Australian Institute of Company Directors

18 Jamison Street,
Sydney NSW 2000

t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

11 October 2024

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Via email: legcon.sen@aph.gov.au

Dear Committee Secretary,

Privacy and Other Legislation Amendment Bill 2024

Thank you for the opportunity to provide comment to the Senate Legal and Constitutional Affairs Committee (**Committee**) inquiry on the *Privacy and Other Legislation Amendment Bill 2024* (**Bill**) that would amend the *Privacy Act 1988* (**Privacy Act**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of 53,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises (**SMEs**) and the government sector.

The AICD has in recent years engaged extensively on proposed privacy and cyber security reforms as part of the review of the *Privacy Act 1988* (**Privacy Act Review**), Australia's 2023-2030 Cyber Security Strategy, amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and artificial intelligence (**AI**) regulatory settings.[1]

We have also sought to support our membership to improve their knowledge of cyber security and data management best practice through extensive guidance materials and education opportunities, including the AICD-Cyber Security Cooperative Research Centre Cyber Security Governance Principles.

The AICD's policy positions on the Bill have been informed by engagement with privacy and legal experts, industry bodies and AICD members.

Executive Summary

We support reforms that will modernise the Privacy Act to ensure it reflects a digital economy where individuals and businesses are engaging, and providing personal information, in innovative ways.

However, we have urged the Government to consider legislative amendments to the Privacy Act holistically with other potential reforms in adjacent policy areas, including implementation of the 2023-2030 Australian Cyber Security Strategy and the Mandatory Guardrails for AI. A coordinated approach across portfolios must be taken to ensure policy settings and reforms are consistent, do not unnecessarily

[1] AICD submission to the Review of the Privacy Act – Report, March 2023, available here; AICD submission to the Review of the Privacy Act – Discussion Paper, January 2022, available here; AICD submission to Mandatory Guardrails for High-Risk AI, October 2024, available here.

add to the existing complexity of cyber security and data management obligations or conflict in a way that undermines their policy objectives.

We consider there is an opportunity for industry to be a genuine partner with Government in driving a 'team Australia' agenda to building data governance practices and cyber resilience. The speed at which the threat landscape has been evolving, consistent with changes in technology and personal behaviour with digital products, makes reforms focused solely on strengthening the 'stick' or creating a litigious environment surrounding personal privacy, counterproductive.

It is critical that the Bill appropriately balances strengthening how Australians' personal information is collected, stored and protected, without unduly stifling the innovative use of data or imposing unnecessary regulatory burden – particularly for smaller entities with limited resources.

Our key points are as follows:

- **Statutory tort for serious invasions of privacy:**
    - We provide qualified support for a statutory tort for serious invasions of privacy based on the model recommended by the ALRC Report 123. It is critical that the statutory tort be confined to 'serious' invasions of privacy and require a fault element of 'intentionality or recklessness'. We strongly urge these thresholds be retained in the Bill.
    - We do not support an outcome where it would be open to claimants to seek compensation for the same invasion of privacy under multiple heads of claim – for example, under both the statutory tort and a direct right of action, potentially on different evidentiary grounds. It is critical that the propensity for class actions to be brought under both redress mechanisms, potentially concurrently, be factored in - particularly in relation to data breaches resulting from a cyber attack.
    - We strongly recommend further consideration be given to how the proposed statutory tort would interact with a direct right of action should the Government seek to introduce this latter mechanism as part of future reforms. We also recommend that clarification be provided that an entity cannot be subject to two separate claims under a statutory tort and direct right of action proceeding for the same actionable conduct.
- **Keeping personal information secure – APP 11**
    - We support amending APP 11 to state that 'reasonable steps' to secure personal information includes 'technical and organisational measures'.
    - We recommend that the OAIC enhance its guidance on 'reasonable steps' under APP 11 to assist entities in protecting personal information, consistent with proposal 21.2 of the Privacy Act Review.
- **Office of the Australian Information Commissioner (OAIC) code making powers**
    - We do not support providing the OAIC with the ability to develop APP codes at the direction of the Minister. The existing industry-led code development process under the Privacy Act is sufficient and a regulator code-making power is unnecessary.
    - Providing a regulator with delegated legislation capacity should be approached with considerable caution, particularly where the code is intended to impose significant new

policy on entities. This approach could undermine the legitimate role of the legislature and risk regulator over-reach.

  - We are also concerned that giving the regulator such broad powers would result in a significant volume of delegated legislation. This would add to the complexity and challenges for entities seeking to comply with the obligations, particularly those with limited resources.

