INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

31 March 2023

Attorney-General's Department

4 National Circuit
Barton ACT 2600

By submission: https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/

RE: Privacy Act Review Report

INTRODUCTION

Thank you for the opportunity to express the Internet Association of Australia's (**IAA**) perspective in response to the Privacy Act Review Report (**Report**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet Service Providers (**ISPs**). This response will focus on proposals related to these members, primarily in representation of our members, as well as in support for the general wellbeing of the Internet and telecommunications industry.

We have been actively involved in the development of Australia's privacy law framework, having responded to the Privacy Act Review Discussion Paper (**Discussion Paper**) in January 2022, as well as the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* in November 2022. IAA and our members recognise the need for the review of the *Privacy Act 1988* (**the Act**) and for significant improvements to the regulatory privacy framework in Australia to ensure the appropriate protection of personal information, and giving individuals greater control over their data.

We acknowledge that the recent data breach incidents, many of which have been on unprecedented scales, highlight the increased threat landscape. It is widely known that cyber security attacks will only increase in volume and sophistication as we continue to evolve as a data-driven Internet economy. In that light, IAA and our members reiterate our sincere commitment to the role we should play in the protection of Australians' data. Increased security attacks targeting our data is a real issue facing all of Australia, and requires a united approach between government, the private sector, and the Australian community in order to achieve a framework that is appropriate, balanced and effective in actually protecting privacy.

To that end, we are also concerned about the focus that the Australian government seems to be taking with respect to uplifting privacy and data protection. Namely, many of the proposed reforms contained in the Report seem to be intended to increase compliance requirements and enforcement measures. Although we acknowledge the genuine need to introduce such measures, we are concerned about their efficacy, and strongly recommend that a more collaborative approach is taken.

Generally speaking, requiring entities to comply with burdensome obligations will not necessarily result in greater compliance or more secure and resilient practices and procedures. Moreover, we are concerned about the unintended adverse consequences this could result in as entities struggle to satisfy their complex obligations, face pecuniary and other penalties for failure to do so, thereby causing further impedance to the implementation of practices and protections to actually protect their data sets. This is not favourable to the entity, the individuals to whom the data relates, or the Australian government.

We are concerned that the AGD review of the Act is focusing too much on the legislative formulation whereas a more comprehensive investigation should be conducted to understand industry practice, gaps in compliance, factors contributing to any such gaps and how best to ensure compliance, which is not necessarily achieved through more prescriptive legislation and enforcement measures.

Thus, it is crucial that we collaborate to develop not only a legislative framework, but also ensure actual practices that will ensure the safe and reasonable handling of all Australians' personal information.

RESPONSE TO PROPOSALS

PERSONAL INFROMATION, DE-IDENTIFICATION AND SENSITIVE INFORMATION

Proposal 4.1 and Proposal 4.2

We do not support the amendment of the definition of personal information to information or opinion "about" to "relates to" and individual.

We understand the objective behind this amendment is to ensure that technical data such as metadata can be captured within the definition.

Firstly, we acknowledge that the Report clarifies that such technical or otherwise other data that "relates to" an individual must still be able to reasonably identify an individual to be considered personal information. We recommend this to be expressed in the Act to emphasise the requirement for any information to be capable of identifying an individual for the avoidance of any doubt. Particularly with regards to technical data, we note that not all metadata is personal information in and of itself. Therefore, emphasising this qualifier is necessary and helpful.

In addition, we oppose amending the definition to "relates to" which would have the effect of broadening the scope of personal information beyond the intentions of government to capture metadata. Instead, we recommend that this should be clarified in the Act and OAIC guidance that personal information can include technical data when it is capable of reasonably identifying a person. We believe this to be a more effective way to ensure appropriate information is captured within the definition, without resulting in unnecessary confusion as entities struggle with delineating what information 'relating to' an individual is capable of being 'personal' information.

Proposal 4.4

We strongly support the Report's explanation there will be additional support provided by the OAIC guidance to clarify terms.

FLEXIBILITY

Proposal 5.2

We recommend that a minimum public consultation period is set out even for the creation of temporary APP codes.

