Privacy complaints should be handled by one regulator, with the OAIC a likely choice given its privacy expertise.

11. Enforcement and regulation

In our submission to the AGD on its OP Bill, we commented on its proposals to strengthen regulatory enforcement powers and penalties that we consider also pertinent to the review of the Privacy Act.

Setting aside our issues with the OP Bill, we were also concerned regarding the lack of options presented in the RIS for that Bill to demonstrate that the solution offered (including the introduction of an OP Code) was the most appropriate response. This was acknowledged in the RIS where only one option had been put forward, indicating that it was to meet Government's commitment to strengthen the Privacy Act by introducing reforms to amend the Act, centred around introducing a binding OP Code and strengthening enforcement measures and penalties.[33]

We consider that good policy and regulatory practice should entail a proper consideration of various options once the problem has been properly assessed, rather than immediately leaping to one solution. This is more reason why the Privacy Act Review should take precedence over the OP Bill and properly consulted upon.

11.1 Providing sufficient resources for the regulator

We are cautious with proposals to strengthen regulatory enforcement powers and penalties without a proper assessment of whether the regulator (in this case, OAIC) has the sufficient resources funded by Government to execute its functions. For instance, there may be adequate regulations in place, but the regulator may have insufficient resources. If the regulator were to be provided with sufficient resources that contributed to addressing an identified issue, then this suggests that the regulations in place are sufficient. We suggest this would be a more prudent step rather than immediately resorting to legislative reforms associated with enforcement (such as the ones proposed in the Discussion Paper) in the first instance.

11.2 Providing business transition assistance

While the OP Bill heavily focused on traditional regulatory approaches such as amending legislation, creating new regulations, and increasing enforcement powers and penalties, there lacked alternative solutions that may be more productivity enhancing and effective. For example, there is an important role that the Government or OAIC can provide through developing business uplift with respect to privacy.

Consider the NDB Scheme under the Privacy Act as an example. While the OAIC produces half-yearly reports about the Scheme, it would be useful for the OAIC to develop with industry more proactive initiatives to help mitigate such breaches occurring in the first place, as noted earlier. The introduction of the mandatory NDB Scheme left many businesses stranded with a compliance mindset as opposed to providing them with adequate uplift support – this is likely to be an even more significant issue for SMEs. While the RIS for the OP Bill briefly mentioned about how businesses may benefit from improved OAIC education material and programs based on the OAIC's increased ability to understand emerging systemic privacy issues, it would be useful to see an industry engagement plan developed that clearly spelt out meaningful actions (including resourcing, scheduled initiatives and collaboration with key stakeholders) and measures of success. This could

[33] AGD RIS for the OP Bill (October 2021), p. 13.

be co-designed with industry to develop a genuinely effective and mutual outcome that benefits the Australian community. Again, this is an example of a matter that should be considered as part of the broader Privacy Act Review.

If it were decided to proceed with an amendment to the legislation that could lead to some form of OP Code for example, it will be important that companies are provided with proper transition support from Government to meet these new compliance requirements. This will be especially important for companies that are not traditionally subject to these types of online activity reforms. These companies will need as much assistance as possible to ensure that they are properly accounted for. This includes Government funding and being provided a reasonable timeframe to meet any new compliance requirements. It is important to note that this is not necessarily about providing funding support for large technology businesses, but about SMEs and wider industry that may be captured under these requirements with practical uplift support. Related to this, relevant industry associations that might be required to develop industry codes should be properly identified, consulted with and appropriately supported by Government (including funding and resources) to undertake such activities.

12. Small business exemption

The small business exemption in the Privacy Act remains a necessary part of the regulatory system and should be neither removed nor narrowed. The exemption serves a necessary purpose in ensuring businesses are not overly burdened by the compliance measures necessary to satisfy the APPs.

Small businesses would benefit from being provided with assistance in terms of "best practice" in safeguarding personal information. However, the Australian Government should not impose strict requirements which small businesses may struggle to implement.