- **New penalty provisions**

  - We support the introduction of mid and lower tier penalty provisions that are commensurate with the seriousness of the interference with privacy and the OAIC being able to issue infringement notices for minor breaches of the Privacy Act.

- **Increased transparency on automated decision making**

  - We do not support the proposed changes to APP 1 in respect of the transparency of automated decision making. We consider this requirement will capture many common business tools and decision-making aids with a significant cost and compliance burden to entities. We are not satisfied this change will result in material transparency benefits that will outweigh the significant cost of meeting the requirement.

  - We are also concerned that the proposal does not align with the Government's direction on the Mandatory Guardrails for AI that is risk based (which will be subject to mandatory safety guardrails, with guardrails 5, 6 and 7 likely to intersect with proposed ADM requirements), separating AI between 'high risk and low risk' uses. We are also concerned that, as currently drafted, this obligation will onerous and costly for entities to implement.

  - We recommend this requirement apply only where the entity has arranged for a computer program has 'solely' or 'wholly' made a decision.

- **Overseas data flows**

  - We support amending APP 8 to facilitate the overseas disclosure of personal information to jurisdictions prescribed by regulations.

Enclosed at **Attachment A** are our detailed responses to the proposals.

Next Steps

We hope our submission will be of assistance to the Committee. If you would like to discuss any aspects further, please contact Christian Gergis, Head of Policy, at cgergis@aicd.com.au, Simon Mitchell, Senior Policy Adviser at smitchell@aicd.com.au, or Laura Bacon, Senior Policy Adviser at lbacon@aicd.com.au.

Yours sincerely,

Louise Petschler GAICD
General Manager, Education & Policy Leadership

Attachment A: Responses to key proposals

1. Statutory Tort for serious invasions of privacy

The AICD provides qualified support for the proposed statutory tort for serious invasions of privacy based on the model recommended by the ALRC Report 123.

However, it is difficult to comment definitively on this proposal without understanding how the statutory tort would interact with a direct right of action - the subject of earlier consultation by Government but not included in this tranche of legislation. The AICD does not, for example, have an understanding of how the Government's thinking has evolved regarding the direct right of action since providing in-principle support for the mechanism in response to the Privacy Act Review. We outline below our concerns regarding having multiple legal pathways for compensation relating to the same actionable conduct.

Our comments in relation to the statutory tort are provided with a focus on how it would operate in relation to the misuse of information. However, we recognise that a statutory tort is intended to provide a means of redress for claimants in respect of a broader conception of privacy, and privacy invasions, than what is covered by the Privacy Act (for example, an intrusion on a person's physical privacy). We also recognise that the tort would provide recourse for claimants against non-APP entities such as individuals and small businesses, not currently covered by the Privacy Act requirements.

In our view, it is critical that a statutory tort be confined to 'serious' invasions of privacy and require a fault element of 'intentionality or recklessness'. We strongly urge these thresholds be retained in the Bill.

Mere 'negligence' is not sufficient – particularly where it is proposed that the statutory tort be actionable even without proof of actual loss or damage. Further, what system or processes are deemed negligent in terms of protection of data is unclear given the evolving nature of data governance and the dynamic threat environment.

As noted by the ALRC:[2]

> *If the tort were not confined to intentional or reckless invasions of privacy, but was extended to include negligence or provide for strict liability, this would undermine an important justification for making the tort actionable without proof of damage. Rather, such an extension would require proof of actual damage to be consistent with other tort law.*

We note further that a statutory tort with a fault threshold of 'intentionality or recklessness' would be consistent with comparable jurisdictions such as the UK, New Zealand and the US.[3]

Class action risks

Our understanding of the Bill is that the proposed statutory tort, requiring a fault threshold of 'intentionality and recklessness', is generally not intended to be actionable in circumstances where an entity is the victim of a data breach caused by a cyber attack, and the misuse of information is by a malicious third party.

However, there is a risk that a lower fault threshold of 'negligence' and no requirement for a 'serious' invasion of privacy would allow potentially opportunistic class actions in respect of data breaches – particularly where: there is no requirement to prove actual loss or damage; plaintiff law firms and litigation funders have commercial imperatives that incentivise litigation; and the novelty of the law in

[2] ALRC Report 123, p. 117.
[3] ALRC Report 123, p.94.

Australia. A claim involving hundreds of thousands, or even millions of customers, could have a major financial impact on entities if a court were to determine that the appropriate compensation (including for emotional distress) was a small sum such as a few hundred dollars for each individual.

