AIIA Submission to

Privacy Act Review – Discussion Paper

22nd December 2021

About the AIIA

The Australian Information Industry Association (**AIIA**) is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

The AIIA represents the end-to-end digital ecosystem in Australia, including:

- large Australian technology, telecommunications and digital and cloud infrastructure companies;
- a large number of small and medium businesses, start-ups, universities and digital incubators; and
- multinational companies.

Introduction

The AIIA welcomes the opportunity to contribute to this Privacy Act Review – Discussion Paper and the implementation of changes made to the *Privacy Act 1988* (Cth) (**Privacy Act**).

The key objectives for the AIIA's members are to provide excellent service to their customers including by achieving efficiencies and innovating. To the extent the proposed changes to the Privacy Act allow for these objectives, including by streamlining compliance and making Australia's laws more aligned with other jurisdictions, including GDPR, the AIIA is supportive of such changes.

Whilst the AIIA supports the objective to update the Privacy Act to make it fit for purpose in the digital era, we believe a core review objective should be to ensure alignment with other jurisdictions (in particular Europe's GDPR scheme and the US) in an increasingly interconnected world where free flow of data across borders is essential for global trade, and digital services to flourish which benefit both national economies as well as the consumer. The AIIA comments on the following issues in the Discussion Paper.

Right of erasure

In light of submitter feedback, should a 'right to erasure' be introduced into the Act?

The AIIA submits that the introduction of a right of erasure would not add any additional consumer protections given the existing measures under APP11.2 and APP6 and the proposed changes to introduce a right to object. These existing protections prevent the use or disclosure for purposes other than which the information was collected or beyond the period in which the entity reasonably requires the information for the its legitimate purposes.

If it is concluded that Australia could never achieve GDPR adequacy without the inclusion of a right of erasure, this may be reason to incorporate such a right. However, as discussed below, the right balance must be struck, and the significant technical difficulties in responding to certain requests must be taken into account.

Should an erasure request be only available on a limited number of grounds, as is the case under Article 17 of the GDPR?

If a right of erasure is to be introduced, the AIIA considers that an erasure request be only available on a limited number of grounds as is the case under Article 17 of the GDPR.

What exceptions should apply to address the concerns raised in the government response to the ACCC's DPI report in relation to freedom of speech, challenges during law enforcement and national security investigations, and practical difficulties for industry?

The AIIA considers that the proposed exemptions outlined in the Discussion Paper should apply to address concerns regarding law enforcement, national security and practical difficulties. The AIIA supports a broader exception on legal grounds than just to address concerns around law enforcement. For example, entities will have their own legitimate reasons to retain information to defend or initiate potential legal claims. It might be difficult to know whether information will be required for this reason at the time of request. An obvious exemption should apply where there are existing legal proceedings on foot, but also as in Article 17(3)(e) of the GDPR, where an exemption is required for the establishment, exercise or defence of legal claims.

In particular, AIIA members would support the following exemptions:

- An exemption where personal information is required for a transaction or contract

  The AIIA agrees with the submissions that outline concerns regarding erasure requests that would result in the entity being unable to complete a transaction.

- An exemption where erasure is technically impractical or would constitute an unreasonable burden.

  There may be some argument that entities are already subject to a requirement under APP11.2, to destroy or de-identify information when it is no longer required and that this should mean they are well placed to respond to erasure requests. However, an important distinction between the obligations of an entity under APP11.2 and the proposed right of erasure is that the obligations under APP11.2 would be managed by an entity on more of a wholesale basis. The entity would build measures into its processes to manage compliance and largely be able to predict and plan for when information would likely be made on an individual or more ad-hoc basis. Additionally, the obligation under APP11.2 has a number of qualifications which are also important to take into account for a right of erasure.

The right of erasure would also need to acknowledge existing statutory record retention requirements, such as those applying to taxation and corporate records, including those required by legislation applying in foreign markets.

How would entities determine whether one of the exemptions applies in practice?