Proposal 5.3, Proposal 5.4 and Proposal 5.5

Similarly, we recommend that Emergency Declarations are also subject to certain minimum consultation periods. We note that the circumstances may dictate the urgency of when Declarations are required. However, it is still important that the public is engaged and that any legislation is measured and appropriate for the circumstances.

SMALL BUSINESS EXEMPTION

Proposal 6.1

We reiterate our position that the small business exemption should not be removed from the Act. If an impact analysis is to be conducted as expressed in the Report, it is more appropriate to express that the Attorney General's Department (**AGD**) will consider whether the small business exemption requires removal.

We note that in the Discussion Paper, the AGD expressed its intention to continue the small business exemption. We assume that this changed position to remove the exemption may have been influenced by the submissions received in response to the Discussion Paper urging the AGD to remove the exemption, which the Report comments the AGD to have received a large number of responses in favour of the removal of the exemption. However, we note that this is not necessarily fair nor does it necessarily accurately capture the views of stakeholders. We note that small businesses are underrepresented in consultation processes due to their limited resources to respond to lengthy papers that are often complex in nature, dealing with legislative frameworks and unfamiliar terms. Moreover, small businesses may have been further unmotivated to respond and comment on their need for the small business exemption given the Discussion Paper expressed the intention to continue the exemption, thereby not seeing the need to explain why this is important.

Moreover, we stress that the burden of complying with the APPs and other privacy obligations is extremely likely to have unintended adverse outcomes. Small businesses are not positioned to comply with these obligations because they require considerable resources and understanding of complex regulatory frameworks. In particular, in the broader context of the other proposals posited in the Report, including enforcement measures and the direct right of action being made available to individuals, there needs to be a way to draft such measures in an appropriate manner in acknowledgement of the proportionate risk, harm and resources related to small businesses.

Therefore, we strongly urge the AGD to reconsider its decision to remove the small business exemption. Rather, we support its commitment to further consultation to assess what steps are appropriate to ensure greater privacy practices by small businesses. This may include the removal of the small business exemption, if indeed it is determined such removal is necessary, but this should not be a given. IAA would be happy to work with government and other stakeholders in such a consultation to determine what measures are needed.

PRIVACY POLICIES AND COLLECTION NOTICES

Proposal 10.3

We generally support the development of additional OAIC guidance and other templates and layouts to assist entities with their creation and maintenance of appropriate privacy policies and collection notices, particularly those specific for relevant sectors. However, we support this to be done through OAIC guidance and oppose the development of APP Codes. Any standardised templates should remain as guidance, and we do not support the development of any further prescriptive regulations. It is important that industry has flexibility to devise policies and notices that are relevant to their circumstances. This also encourages entities to take a more active approach in understanding their own practices and procedures to accurately reflect these in their policies and notices.

If privacy policies and collection notices are to play a crucial role in fostering transparency over entities' handling of personal information, it is more meaningful that they consider their practices and reflect on their policies and notices as opposed to simply adopting standardised templates.

CONSENT AND PRIVACY DEFAULT SETTINGS

Proposal 11.2

We support the creation of greater OAIC guidance, particularly in respect of consent requests which can be difficult for entities – this may enable smaller entities with limited resources to understand what constitutes valid consent.

However, we again emphasise that any material that is provided is done so on a guidance basis only and the framework of consent is not overly prescriptive. There needs to be sufficient recognition that valid consent can appear differently depending on the circumstances. Any template consent requests shouldn't limit how entities issue their own requests providing they still satisfy the definition of 'consent' as proposed in Proposal 11.1.

FAIR AND REASONABLE PERSONAL INFORMATION HANDLING

Proposal 12.1

While we do not generally take issue with the development of the objective test that collection, use and disclosure of personal information must be fair and reasonable, we question whether this is expressly necessary.