The *Privacy Amendment (Private Sector) Act 2000* (Cth) which extended coverage of the Privacy Act to some parts of the private sector included the limited exemption for small businesses from application of the APPs. The rationale for the inclusion of the exemption is clear from the explanatory memorandum which provided (emphasis added):[34]

> *All small businesses will be exempt from the operation of the legislation for a period of 12 months after the commencement of the legislation. This delayed application is designed to allow small business extra time to ensure compliance with the legislation. After the initial period it is intended that small business be exempt from the legislation unless there is a privacy risk.* ***This is in accordance with Government policy to minimise compliance costs for small business****.*

It was recognised by the drafters of the legislation that the compliance costs for small businesses would likely be exorbitant. This is also reflected in the second reading speech by the then Attorney-General in favour of the Bill:

> *Similarly, while protecting privacy is an important goal****, it must be balanced against the need to avoid unnecessary costs on small business****. For this reason, only small businesses that pose a high risk to privacy will be required to comply with the legislation.*
>
> *Small business is defined in the legislation as a business with an annual turnover of $3 million or less. Such businesses will be exempt unless they hold personal health information and provide a health service, trade in personal information, are a Commonwealth contracted service provider or are prescribed by regulation.*

[34] Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*, p. 5.

The power to prescribe small businesses, or particular acts or practices of small businesses, provides a flexible way to ensure that other risks to privacy can be brought within the legislation where that is necessary and in the public interest. In considering whether the circumstances justify bringing small businesses within the regulatory scheme, the Privacy Commissioner must be consulted. I also intend to consult with the minister for small business before making a decision on such a regulation.

In addition, small businesses will not be subject to the legislation for a period of 12 months after it comes into force. The government appreciates that small business needs to focus on implementing the new tax system. The extra time given to small business will provide ample opportunity for them to implement the changes to the tax system before turning to how they will handle personal information.

Even so, with the increasing demands from consumers and larger business partners for greater respect for privacy, more small businesses are recognising that good privacy practices are good business practices. The bill provides an excellent foundation for Australian small businesses to take the initiative voluntarily in relation to privacy. This will allow them to capitalise on the increased consumer and business confidence that results from proper practices.

The concerns expressed by the Attorney-General continue to be relevant today. Smaller businesses lack dedicated staff with an in-depth knowledge of privacy law to assist in ensuring full compliance with the APPs. For "micro-businesses", the burden of understanding and executing obligations under the Privacy Act would be substantial. With the continued COVID-19 pandemic, smaller businesses have been required to devote significant resources to ensuring State and Federal regulations, aimed at controlling the spread of the virus, are complied with. The last few years have been particularly burdensome for businesses confronted with a patchwork of mandatory control measures which have impacted their operations.

Small businesses currently in the grip of significant difficulties brought on by the current pandemic should not be subject to increased layers of regulation. More benefit is likely to result from encouraging businesses to pursue best practice outcomes in their dealings with personal information. Educative programs are a preferable strategy to encourage best practice information collection and handling.

13. Employee records exemption

For the reasons outlined in section 5 of Ai Group's November 2020 submission, we oppose any proposed narrowing of the employee records exemption. Handling of employee records is best dealt with under current workplace legislation and employers should not be subject to multiple layers of regulation pertaining to the same subject matter.

Any watering down of the employee records exemption in the Privacy Act is likely to cause significant confusion regarding the interaction with existing controls in workplace legislation and will potentially put employers at risk of contravening the Privacy Act in the ordinary course of administering the employment relationship. The ongoing pandemic has demonstrated to employers the need to procure information from workers in the form of taking temperatures or ascertaining vaccination status in order to mitigate the risk of spreading the virus. Additional restrictions pertaining to dealing with such information will further impede employers in taking such reasonable management action.

Rather than being narrowed, as proposed in our November 2020 submission there is a need to ensure that the employee records exemption is extended to cover host employers engaging in labour hire arrangements. Such businesses are not covered by the exemption and, as a result, encounter significant difficulties in dealing with personal information which is necessary to undertake reasonable management action. Host employers often need to procure health information regarding

workers to properly undertake COVID-19 containment measures. The employee records exemption needs to be extended to ensure that labour hire operations are not obstructed by the inability of host employers to deal efficiently with records pertaining to staff that are not directly engaged.

The imposition of a "fair and reasonable" test would not assist employers in retaining current administrative flexibilities regarding the treatment of employee records. The term "fair and reasonable" in the context of employee records is untested and its inclusion would encourage litigation to determine its parameters. Although a concept of fairness is currently contained in APP 3.5, any existing guidance on this term would likely be of limited assistance with respect to employment records given the unique nature of the employment relationship. Employers will be unable to efficiently discharge their obligations to their employees without retaining existing flexibilities regarding usage of personal information regarding their staff.

As outlined in our November 2020 submission, the Decision of the Full Bench of the Fair Work Commission in *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 exposed a significant shortcoming in the existing exemption in that it did not apply to records before they were held by the employer. The Decision highlighted that the employee records exemption is excessively narrow in that it restricts employers from directing their employees to provide essential information which may be necessary to implement appropriate COVID-19 protections. Ai Group urges the Australian Government to address this gap in the exemption to ensure that employers are able to request that their staff submit to temperature checks and provide vaccination status without requiring consent.