Guidance would need to be developed by the OAIC and potentially others to assist in determining whether an exemption applies in practice. This would particularly apply in relation to public interest grounds and where information is required for law enforcement. In these cases most entities would not have access to sufficient information to enable them to make informed decisions. Law enforcement concerns would be difficult for an entity to manage – for example it would not always be evident that the data was required for law enforcement proceedings, as this might not be known until a later date. By this time, the information would be destroyed and no longer available for law enforcement agencies.

In regards to other proposed exemptions, the AIIA submits that entities would likely employ a similar process to determining the applicability of existing exemptions under the Privacy Act, such as when consent is not required, when an individual's access for personal information cannot be met.

Should a right to erasure apply to personal information available online, including search results?

The same criteria should apply to information available online, including the exception where it is technically impossible or would constitute an unreasonable burden.

Other considerations

- Consistent with APP11.2, the erasure request might also be met by a provider de-identifying (or anonymising) the information. This may preserve valuable data that contributes to, for instance, medical or important social research, or improving customer experience.
- The AIIA agrees with submissions made to the effect that erasure requests should be directed to data controllers who then pass on the requests to data processors (as those concepts are described in the Discussion Paper and discussed further below). Data controllers are better able to manage this process, and data processers will often be under contractual obligations not to modify or delete any data held by them in respect of the relationship with the data controller.

Controllers and processors of personal information

The AIIA supports the submissions in response to the Issues Paper that recommended introducing the concepts of controllers and processors in the Act. The AIIA agrees that the distinction would increase the efficiency of the Act by allocating responsibilities relating to notification, consent and security.

Are there any other advantages or disadvantages of introducing these concepts in the Act?

The AIIA supports the advantages outlined in previous submissions to the Issues Paper, and does not consider that there would be any disadvantages beyond those that already exist in the Act without these concepts.

If limitations in the Act's coverage makes full adoption of these concepts impractical, would partial adoption be beneficial? If yes, how could this occur without being overly complex?

The AIIA does not believe a full adoption would be impractical. If the full adoption of the concepts were implemented the AIIA does not consider that, in practice, this would actually result in any adverse effects on the privacy of individuals. An existing analysis of breaches involving small business controllers and processors who are subject to the Act could be undertaken to determine if any would breaches would not have been reported but for this change. As the data processor is essentially only carrying out the instructions of the data controller, it also would seem unfair to subject the data processor, and not the data controller, to the Act.

Alternatively, the AIIA would still support a partial adoption such that the concepts are only introduced where both the data controller and data processor are subject to the Act, and does not consider that this would add any further complexity than is currently the case. That is because currently there is an unnecessary and undue compliance burden on a data processor that would at least be partially redressed by properly placing certain obligations on data controllers in the event they are subject to the Act. It is likely that entities would already have processes in place for dealing with small business customers due to distinctions made in consumer law and unfair contract laws.

If adopted, what obligations under the Act should processors have (record keeping, security, NDB etc.)?

It would follow that processors should have responsibilities to:

- follow the controller's reasonable and lawful instructions;
- keep data secure;
- notify the controller of a data breach to the extent it does or should be aware of it; and
- provide reasonable assistance to the controller in remedying and investigating the breach.

Overseas data flows

Proposal 1: Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

The AIIA supports the introduction of a mechanism to prescribe countries and certification schemes under APP 8.2(a). This is a common point of confusion, as entities are left to guess whether an overseas regime is equivalent.

Proposal 2: Introduce Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

The AIIA is not opposed to the introduction of standard contractual terms, but believes the SCCs should be optional. The concern with the SCCs under the GDPR is that they are very lengthy. They add unnecessary length and complexity to data processing agreements where otherwise providers are generally under pressure to present very commercial and succinct legal agreements.

Proposal 3: Remove the informed consent exception in APP 8.2(b).

The AIIA does not support the removal of the informed consent exception in APP 8.2(b), and believes the original rationale for this exception still remains valid. This is particularly relevant where there is a power imbalance between an APP entity such that it cannot get the overseas entity to agree to contractual terms.