The AICD has been involved in past reforms to the regulatory settings and commercial incentives driving Australia's attractiveness for securities class actions and litigation funding. We have received market feedback that those pre-reform settings resulted in adverse economic and legal consequences, including a D&O insurance market that has until recently been in crisis.[4] We consider that any legislative reforms that provide new avenues for class actions should be carefully considered and proportionate to the harm suffered by claimants.

Special considerations for data breaches stemming from cyber attacks

In many cases, data breaches are the direct result of third-party cyber attacks which continue to regularly impact Australian entities, large and small, private and public, government and non-government, in a dynamic and high threat operating environment. Even organisations with the most rigorous cyber security practices, that take all reasonable steps to protect their data, can fall victim to sophisticated, sometimes state-sponsored, cyber attacks. Certain organisations may face heightened exposure given their critical role in the Australian economy (e.g. critical infrastructure providers), and the unsettled state of geo-politics currently.

In the aftermath of a data breach, public policy settings should incentivise organisations to focus on response and recovery, as well as appropriate protection and remediation of affected individuals, rather than encouraging responses with litigation risk front of mind.

Again, it is critical that the statutory tort be confined to 'serious' invasions of privacy, involving 'intention or recklessness' so that negligence on the part of an entity, the subject of a data breach, does not give rise to a cause of action in these circumstances.

We recommend that clarification be provided in the Explanatory Memorandum about what constitutes "misuse of information" to make clear that where an entity is a victim of a data breach and a third-party misuses personal information, the entity would not be liable where they had no knowledge or were not reckless in regard to that risk. This addition would be consistent with the example provided in the Explanatory Memorandum that "a defendant who establishes a digital platform that is used by a third party to invade privacy would not be liable where they have no knowledge of the invasion of privacy".

Cumulative impact of multiple redress mechanisms

The AICD, in our submission to the Privacy Act Review, has previously raised strong concerns with the cumulative impact of multiple redress mechanisms should both the statutory tort and a direct right of action be legislated.[5]

While the AICD is supportive of a statutory tort for invasions of privacy, we do not support an outcome where it would be open to claimants to seek compensation for the same actionable conduct under multiple heads of claim – potentially on different evidentiary grounds. Depending on how each cause of action is constructed, there is the potential for actions under a statutory tort and direct right of action to run concurrently (including by way of class action) in addition to any penalties sought by the OAIC to be applied by the court for a breach of the APPs.

[4] AICD submission to the Statutory Review of Reforms to Australia's Continuous Disclosure Laws, available here.
[5] AICD submission to the Review of the Privacy Act – Report, March 2023, available here.

This is of particular concern considering what appears to be a potentially lower barrier for bringing a claim under the direct right of action, based on previous proposals included in discussion papers under the Privacy Act Review. For example, no fault threshold has been proposed for conduct that amounts to an 'interference with privacy'. In our view, should a direct right of action be legislated as part of future reforms it should be limited to 'serious interferences' with privacy and require a high fault threshold of 'recklessness or intent', consistent with the statutory tort proposed.

Moreover, while a gateway model has been proposed - requiring individuals to make a complaint first to the OAIC to assess for conciliation before a claim may proceed to the Federal Court - our interpretation is that a complainant may still seek leave to the Federal Court instead of pursuing conciliation (at a complainant's election), or even in circumstances where the OAIC has determined that there has been *no* breach of the Privacy Act and has terminated the matter.

Our concerns with this are two-fold:

- Firstly, a claimant may seek to bypass the gateway model by electing not to participate in a conciliation process via the OAIC. This risk is even more pronounced in the case of class actions initiated on behalf of claimants which could be very lucrative for plaintiff law firms and litigation funders, even should individual claims be relatively modest. By way of comparison, jurisdictions such as New Zealand and Singapore require the conciliation process to be exhausted before a claim under a direct right of action can proceed to a court; and

- Secondly, without a harm threshold that requires a 'serious' interference with privacy, there is a risk that a direct right of action will be pursued in court even where the OAIC has established that an entity has taken reasonable steps under APP11 to protect personal information.

In the absence of further detail from Government regarding the design of the proposed direct right of action, we strongly urge consideration be given to if/how both the proposed statutory tort and direct right of action would operate in parallel so that there are no unintended consequences. In our view, clarification should be provided that an entity cannot be subject to two separate claims under a statutory tort and direct right of action proceeding for the same actionable conduct.

2. Security, retention and destruction – APP 11

We support the proposal to amend APP 11 under Item 34 of the Bill to state that 'reasonable steps' to secure personal information includes 'technical and organisational measures'.