Modification of APPs 12 and 13 to provide a limited right to access or correct employee records is unnecessary and potentially opens a conflict with regulations 3.42, 3.43 and 3.44 of the Fair Work Regulations which already impose obligations upon employers and former employers regarding disclosure and accuracy of employee records. Significant penalties apply for breaching these regulations. The confusion and detriment which would arise from narrowing or removing the employee records exemption would not be ameliorated by providing a limited restriction on the application of APPs 12 and 13. Such modifications would merely overlap with existing regulation and open the way to litigation over the extent of the rights under APPs 12 and 13 in the employment context.

Introducing an additional requirement to take reasonable steps to protect employees' personal information from misuse, interference or loss would unhelpfully cover the same ground as existing requirements under reg 3.44 of the Fair Work Regulations which restricts alteration of employee records and imposes a positive obligation upon employers to ensure that certain employee records are not altered by another person except where provided for under the Regulations or the *Fair Work Act 2009* (Cth) (FW Act). Regulation 3.44(6) also prohibits a person making use of an entry in an employee record if the person does so knowing that the entry is false or misleading. Additional obligations imposed upon employers under the Privacy Act are unnecessary given the existing protections in the FW Regulations.

Any productive debate concerning the privacy obligations in place to protect employee records need to take place within the confines of workplace relations legislation which comprehensively deals with this area. Investigation and enforcement of breaches of existing record requirements are already dealt with within the framework of the FW Act. It is not appropriate for duplication to occur by removing or narrowing the employee records exemption.

14. Direct right of action

In Ai Group's November 2020 submission to the Inquiry, we opposed the introduction of a direct right of action for individual claimants and for groups instituting representative proceedings. The model proposed in recommendation 25.1 of the Discussion Paper does not constitute an appropriate regulatory response to the issues surrounding enforcement of the Privacy Act. The existing enforcement options available under the Privacy Act remain fit for purpose. Any perceived

deficiencies in the current enforcement framework should be addressed by ensuring adequate resources are available to the OAIC. Given the ongoing reform efforts by the Federal Government to regulate the class action industry, caution is needed before expanding the class action system to encompass proceeding instituted by groups under the Privacy Act.

The OAIC is well placed to evaluate contraventions of privacy legislation and take appropriate action on behalf of persons impacted by a potential breach. Any asserted deficiencies in the present enforcement framework should be addressed within the parameters currently set by the Privacy Act with the OAIC as the entity responsible for initiating such action.

Complaints and investigations relating to interferences with an individual's privacy are appropriately dealt with under Part V of the Privacy Act. Complaints may be brought to the Information Commissioner or an investigation conducted on the Commissioner's own motion. The Commissioner may take action that includes conducting a hearing or conference or making a determination which is enforceable in the Federal Court or Federal Circuit Court. The Commissioner's powers are broad and encompass a capacity to accept an enforceable undertaking or seek an injunction to prevent further breaches of the Privacy Act.

The OAIC has demonstrated capability to deal with the quantity of matters to which it is referred. In its Annual Report for the 2020/21 reporting period, the OAIC reported that it had made 17 privacy determinations, more than in any previous year. It also resolved 94% of privacy complaints within a 12-month period (more than the previous reporting period). The OAIC's most recent annual report demonstrates that 93% of privacy complaints are closed through early resolution and conciliation. The report notes that during the 2020/21 reporting period, the OAIC "introduced process improvements which resulted in reduced handling times for complaints referred for further investigation, including faster up-front assessments, streamlined investigation processes, and an increased focus on early resolution and conciliation". The Australian Government should not divert complaints away from the OAIC and toward the Court system. Regulatory responses to challenges in relation to privacy should centre on appropriate resourcing and empowerment of the OAIC.