Proposal 4: Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

The AIIA does not support strengthening the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in an entity's APP privacy policy. It is difficult enough for entities to comply with the provisions as they currently stand. Often the overseas entities have significantly more power and are therefore harder to obtain clear information from. APP entities rely on obtaining this information in order to meet their obligations to notify of certain matters under the Act. Whilst it may be argued that APP entities should not deal with such overseas companies if they are not forthcoming with this information, there is often very little choice but to do so in order to deliver certain services to end users. The AIIA does not consider that the way that Act currently operates is generating any issues for consumers in this regard (with consumers having no avenues of recourse) and that this is at best a hypothetical problem.

Proposal 5: Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

The AIIA supports the introduction of definitions for 'use' and 'disclosure' but submits that the obligation in APP8 should remain relevant only to disclosures.

Proposal 6: Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

The AIIA does not believe that the Act needs to be amended to clarify what circumstances are relevant to determining 'reasonable steps' for the purpose of APP 8.1. The OAIC's Guidance is sufficient in this instance, and the AIIA would be concerned that such an amendment would be overly prescriptive when the practical reality is that each fact scenario will introduce different circumstances for consideration.

Security and "Legitimate Interest"

All organisations should deploy cybersecurity capabilities to protect data, systems and infrastructure, and this requires monitoring networks, systems and devices for anomalous behaviour and preventing unauthorised access. To perform such functions, organisations have to process data, including data received from customers, employees and/or third parties. For example, this includes scanning IP addresses and metadata on endpoints to check for malicious activity or scanning applications in the cloud to ensure they have not been compromised. All of these actions are necessary to protect organisations against cyberattacks. For this reason, in order to process such personal data, companies rely on legitimate interest under the EU General Data Protection Regulation (GDPR) as the legal basis for processing. Specifically, the relevant recital in the GDPR is Article 49:

> *"The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned".*

The AIIA would encourage the Australian Government to adopt a similar legitimate interest principle and provide greater clarity on what constitutes legitimate interest by including a list of examples within any revised legislation. The AIIA would encourage specific reference to the use of data to improve or review an organisation's system or network security. However, we urge the Government to ensure that the definition of legitimate interest is in line with the definition in GDPR. This is important for two reasons. Firstly, many global companies have already come to rely on the GDPR definition, so the introduction of a conflicting definition could potentially inject uncertainty into global data flows and processing. Secondly, and critically, this will help ensure Australia attains adequacy with the GDPR.

Small business impact

The AIIA is mindful of the impact of an extension of privacy laws to those small businesses that are currently exempt. Any such extension would need to be staged and accompanied by appropriate education and support, with a suitable transition period before any laws and regulatory frameworks became enforceable.

The introduction of new tools, such as a default statutory privacy policy, may also reduce compliance costs.

Notifiable Data Breaches scheme

The AIIA submits that the current scheme is effective and is achieving its intended purpose, though further improvements could be made as outlined below.

- The AIIA supports the harmonisation of domestic schemes and shares the concerns of submissions that highlighted overlapping reporting obligations. If an entity reports under the centralised NDB scheme, this should satisfy its obligations under any other regime. Entities should not have to deal with multiple government agencies in respect of the same subject matter and should instead be focusing on the breach itself (please refer to *Harmonisation of domestic regulations and frameworks* for further information).