Through consideration of the APPs, many of which already apply this objective test, we view the intention behind the APPs to be sufficiently clear. If it appears that entities are still collecting, using and disclosing personal information in manners that are not reasonable or fair, it suggests there are other issues underlying such practices as opposed to a deficiency in the APPs. There should be greater effort to understand why such entities have unreasonable and/or unfair personal information handling practices. We believe this to reveal more useful information that can assist government in devising strategies to ensure best practice personal information handling, more so than simply amending the legislation.

In addition, if the proposed amendment is indeed implemented, we encourage that greater clarification of the meaning and examples of "fair and reasonable in the circumstances" is provided either in the Act or OAIC guidance.

Proposal 12.2

We recommend that the following factors are also included in matters that should be taken into account when determining whether collection, use or disclosure of personal information is fair and reasonable in the circumstances:

- the kind and amount of security measures and mechanisms in place by the APP entity to protect against harm of misuse, interference and loss
- the nature or mechanism of the disclosure, particularly whether the access was authorised
- whether the personal information was subject to modification, or anonymisation/deidentification.

ADDITIONAL PROTECTIONS

Proposal 13.1

We recommend that this proposal is drafted in such a way that also specifies retention requirements for PIAs.

Proposal 13.3

The OAIC guidance materials will be what many APP entities use and rely on to understand the APPs. This will be particularly true for smaller entities if they are indeed subject to the Act. In addition, there is a potential that the guidance will be used against APP entities in the case of an investigation into an entity's compliance where it is found the entity did not adhere to the examples provided in the guidance.

As such, with respect of these new technologies, it is crucial that the guidance is appropriate, practical and effective. Therefore, we recommend the OAIC develop practice-specific guidance through engagement with relevant industries. It is important that the guidance appropriately reflects the technical nature of technologies and is actually capable of being adhered to by entities.

Proposal 13.4

We oppose this proposal as it is set out in the Report. This requirement should only be invoked in certain circumstances that depend on the kind and nature of the personal information being dealt with. While this may be intended to be implied by nature of APP 3.6(b) which allows for entities to collect personal information about an individual from third parties where it is unreasonable or impracticable to collect it directly from the individual, this "unreasonable or impracticable" limiter should also be expressly set out for the new proposed amendment.

Furthermore, there should be increased guidance provided on what is 'reasonable' in the circumstances. This should acknowledge the wide array of circumstances where it is reasonable to not take steps, as well as reasonable steps not needing to be extensive or pose unnecessary burdens.

ORGANISATIONAL ACCOUNTABILITY

Proposal 15.1

We question the need for this amendment and believe it to be sufficiently covered by APP 6 which limits the circumstances in which an entity can use or disclose personal information for a

secondary purpose. Again, if it appears that there is a gap in the practices of entities with regards to appropriately using or disclosing personal information, this suggests a lack of understanding across entities regarding the difference between a primary and secondary purpose or some other underlying issue(s) that needs addressing. Adding further requirements such as record keeping is not an efficient nor effective way of achieving improved personal information handling practices. It only creates further burdens that obfuscate the principles and objectives of the Act.

If this proposal is implemented, we strongly recommend that this amendment is drafted in a way to ensure that recording the purposes should only be for high risk privacy activities or another method of limiting this requirement. Although the Report acknowledges that making such a record will not be required where the purpose is self-evident, this should be clearly expressed in the legislation. We also recommend this is clearly expressed in OAIC guidance.

Proposal 15.2

We oppose the requirement of a senior employee to be the privacy officer of an entity. We note that this does not reflect the practices or structure of all businesses, particularly smaller businesses. The appointment or designation of an employee with requisite experience or knowledge or relevant background should be the qualifiers, as opposed to seniority. Particularly in businesses with small teams, seniority will not always equate to relevant privacy or legislative knowledge, or it will be very burdensome for senior staff to also take on this role if there are other employees more suited to the role. As such, we recommend that the requirement of the policy officer to be a senior employee be an expectation where relevant, and for this to be set out in the OAIC guidance instead of the Act.

VULNERABLE PERSONS

In general, we support greater protections for vulnerable persons and acknowledge that an individual's vulnerability can affect their capacity to provide consent due to the nature of their vulnerability. However, we posit that the general uplift of baseline protections which the other proposals strive to achieve, should be done so that this sufficiently protects individuals facing vulnerability.