As noted in the Bill's Explanatory Memorandum, this amendment is intended to promote the importance of implementing technical and organisational measures (such as encrypting data, securing access to systems and premises, and undertaking staff training) to address information security risks. These controls would help minimise the risk of data breaches and harm arising from cyber incidents, which can cause significant detriment to affected individuals.

Consistent with proposal 21.2 of the Privacy Act Review, the AICD considers it critical that the OAIC enhance its guidance on 'reasonable steps' under APP 11 to assist entities in protecting personal information. This guidance should be consistent with existing Australian cyber security regulatory frameworks, including that developed by the Australian Signals Directorate and the Australian Prudential Regulation Authority prudential requirements set out in in CPS 234 *Information Security*.

3. OAIC permanent code-making powers

The AICD does not support the proposed amendments under Item 5 of the Bill for OAIC to be provided with powers to develop APP codes at the direction of the Minister where there is a public interest. We

consider this power is unnecessary and runs the risk of new codes in the future containing significant new policy that should be contained within the Privacy Act itself and subject to the usual parliamentary scrutiny.

Our strong view is that the existing industry-led code development process under the Act is sufficient, and it has not been demonstrated that there are such deficiencies with this process that it requires this new OAIC power. Further, where there are exceptional or urgent circumstances that require the development of a code this can be addressed under the proposed temporary code-making powers to be included in Section 26GB. A temporary code for one year, as is proposed in the Bill, strikes the appropriate balance of allowing the OAIC to respond to a particularly pressing privacy issue within an industry or across the economy while providing time for an industry developed code or amendments to the Privacy Act, if required.

The Explanatory Memorandum notes that the APP code itself will be a legislative instrument. Providing a regulator with delegated legislation capacity of this nature should be approached with considerable caution. The ALRC noted in Report 129 that the making of delegated legislation can limit public scrutiny and accountability. Further, the ALRC cited the Department of Prime Minister and Cabinet Legislation Handbook as what are appropriate matters for primary legislation, this includes:

> *(b) significant questions of policy including significant new policy or fundamental changes to existing policy;*
>
> *(c) rules which have a significant impact on individual rights and liberties; and*
>
> *(d) provisions imposing obligations on citizens or organisations to undertake certain activities (for example, to provide information or submit documentation, noting that the detail of the information or documents required should be included in subordinate legislation) or desist from activities (for example, to prohibit an activity and impose penalties or sanctions for engaging in an activity).*[6]

It is clear from the OAIC's submission to the Privacy Act Review Discussion Paper and the Explanatory Memorandum that it is contemplated that this code-making process would be utilised for new significant policy making that will impose new obligations on potentially all entities.[7] The Explanatory Memorandum notes the following:

> *It is expected that new or emerging technology will raise new privacy risks, and there will be a growing need for APP codes to provide certainty on privacy protections when handling specific types of personal information or handling personal information for specific purposes.*[8]

Our view is that this approach to code-making would undermine the legitimate role of the legislature and would be inconsistent with guidance in the Legislation Handbook, thereby risking regulator over-reach.

We are also concerned that given the broad concept of 'public benefit', that were the OAIC to have the power to make codes, it would eventually result in a significant volume of delegated legislation. This would only add to the complexity and challenges for entities seeking to comply with the obligations, particularly those with limited resources. We note that in financial services laws, for example, the ALRC has found that the proliferation of delegated legislative powers under Chapter 7 of the *Corporations Act* and their exercise in myriad regulatory legislative instruments is a significant source of complexity for users

---

[6] ALRC, Traditional Rights and Freedoms—Encroachments by Commonwealth Laws Final Report, March 2016, page 457 - citing the Department of Prime Minister and Cabinet Canberra, Legislation Handbook (1999).
[7] OAIC submission, Privacy Act Review Discussion Paper, December 2021, page 44.
[8] Explanatory Memorandum, Schedule 1 - Privacy reforms, paragraph 17.

in understanding and meeting the law.[9] We would be very concerned if this dynamic was to be replicated in Australian privacy law.

4. New penalty provisions

The AICD supports the introduction of mid and lower tier penalty provisions that are commensurate with the seriousness of the interference with privacy and the OAIC being able to issue infringement notices for minor breaches of the Privacy Act under item 56 of the Bill.

A well-designed tiered model has the potential to reflect that privacy breaches, particularly those involving cyber-crime and data theft, run along a spectrum of culpability where the entity holding the data may also be a victim of a sophisticated attack and have limited ability to defend or prevent the data breach from occurring.