- The AIIA would also support harmonisation with international schemes and suggests this might be achieved in a similar way to the Madrid Protocol for trademarks which allows entities to submit an application in one jurisdiction and that information is shared with selected signatories throughout the world.
- The AIIA again supports submissions in favour of introducing a distinction between data controllers and processors, such as in the GDPR, to reduce confusion and compliance burdens in having multiple parties with notification obligations.
- The AIIA believes that the current obligations to report breaches 'as soon as reasonably practicable' strikes the right balance between requiring entities to report the breach promptly, and obtaining sufficient information to better ensure the notification is meaningful and not misleading to the affected individual. In any case, if the entity does not report the breach as soon as it could or should have, it faces further risk of failing to mitigate harm to individuals and being liable for any resulting loss and damage suffered as result of that delay. This should be sufficient deterrence, and overwhelmingly, organisations will want to do the right thing by affected individuals in this regard.
- The AIIA does not believe there is any utility in amending subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates. Such a requirement would be overly prescriptive and sufficient information is already including in guidance provided by the OAIC.
- Likewise, the AIIA does not believe there is any merit in revisiting the 'serious harm' threshold. The current threshold strikes the right balance and protects individuals from experiencing notification fatigue which then results in the failure to take any notifications seriously, including those which genuinely require attention.

Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues

The AIIA supports the harmonisation of privacy laws within Australia and supports a full mirroring of state and federal laws to reduce complexity of doing business in Australia. This is particularly the case for providers who are contractors to both state and Commonwealth government bodies and end up being contractually required to comply with both sets of laws and for health technology providers which also have state-based health records laws to comply with. Instead the health records laws, to the extent they serve a relevant purpose, should be incorporated into the Commonwealth Act in line with obligations around sensitive information. All aspects of Commonwealth, state and territory privacy laws that should be considered for harmonisation by this working group.

Fund the OAIC through an industry funding arrangement

The AIIA strongly opposes the introduction of an industry funding model incorporating any form of cost recovery levy or statutory levy. It is inappropriate to look to industry to fund the cost of the OAIC's activities, and simply creates another tax on doing business in Australia which should instead be collected centrally and distributed amongst government departments accordingly.

Advice on Section 26WH Privacy Act - Ransomware

The AIIA notes that in the *Notifiable Data Breaches Report: January–June 2021*, the Government observed "a number of entities assessed that a ransomware attack did not constitute an eligible data breach due

to a 'lack of evidence' that access to or exfiltration of data had occurred." The AIIA welcomes the clarification from the Government that:

> "It is insufficient for an entity to rely on the absence of evidence of access to or exfiltration of data to conclusively determine that an eligible data breach has not occurred. Where an entity cannot confirm whether a malicious actor has accessed, viewed or exfiltrated data stored within the compromised network, there will generally be reasonable grounds to believe that an eligible data breach may have occurred and an assessment under section 26WH will be required."

The AIIA encourages the Government to continue to proactively engage with key stakeholders, including those in the legal community, to ensure this advice is socialised and well understood.

Conclusion and recommendations

The AIIA supports the intent of the review of the Privacy Act to update it for a modern digital economy. A balance must be struck between providing privacy safeguards for the citizen and placing arduous reporting burdens on industry and compliance regimes. In particular, the Privacy Act should not function as an impediment to economic recovery and ongoing prosperity. As the global economy attempts to counter the effects of the COVID-19 pandemic, the implementation of onerous reporting requirements on businesses – such as overreliance on 'opt in' regulatory measures, uncertain compliance obligations or lack of alignment and interoperability with other jurisdictions – has the potential undermine economic stability. With this in mind, the AIIA supports the pursuit of the harmonisation in order to both strengthen privacy and ensure our economic interests are maintained

Recommendations

1. That the Privacy Act incorporates the distinction between 'Processor' and 'Controller' as per the General Data Protection Regulation (GDPR), for example:

   'Controller' meaning the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Commonwealth or State law, the controller or the specific criteria for its nomination may be provided for by Commonwealth or State law

   'Processor' meaning a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2. The legislation and supporting regulatory frameworks, such as reporting regimes, are harmonised to alleviate reporting overlap and other onerous requirements on companies where possible.

3. That the Government makes distinctions between small and medium-sized enterprises (SMEs) and larger entities and develops regulatory requirements that can be met by each class of organisation.

4. That the Office of the Australian Information Commissioner not be funded by industry.

If you have any questions about the content of this submission, please contact policy@aiia.com.au.

Yours sincerely,

SIMON BUSH

General Manager, Policy and Advocacy