The proposed model is not an appropriate reform in that it would enable representative proceedings to be initiated under the Privacy Act. Class action proceedings are currently beset by numerous failings which encourage speculative litigation and inflate legal costs at the expense of defendants and class members. In Ai Group's November 2020 submission, we outlined the regulatory challenges which were being examined as part of the Parliamentary Joint Committee on Corporations and Financial Services' Inquiry into litigation funding and the regulation of the class action industry. Since that submission was filed, the Committee has tabled its report which concluded that recent case law suggests that the present regulation of the class action industry is inadequate.[35] The report said:[36]

> *The growth in the scale of litigation funding, the participation of international litigation funders in the Australian market, and the frequency of windfall profits, highlights the need to reassess whether representative plaintiffs, class members and defendants are achieving reasonable, proportionate and fair outcomes.*

The Committee identified a number of areas where it saw significant value in reforming the current class action regime. In seeking to address some of those areas, the Treasury released an exposure draft of the *Treasury Laws Amendment (Measures for Consultation) Bill 2021: Litigation funders*. A consultation process in relation to that Bill took place from 30 September 2021 to 6 October 2021. The Bill formed the framework for the *Corporations Amendment (Improving Outcomes for Litigation*

[35] Parliamentary Joint Committee on Corporations and Financial Services, "Litigation funding and the regulation of the class action industry" (Report, 21 December 2020), p. xv.

[36] Parliamentary Joint Committee on Corporations and Financial Services, "Litigation funding and the regulation of the class action industry" (Report, 21 December 2020), p. xv.

Funding Participants) Bill 2021 (Litigation Funding Bill) which was also subject to a Parliamentary Joint Committee Inquiry and remains before Parliament. The Litigation Funding Bill imposes express obligations regarding the constitution of class action litigation funding schemes and sets appropriate parameters regarding claims proceeds distribution methods. The Litigation Funding Bill also places necessary restrictions on common fund orders.

The Australian Government should not institute reforms allowing privacy matters to be pursued as representative proceedings while significant problems remain in the class action system.

It is also notable that in the 2020/21 reporting period, the OAIC resolved 1,746 matters through a representative complaint finalised in January 2021. This demonstrates that multiple complainants can effectively pursue redress through the OAIC under the current regulatory system.

15. Statutory tort of privacy

A number of detriments in introducing a statutory tort for invasion of privacy were comprehensively outlined in Ai Group's November 2020 submission. The current regulatory regime is sufficient to ensure that complainants have sufficient avenues available for redress in the event that they are impacted by a privacy breach. Introduction of a statutory tort would invariably lead to an increase in litigation with associated legal and insurance costs for business, particularly if such a tort were to encompass damages for emotional distress. Businesses should not be faced with the prospect of damages pursuant to a statutory tort where appropriate recourse is currently available through the complaints mechanisms under the Privacy Act.

In the event that a statutory tort is legislated for, despite Ai Group's opposition, it is essential that an exemption for employee records is maintained given the specific complications which arise in the workplace context. For example:

- In the event that such reforms extend liability on the basis of negligence or recklessness, employers may be forced to take an overly cautious approach in dealing with employee records – for example, in the event of a medical emergency requiring the provision of an employee's health information or where a financial service provider seeks information from an employer regarding an employee's financial status;

- Employers are subject to obligations under the FW Act to provide information to certain bodies such as the Fair Work Ombudsman and registered organisations; and

- The *Building and Construction Industry (Improving Productivity) Act 2016* (Cth) (BCCI Act) empowers authorised officers to require employers to provide information which may include personal information about an employee.

There is a public interest in ensuring that employers are able to effectively manage their workforce through the reasonable use of personal information.

Present uncertainty regarding whether the common law will develop of tort of invasion of privacy over time leaves businesses in a difficult position as to determining the degree of risk to which they are exposed in dealing with information. Any proposed reforms to the Privacy Act should confirm that the legislation covers the field with respect to recourse available to a complainant and rule out the possibility of a common law tort emerging.

.

ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for nearly 150 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, ICT, transport & logistics, engineering, food, labour hire, mining services, the defence industry and civil airlines.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

OFFICE ADDRESSES

NEW SOUTH WALES

Sydney
51 Walker Street
North Sydney NSW 2060

Western Sydney
Level 2, 100 George Street
Parramatta NSW 2150

Albury Wodonga
560 David Street
Albury NSW 2640

Hunter
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300

VICTORIA

Melbourne
Level 2 / 441 St Kilda Road
Melbourne VIC 3004

Bendigo
87 Wil Street
Bendigo VIC 3550

QUEENSLAND

Brisbane
202 Boundary Street Spring Hill
QLD 4000

ACT

Canberra
Ground Floor,
42 Macquarie Street
Barton ACT 2600

SOUTH AUSTRALIA

Adelaide
Level 1 / 45 Greenhill Road
Wayville SA 5034

WESTERN AUSTRALIA

South Perth
Suite 6, Level 3 South Shore Centre 85
South Perth Esplanade
South Perth WA 6151

www.aigroup.com.au