In particular, we are concerned that if greater requirements and obligations are implemented with respect to vulnerable people, this could result in further invasions of privacy, and a greater requirement to obtain personal information. For example, if personal information about the person's vulnerability, which by its nature is likely to be sensitive information, is required to be recorded, this poses greater risks due to the collection of such information by an entity.

As such, we support greater consideration and consultation on the best ways to ensure protection of vulnerable individuals without exposing them and entities to increased risks.

RIGHTS OF THE INDIVIDUAL

Proposal 18.1

We support the continuation of ensuring commercially sensitive decision-making processes is a factor for consideration. We also recommend that the amendment is not drafted in such a way to encroach on other individuals' privacy through disclosure of entities' source of collection of personal information.

Proposal 18.3

We oppose proposal 18.3(b) which requires entities to notify third parties of erasure request unless it is impossible or involves disproportionate effort. We do not understand what this proposal seeks to achieve. Simply notifying other entities of an individual's request does not compel that third party to also erase their records. If that is the intention of the proposal, this suggests an assumption that individuals who have requested an entity to erase their personal information would also want the third party to also erase their information, which may not actually be the case.

As individuals are being notified of the third party who gave the entity their personal information, the decision of whether or not the individual also wants that third party to erase their records should remain with the individual.

Recommendation 18.8

We recommend the OAIC to provide guidance as to what is "reasonable assistance".

AUTOMATED DECISION MAKING

In general, we believe that the proposals listed under this chapter require greater consideration and multi-stakeholder consultation before any changes and/or requirements are implemented into the Act.

SECURITY, RETENTION AND DESTRUCTION

Proposal 21.2

In general, we do not take issue with this proposal. However, we emphasise the importance of ensuring that the baseline outcomes are not overly prescriptive or burdensome. We reiterate the need to focus on actual practices and behaviour rather than on legislative prescriptions.

Proposal 21.4

If this proposal is indeed implemented, we recommend that it is expressly stated that the measures taken to protect de-identified personal information need not be at the same level of security measures taken for personal information. There is after all, a reason why de-identification in itself is a measure set out in the APPs as a way to ensure the protection of individuals' privacy and therefore should not pose the same level of risk to require extensive security measures.

Proposal 21.6

We strongly support this proposal and recommend that this be a key focus of work for the government and any new body that is established to conduct this work.

The retention of unnecessary information from many years prior continues to present itself as a key issue in recent data breach cases, as we know companies are retaining personal information due to confusing data retention laws across different legislative frameworks.

Furthermore, in addition to retention, there should also be a focus on different legislation or agencies requiring certain personal information for verification processes. There should be concerted effort to ensure that agencies and government are not requiring businesses to utilise unnecessarily high levels of identity verification which result in the creation of honeypots for malicious actors.

Proposal 21.7 and Proposal 21.8

We strongly recommend that these proposals are only introduced after the completion of proposal 21.6 so that entities understand what the mandatory retention periods are for different data and kinds of personal information.

We reiterate that issues related to retention are due to entities being confused and generally unaware of what is lawful or not. Requiring entities to establish their own retention periods without clarifying the position at law will likely result in other unintended adverse consequences.

CONTROLLERS AND PROCESSORS OF PERSONAL INFORMATION

We support the consideration of any new concepts requiring introduction being based on the outcomes of consultation regarding the small business exemption.

OVERSEAS DATA FLOWS

Proposal 23.3

Again, we recommend that standard contractual clauses developed to assist entities with respect to transfer of personal information overseas should serve as guidance only, and not as a requirement for use. We reiterate the importance of ensuring entities are encouraged to actively consider – and actively manage – their data handling practices and policies for best practice. It is also important to allow business flexibility so that entities can appropriately balance their commercial interests as well as privacy obligations in a way that their compliance with privacy laws is genuine and meaningful.