We also welcome the proposed clarification in the Bill under item 51 on what 'factors' may be taken into account in determining interference with privacy is 'serious' under section 13G of the Privacy Act. However, we strongly encourage further guidance and examples be provided, either in the Bill's Explanatory Memorandum or by the OAIC, on what form of conduct or omission would give rise to a serious, mid and lower tier penalty. This clarity would assist entities to better understand the relevant regulatory expectations and the potential legal consequences of not meeting them.

5. Increased transparency on automated decisions

The AICD does not support the current drafting under Item 88 of the Bill that would amend APP 1 to require changes to entity privacy policies to disclose the use of automated decision-making (**ADM**).

Consistent with our recent submission on AI guardrails, we in-principle support greater transparency on the use of ADM, including where AI tools or systems are utilised. However, we are concerned that as currently drafted the proposed changes to APP 1 will be very costly to implement and maintain and will result in limited transparency benefits. We are also of the view that the proposal is inconsistent with the Government's direction on the regulation of AI that focuses on 'high risk' use.

Complexity of drafting

ADM in businesses can run the spectrum from complex AI systems to more rudimentary or basic software and spreadsheets. Our interpretation of '*for a computer program to make, or do a thing that is substantially and directly related to making, a decision*…' and the detail in the Explanatory Memorandum is that this requirement will capture common business tools used in human decision making.

The Explanatory Memorandum notes an example of where Microsoft Excel is used as a key input in human decision making this would need to be detailed in the privacy policy. For large businesses there is widespread use of common spreadsheet and database software in decision-making and it seems to be highly complex and unworkable to require all of these uses to be included in the privacy policy.

In addition, it is not apparent what transparency benefits this change would result in, or what concerns it is seeking to address, with common business decision-making tools. Our reading of the Privacy Act Review Final Report is that the predominant concern with ADM relates to systems that are solely or wholly making decisions, particularly AI and machine learning systems, not formulas or macros in Microsoft Excel that aid decision-making.[10] It is burdensome and unnecessary for this obligation to cover all computer

[9] ALRC, Summary Report - Confronting Complexity: Reforming Corporations and Financial Services Legislation, November 2023, page 37.
[10] Privacy Act Review Final Report, February 2023, page 188.

programs and systems. Further, as discussed below this approach is inconsistent with the risk-based approach of regulating AI that the Government has proposed.

We recommend that the drafting of this proposal is amended such that it is limited to where the 'computer program' has '*solely*' or '*wholly*' made the decision. That is, there is no human oversight or involvement in the decision. This change would remove the current complexity involving with interpreting 'substantially' and 'directly related to' and would like substantially reduce compliance costs with meeting this requirement.

Our view is that this approach would also be more consistent with the harm that we understand the proposal is seeking to address and be aligned with the AI regulatory proposals.

Alignment with AI proposals

We are also concerned that this ADM proposal does not align with the Government's direction on the Mandatory Guardrails for AI that is risk based, namely separating AI between 'high risk and low risk' uses. The ADM proposal in the Bill is not risk based in that it captures all ADM tools or steps regardless of any risk or complexity.

As discussed above, we recommend a drafting change to this obligation to limit the requirement to where the computer program has 'solely' or 'wholly' made a decision. This change would be more consistent with our understanding of the transparency requirements that are being explored in respect of AI Guardrails and the 'high risk' framework.

Further, we consider the Committee should recommend that further consultation occur with the Department of Industry, Science and Resources on the development of AI Guardrails, particularly guardrails 5, 6 and 7.[11] We are concerned that this proposed change to the Privacy Act would result in contradictory and inconsistent regulatory settings in respect of the transparency of AI systems. For instance, a business may not have to disclose the use of a low-risk AI system under the Guardrails but then separately be required to disclose that use in its privacy policy under this proposal. This outcome will not only create cost and uncertainty for businesses but also be confusion for individuals.

6. Overseas data flows

The AICD supports the proposal to amend APP 8 under Items 36 – 38 of the Bill to facilitate the overseas disclosure of personal information to jurisdictions prescribed by regulations.

Feedback we have received indicates that this change will result in modest benefits for some businesses that transfer personal information overseas through no longer having to undertake a standalone assessment of a jurisdiction and its compatibility with the APPs.

We consider the Ministerial decision-making steps to designate a country as a 'substantially similar' are appropriate.

[11] Guardrail 5: Enable human control or intervention in an AI system to achieve meaningful human oversight. Guardrail 6: Inform end-users regarding AI-enabled decisions, interactions with AI and AI-generated content. Guardrail 7: Establish processes for people impacted by AI systems to challenge use or outcomes.