Proposal 23.5

We recommend that in introducing this amendment, that the same caveat "where it is practicable to specify those countries" is extended so that the specification of the types of personal information being transferred overseas in collection notices is only required where it is practicable to specify those types of personal information.

ENFORCEMENT

Again, IAA acknowledges the need for enforcement measures. However, we strongly recommend that the focus should be on encouraging compliance and identifying the pain points for entities as to why they are non-compliant with privacy laws.

Proposal 25.1

If new civil penalties are to be implemented, we recommend a grace period is also introduced so that entities are given time to understand and implement new requirements.

We also recommend that penalties are also introduced with a set of considerations before penalties are enforced. Especially in the context that small business may no longer be exempt, the relative size of the entity and the effects of imposing the penalty should be considerations that are taken into account.

Proposal 25.6

Similarly, we recommend that the Act introduce a set of considerations that the Federal Court, Federal Circuit Court and Family Court of Australia take into account when making an order.

Proposal 25.10

We support the organisational review of the OAIC but encourage other focuses for OAIC instead of merely enforcement. Again, we reiterate the need for alternative means of ensuring compliance and uplift of privacy handling practices across industry as opposed to punitive measures.

DIRECT RIGHT OF ACTION

Proposal 26.1

We reiterate our position in response to the Discussion Paper and oppose the introduction of a direct right of action. Court action is a burdensome avenue for all parties involved. If some form of direct remedy for individuals is to be introduced, another arena outside of the court system should be considered. We do not see court action to sufficiently protect or assist individuals who have had their privacy interfered with, if they are to be part of long and expensive court processes.

However, if this proposal is indeed implemented, we also recommend that the legislation expressly sets out some limitation to ensure that this will not result in vexatious and frivolous litigation which would unnecessarily and extremely negatively affect courts and entities.

STATUTORY TORT

We also reiterate our opposition to the introduction of a statutory tort for privacy. However, if this is to be implemented, we recommend that there is greater consultation conducted specific to just the creation of a new tort and not just as part of the broader review of the Act. Moreover, this should be extended beyond the consultation with states and territories as proposed in the Report, and rather, should be a broader multi-stakeholder consultation.

NOTIFIABLE DATA BREACH RESPONSE SCHEME

Proposal 28.1

We support further work to be conducted to facilitate reporting processes to assist the OAIC and entities who are subject to multiple reporting obligations. Noting the highly stressful period following a data breach, we strongly support simplifying the processes involved.

Proposal 28.4

We also support changes to enable the Attorney-General to permit the sharing of information where it would reduce harm in the case of an eligible breach.

It is widely recognised that the number and sophistication of cyber-attacks will only increase as we increasingly evolve as a data-driven economy. We strongly believe that in the face of this reality, collaboration and cooperation is what is required, and we also recommend this approach be extended to the overall privacy framework.

INTERACTION WITH OTHER SCHEMES

Proposal 29.3

We strongly support the harmonisation of privacy laws. Again, we reiterate that the focus in the review of Australia's stance on privacy should be to ensure active engagement, and actually improve compliance and best practice adoption with regards to the handling of personal information. Simply toughening legislation is not the only or perhaps the best method to achieve

this. Rather, simplifying obligations so that entities actually understand what is required of them, ensuring that the requirements are effective, appropriate, and that entities are indeed capable of achieving them is what is important. We believe harmonisation of privacy laws should be conducted with this focus in mind.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the consultation on the Privacy Act Review Report. We reiterate our commitment to the development and improvement of Australia's privacy framework and understand the importance of this work. However, we stress that the best way to achieve this is not necessarily through stricter regulation. Conversely, this may have the effect of creating greater barriers to compliance. This is particularly the case in respect of small businesses who will likely feel the burden of compliance the greatest, and struggle with interpreting the legislation. As such, we strongly recommend that there is concerted and collaborative effort to investigate current industry practices and procedures to assess where the gaps are, and how best to ameliorate such shortcomings. To this end, we sincerely look forward to working with government, industry, academia, civil society and other stakeholders to devise not only privacy legislation, but also best practices for handling personal information that will actually protect individual privacy.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia