

# BCA

Business Council of Australia

## Privacy and Other Legislation Amendment Bill 2024: Senate Legal and Constitutional Affairs Legislation Committee

Submission of the Business  
Council of Australia

October 2024



# Contents

1.	Overview .....	2
2.	Key recommendations .....	3
3.	<b>Schedule 1 – Privacy Act amendments .....</b>	<b>5</b>
3.1	Automated decisions and privacy policies .....	5
3.1.1	Expansion into ‘interests’ is too broad.....	5
3.1.2	Definition of automated decision making is too broad .....	5
3.1.3	Defining harm .....	5
3.1.4	Flexibility in transparency .....	6
3.1.5	Personal circumstances .....	6
3.1.6	Sensitive information .....	6
3.1.7	Divergence from AI regulation.....	7
3.1.8	Compliance and guidance.....	7
3.2	Expansion of APP code making power.....	8
3.2.1	Ability to make codes.....	8
3.2.2	New and emerging technology.....	8
3.2.3	Civil penalty provision for breaching the APP.....	9
3.3	Children’s Online Privacy Code.....	9
3.3.1	Types of online services .....	9
3.3.2	UK’s Age Appropriate Design Code .....	9
3.3.3	Definition of ‘child’ .....	10
3.4	Serious interference with privacy .....	10
3.5	Public inquiries by the Information Commissioner .....	10
4.	<b>Schedule 2 – Statutory tort for serious invasions of privacy.....</b>	<b>11</b>
4.1	Overview .....	11
4.2	Unreasonably broad .....	11
4.3	Direct right of action .....	11
4.4	Information that relates to a person .....	11
4.5	Misusing information .....	11
4.6	Recklessness.....	11
4.7	Serious harm.....	12
4.8	Employee records.....	12
4.9	A conciliation process .....	12
4.10	Vicarious liability .....	12
4.11	Innocent dissemination.....	12

# 1. Overview

The Business Council of Australia (BCA) represents over 130 of Australia's leading businesses. Our members include some of Australia's largest banking, telecommunications and technology companies. We champion the role that responsible businesses play in generating sustainable economic growth and advocate for policy settings that are in the national interest.

We welcome this opportunity to provide a submission to the Legal and Constitutional Affairs Legislation Committee on the Privacy and Other Legislation Amendment Bill 2024.

The BCA supports modernising Australia's privacy protection framework. Australians deserve privacy protections, and businesses should be supported to modernise, grow, and compete in an increasingly challenging global environment.

We agree that the *Privacy Act 1988 (the Act)* must be updated. Implementation of privacy reforms must allow industry to move forward with confidence.

The Review of the Act (*the Review*) between 2020 and 2023 initiated this process and identified potential reforms. The government's response to the Review in September 2023 then made clear its intended path forward. A number of recommendations from the Review are in the *Privacy and Other Legislation Amendment Bill 2024 (the Bill)*.

The BCA believes that the creation of a new statutory tort, requirements around automated decision making, and the expansion of the Information Commissioner's code making powers need significant work before they are ready. These proposals should be clarified and aligned with a wider government implementation plan.

Many recommendations from the Review have been delayed to a later date. These are some of the most significant changes and will be hugely impactful. They include a changed definition of personal information, the potential removal of the small business exemption, changes to the definition of consent, changes to the employee records exemption, inclusion of a 'fair and reasonable' requirement, changes to the rights of the individual, and organisational accountability.

The current approach to privacy reform is fragmented. Enacting these recommendations into legislation more holistically would mean Australians are more able to benefit from the privacy protections they have been promised. It means industry would have a clearer picture of all impending legislative requirements. And it means industry would more efficiently and effectively manage all new requirements.

Australians may face increased costs due to the regulatory burden placed on industry in managing ongoing changes to their privacy obligations. Australians may stop receiving the services they have come to expect.

Legislative amendments should be accompanied by a reliable cost-benefit analysis that has been co-designed with industry.

Given the far-reaching implications of what has been proposed, government should embrace industry's eagerness to co-design legislation.

Detail on the BCA's positions relating to specific recommendations of the Privacy Act Review can be found [here](#).

## 2. Key recommendations

1. The addition of 'interests' to rights significantly broadens scope for disclosure of ADMs. 'Or interests' should be removed from 'significantly affect the rights or interests of an individual' to align with the Privacy Act Review Report. If government seeks to keep 'or interests', the legislation needs to provide more clarity on what types of interests are intended to be covered.
2. The definition of automated decision making is too broad. This should be narrowed to align with the EU GDPR.
3. The concept of harm should be included. APP 1.7 should be rewritten to define decisions with a 'significant effect' based on the potential risk of harm or negative impacts they might cause.
4. The Bill should allow flexibility in how an APP entity notifies and helps individuals understand how their PI is used in ADM, for example an organisation should be able to choose to provide the information through their privacy policy, or through point in time notifications or collection notices.
5. There should be guidance around how and when an entity would need to examine an individual's 'circumstances', including a definition of circumstances and how circumstances might be assessed as exhibiting 'vulnerability', and whether assessment considers vulnerability permanency, or applies to temporary vulnerability, such as an injury that is expected to fully heal.
6. The requirement to disclose whether personal information is used should be limited to where it may be used as part of ADM processes, and if so, the general types of ADM processes used by a business.
7. APP 1.8 should be redrafted to ensure that the 'kinds of' personal information and 'kinds of' decisions required to be disclosed are crafted at a sufficiently high-level to ensure that commercially sensitive information remains confidential and to mitigate risks of decision manipulation.
8. APP 1.8 should be made subject to relevant commercial and/or public interest exemptions.
9. A more measured and consistent approach should be taken toward regulating ADM and AI.
10. Government should provide sector-specific regulatory guidance and examples to help entities understand how to assess which decisions are 'significant' decisions that are 'substantially and directly' made by automation.
11. The temporary code power is enough where there is a systemic regulatory failure. Moving toward a top-down approach removes the benefit of informed co-design and provides no clear benefits over OAIC guidance.
12. The Minister should be required to consider if the public interests in having a code are adequately balanced against the legitimate interests of entities carrying out activities that are, in the circumstances, beneficial and which align broadly with the public interest.
13. The Minister should be required to consider whether there are existing regulatory frameworks that already target the risk of harms identified, and whether it is more appropriate for those frameworks to be updated, rather than there be the introduction of a separate APP Code.
14. The Minister should be required to publish their intention to have the Commissioner make a code and their rationale under 26GA (1) as to why this is appropriate. This rationale should then be subject to consultation for at least 28 days.
15. The Minister should be required to appoint APP entities or their representatives to collaborate with the Commissioner in developing the code, unless there is a stated reason why doing so would be strictly inappropriate.
16. The introduction of civil penalty provisions for acts or practices which breach specific APPs, combined with the fact that a 'reasonable period' assessment is not easily established, means that '13K (1b) (ix) Australian Privacy Principle 13.5 (dealing with requests)' should be removed.
17. There should be further consideration of the appropriateness of the phrase 'likely to be accessed by children'. This would help to define the online services to which the Children's Online Privacy Code would apply.
18. Section 26GC (5) (a) should be replaced with the following: '(a) the entity is a provider of a service that is likely to be accessed by children and is not a health service; or'

19. A new section 26GC (4) should be inserted: 'To the extent possible, the Children's Online Privacy Code must align with international approaches, including the UK Age Appropriate Design Code'
20. A new section 26GC (9) should be inserted: '(9) In developing the Children's Online Privacy Code, the Commissioner must have regard to international approaches to children's privacy, including the UK Age Appropriate Design Code'.
21. The definition of 'child' should be aligned with existing pieces of legislation and regulation such as the age of criminal responsibility or minimum working age.
22. Factors that a court may consider when determining an interference with privacy should be expanded to include factors such as whether the entity took steps to minimise damage suffered to the individual and whether actions by a third party contributed to the interference with privacy.
23. A mechanism should be developed whereby APP entities (in particular those who are specified in a direction or approval) can provide comments on sensitive aspects of reports that could impact an APP entity's protection of personal information, ahead of their tabling with parliament or publication.
24. The statutory tort for serious invasions of privacy should be limited to APP entities.
25. Government should consult on all direct rights of action proposed to implement via future tranches of amendments to the Act. Failing to do so risks creating systems that compound obligations.
26. Information in s7(1)(a)(ii) should be limited to 'personal information' as defined in the Act.
27. The definition of 'misusing information' should be limited to use, collection or disclosure that is improper or harmful.
28. The standard of intent should be limited to just 'intentional' (vs reckless). It should also include that the intention is to cause harm, damage or distress.
29. The proposed statutory tort for serious invasions of privacy should incorporate a serious harm threshold, or at least requires plaintiffs to prove damage. This would better align with the considered reforms in defamation.
30. The Bill should clarify that 'employee records' are exempt from the definition of 'information' in Schedule 2, s 7(1)(a)(ii).
31. Plaintiffs should first be required to go through an OAIC conciliation process prior to taking action through the proposed statutory tort for serious invasions of privacy. Precedent for this approach can be found in a range of claims under the Fair Work Act 2009 (Cth) for example in relation to unfair dismissal or dismissal-related general protections claims, and under anti-discrimination laws.
32. Employers should be exempted from vicarious liability for the tortious acts of their employees and agents done in the scope or course of employment if they have taken all reasonable steps to prevent wrongful acts.
33. Digital intermediaries should have access to defences such as innocent dissemination and the digital intermediary defence with respect to the publication of information on their platforms.

## 3. Schedule 1 – Privacy Act amendments

### 3.1 Automated decisions and privacy policies

The BCA is concerned that the proposed legislation relating to ADM in Part 15 of the Bill is too broad and risks capturing a wide range of innocuous use cases.

#### 3.1.1 Expansion into ‘interests’ is too broad

The breadth of the provision related to effects is substantially wider than the ADM proposals set out in the Review. The Review refers to

*‘substantially automated decisions which have a legal or similarly significant effect on an individual’s rights’ per proposal 19.1.*

The proposed drafting refers to decisions that

*‘could reasonably be expected to significantly affect the rights or interests of an individual’ (per cl 88, s 1.7(b)).*

The addition of ‘interests’ to rights significantly broadens scope for disclosure of ADMs. Given that non-compliance penalties are significant, an unintended outcome is that organisations over-disclose information. This creates friction for customers and undermines the goal of ensuring transparency about ADM. It may undermine the policy intent of the reform by increasing information overload in a way that is less, not more, understandable to our customers. Privacy policies will become even longer documents. This may make it harder for individuals to seek out important and relevant information when they look for it.

#### 3.1.2 Definition of automated decision making is too broad

The implementation of this amendment would be an exceptionally difficult, time consuming, and costly undertaking for most businesses. It would require APP entities to review all decision-making processes in their business or organisation that rely on personal information. Once such decisions are identified, organisations will then be required to assess the extent to which those decisions relate to ones that could reasonably be expected to significantly affect the rights or interests of an individual and depend solely or substantially on automated means (that is, via a computer program).

The implementation of all new ADM processes would require updates to the APP entity’s privacy policy on an ongoing basis, fed by exhaustive audits of all ADM systems, mapping complex data flows and decision making logic.

The application to computer programs that

*‘make, or do a thing that is substantially and directly related to making, a decision’*

using personal information is incredibly broad. It can be interpreted to extend from basic use of spreadsheet formulas to complex AI systems. The terms ‘significant’ and ‘substantially’ are also imprecise and do little to narrow this breadth. By contrast, requirements relating to automated decisions in global privacy laws are typically limited to decisions that are ‘solely’ based on automated processing or are made without any meaningful human involvement. To give a practical example, if software is used to analyse data for the purpose of supporting decision making, but a human then uses the outputs of that data to make a decision, this could constitute an ‘automated decision’ under the Australian law but would not elsewhere in the world (including under the European Union (EU) General Data Protection Regulation (GDPR)).

#### 3.1.3 Defining harm

To provide more certainty, the BCA recommends that APP 1.7 should be rewritten to define decisions with a ‘significant effect’ based on the potential risk of harm or negative impacts they might cause. Currently, the definition of decisions covered by the rule does not clearly consider the connection between harm and the provision of essential services (like the risks tied to decisions about credit or employment). Defining significance in terms of the risk of harm also aligns with the definition of ‘high risk’ AI uses that the DISR is looking at in its Proposals Paper for Introducing Mandatory Guardrails for AI. We recommend that regulatory frameworks use a

consistent definition of 'high-risk' or 'significant' uses of computer programs to avoid divergent definitions that are difficult to comply with and to better support Australia's digital economy.

### 3.1.4 Flexibility in transparency

Individuals seeking out information about use of ADM in a privacy policy will encounter irrelevant information which could confuse or cause unnecessary concern. This is because privacy policies apply at an organisational level (and therefore need to encompass the privacy practices of the entire organisation). It is likely that many uses of ADM will only be relevant to certain experiences or individual journeys and the appropriate vehicle to provide transparency is the collection notice for that activity.

Individuals will not necessarily be made aware of information at a time when it is important or relevant to them. This is because organisations would simply rely on information in their privacy policy, and fail to take further steps to educate and inform individuals about the use of ADM.

Instead, the BCA would support the introduction of a transparency obligation that retains flexibility in how notification and transparency can be provided to an individual. Specifically, this could instead be achieved by an amendment to APP 5 to add relevant matters that an APP entity must notify an individual of (or otherwise ensure the individual is aware of). Allowing organisations to choose how they provide information about ADMs (whether through a collection notice or a privacy policy) would enable organisations to utilise the most appropriate transparency measures in line with their communication and privacy risk management frameworks. For example:

- A point in time notification. A pop-up box could be provided to customers to outline that their Personal Information (PI) is about to be used to make a decision that may impact them.
- A collection notice. Where a privacy policy applies to entities with multiple customer-facing brands, the use of collection notices can provide greater detail and transparency to customers who are interacting with a specific brand. This could ensure that individuals are made aware of ADM that is relevant to their interactions.
- A Privacy Centre. A 'Privacy Centre' could be used as a centralised hub for large scale organisations with a large customer base to address a range of the organisations privacy protocols and obligations, including data collection processes, individual privacy rights, and procedures for submitting data access requests. This would address the issues around transparency, accessibility and readability.
- Alternate communication methods. An organisation could use different communication approaches (such as audio, visuals or videos) to improve individuals' understanding of processes such as ADM.

### 3.1.5 Personal circumstances

The Explanatory Memorandum to the Bill states that:

*Whether or not a decision could reasonably be expected to significantly affect the rights or interests of an individual depends on the circumstances. For example, a decision's effect on a child or person experiencing vulnerability may be considered significant compared to its effect on other individuals.<sup>1</sup>*

This would require APP entities to do an assessment of every individual's complete personal circumstances to determine vulnerability (which is not described or defined), and then determine whether a decision using ADM need be covered in their privacy policy. Most organisations could not be expected to know the potential range of individual circumstances affecting every person from whom they collect personal data.

### 3.1.6 Sensitive information

Although ADM can pose privacy risks, transparency can also produce its own risks. Entities may be required to disclose sensitive information which has security or commercial implications. The BCA is concerned this could lead to unintended consequences.

Requirements to disclose information about ADM processes could result in security risks, such as where ADM processes are used to detect fraud. The requirement to broadcast how these processes work would tip off fraudsters and help them avoid detection.

---

<sup>1</sup> s 340 (a)

Specifically, the *'kinds of personal information'* and *'kinds of decisions'* that are required to be detailed in a privacy policy should be sufficiently high-level to mitigate risks of decision manipulation by individuals (for example, credit applicants who seek to actively re-set any risk level that banks would ordinarily attach to them as a result of monitoring activities validly undertaken in accordance with law) which could result in unintended effects for the broader economy and inappropriate outcomes for customers (e.g. as a result of inappropriate loan decisions).

Improving efficiency through automation is also an important driver of productivity growth and value for consumers. Organisations should not be required to disclose intellectual property or commercially sensitive information that may discourage or undermine business innovation. The types of personal information which may be involved in ADM may also reveal an entity's algorithms and technology deployed to perform ADM. This would become more of a concern should government proceed with proposal 19.3 from the Report (the right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made).

The European Union's General Data Protection Regulation (GDPR) includes a clause that a data subject's right to access personal data which has been collected about such subject does not extend to trade secrets or intellectual property which, if disclosed, will adversely affect the rights or freedoms of others. There also exists in the Privacy Act the right to refuse access to personal information which reveals commercially sensitive decision-making processes under APP 12.3(j). We consider it appropriate that similar exemptions exist in an ADM context to protect the commercially sensitive information of businesses, as well as preventing altered output of automated decisions through deliberate customer gaming or manipulation.

### 3.1.7 Divergence from AI regulation

This ADM provision also marks a divergence from the government's broader consideration on how to regulate AI through the *Safe and Responsible AI* processes being undertaken by the Department of Industry, Science and Resources (DISR).

Though not all ADM will be enabled by AI, we note that DISR is also looking to apply holistic requirements to AI development and use through mandatory guardrails. This includes looking explicitly at when developers and deployers of AI systems should be required to inform end users regarding AI-enabled decisions through the proposed Guardrail 6. The proposed DISR approach would therefore be much narrower, looking only at AI systems deemed high-risk due to their use. Rather than rush this approach through now, government must coordinate internally to ensure that a measured, consistent and informed approach is taken toward regulating ADM and AI more broadly.

### 3.1.8 Compliance and guidance

Given that assessing all decision-making processes will be an operationally intensive task, we support the grace period of 24 months for compliance.

---

## Recommendations

---

1. The addition of 'interests' to rights significantly broadens scope for disclosure of ADMs. 'Or interests' should be removed from 'significantly affect the rights or interests of an individual' to align with the Privacy Act Review Report. If government seeks to keep 'or interests', the legislation needs to provide more clarity on what types of interests are intended to be covered.
2. The definition of automated decision making is too broad. This should be narrowed to align with the EU GDPR.
3. The concept of harm should be included. APP 1.7 should be rewritten to define decisions with a 'significant effect' based on the potential risk of harm or negative impacts they might cause.
4. The Bill should allow flexibility in how an APP entity notifies and helps individuals understand how their PI is used in ADM, for example an organisation should be able to choose to provide the information through their privacy policy, or through point in time notifications or collection notices.
5. There should be guidance around how and when an entity would need to examine an individual's 'circumstances', including a definition of circumstances and how circumstances might be assessed as exhibiting 'vulnerability', and whether assessment considers vulnerability permanency, or applies to temporary vulnerability, such as an injury that is expected to fully heal.

6. The requirement to disclose whether personal information is used should be limited to where it may be used as part of ADM processes, and if so, the general types of ADM processes used by a business.
7. APP 1.8 should be redrafted to ensure that the ‘kinds of’ personal information and ‘kinds of’ decisions required to be disclosed are crafted at a sufficiently high-level to ensure that commercially sensitive information remains confidential and to mitigate risks of decision manipulation.
8. APP 1.8 should be made subject to relevant commercial and/or public interest exemptions.
9. A more measured and consistent approach should be taken toward regulating ADM and AI.
10. Government should provide sector-specific regulatory guidance and examples to help entities understand how to assess which decisions are ‘significant’ decisions that are ‘substantially and directly’ made by automation.

## 3.2 Expansion of APP code making power

### 3.2.1 Ability to make codes

The BCA does not support the proposed legislation to expand the Commissioner’s ability to make codes in Part 2 of the Bill. This further increases the scope of the Commissioner’s role through delegated legislation, and risks imposing confusing and misinformed compliance obligations on participants.

The implementation of this amendment would provide the Minister power to direct the Commissioner to make codes that will require those APP entities bound by the code to not act in a way, or engage in a practice, that breaches that code. Before giving a such a direction, the Minister must be satisfied that it is in the public interest for there to be a code, and for the Commissioner to develop the code.

Providing the regulator with a power to unilaterally make codes undercuts the principle of separation between regulator and regulation. It creates additional legislation that goes beyond the principles-based foundations of the underlying act.

The proposal varies from the way APP codes are usually made. Currently, APP entities or their representatives draft a code for endorsement by the Commissioner. Having industry draft the code allows those with expertise to determine how to ensure new regulation achieves the desired outcome in the least burdensome manner. This will result in stronger industry compliance while delivering better outcomes for the public. Industry involvement is even more important if the proposed code is to apply across different industry sectors, as what works effectively in one sector may lead to poor outcomes in another. The Commissioner could then review this approach to ensure satisfaction.

Crucially, the legislation does not specify what the Minister must consider in determining that the Commissioner should make a code. This increases the risk of top-down dictation of how industry should operate, without consideration of the experiences of those directly impacted.

### 3.2.2 New and emerging technology

The Explanatory Memorandum to the Bill states 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.’*

While the BCA supports the need for additional guidance on how existing regulation is to apply to emerging technologies like AI, this should not be achieved through a strict code imposed upon industry by government.

Implementing a binding code on new and emerging technology risks stifling innovation and investment, which could lead to significant benefits for consumers and the Australian economy. Binding codes could result in multiple levels of regulation. Contrary to its policy objective, it may serve to introduce further regulatory complexity and obligations that are inadequately harmonised under one federal regime.

In particular, the BCA cautions against creating another level of regulation in industries where there is already a high compliance burden. For example, the financial services industry has adopted various legally or contractually enforceable codes, such as the Banking Code of Practice, ePayments Code, and General Insurance Code of Practice. These existing codes embrace privacy considerations and privacy issues in the context of the industry or conduct it is seeking to regulate.

### 3.2.3 Civil penalty provision for breaching the APP

Currently, APP 13.5 (dealing with requests) requires organisations to deal with APP 13 requests ‘in a reasonable period after the request is made’. The BCA does not believe a ‘reasonable period’ assessment is easily established. The Bill’s proposed amendments introduce civil penalty provisions for acts or practices which breach specific APPs. The Explanatory Memorandum states

*‘These civil penalties have a lower maximum penalty amount to section 13H and target specific obligations that are administrative in nature and where a contravention can be easily established.’*

---

## Recommendations

---

11. The temporary code power is enough where there is a systemic regulatory failure. Moving toward a top-down approach removes the benefit of informed co-design and provides no clear benefits over OAIC guidance.
12. The Minister should be required to consider if the public interests in having a code are adequately balanced against the legitimate interests of entities carrying out activities that are, in the circumstances, beneficial and which align broadly with the public interest.
13. The Minister should be required to consider whether there are existing regulatory frameworks that already target the risk of harms identified, and whether it is more appropriate for those frameworks to be updated, rather than there be the introduction of a separate APP Code.
14. The Minister should be required to publish their intention to have the Commissioner make a code and their rationale under 26GA (1) as to why this is appropriate. This rationale should then be subject to consultation for at least 28 days.
15. The Minister should be required to appoint APP entities or their representatives to collaborate with the Commissioner in developing the code, unless there is a stated reason why doing so would be strictly inappropriate.
16. The introduction of civil penalty provisions for acts or practices which breach specific APPs, combined with the fact that a ‘reasonable period’ assessment is not easily established, means that ‘13K (1b) (ix) Australian Privacy Principle 13.5 (dealing with requests)’ should be removed.

## 3.3 Children’s Online Privacy Code

### 3.3.1 Types of online services

The proposed Code will automatically apply to providers of certain types of online services, if those services are ‘likely to be accessed by children’, which is a vague standard for business to assess. The BCA recommends further consideration on the appropriateness of ‘likely to be accessed by children’, noting that organisations in the UK have found it difficult to operationalise, which has resulted in additional guidance needing to be issued to clarify the application of this definition.

Many companies with services falling within these categories should also play a key role in protecting young people online. Much clearer guidance is needed to help clarify what falls in and outside of scope. It is also problematic that there is no provision in the Bill requiring the OAIC to consult with industry in creating the code. There appears to be little guidance or boundaries around what the substance of the code could entail.

### 3.3.2 UK’s Age Appropriate Design Code

The scope and substance of the Code should be consistent with the UK’s Age Appropriate Design Code. In both the Privacy Act Review Report and the Government’s Response to it, it was made clear that any Children’s Privacy Code should

*‘[t]o the extent possible ... align with international approaches, including the UK Age Appropriate Design Code.’*

However, this has not been reflected in the legislation.

### 3.3.3 Definition of ‘child’

Finally, the current definition of a child proposed in the Bill (as an individual who has not reached 18 years), is inconsistent with existing pieces of legislation and regulation. We seek the harmonisation of the definition of a ‘child’ to increase legal certainty and reduce ambiguity when interpreting laws related to children. For example, the definition proposed in the Bill is inconsistent with:

- The age of criminal responsibility
- Minimum working age (which varies by State jurisdiction), and
- Proposed definitions for social media platforms (and associated policies).

---

## Recommendations

---

17. There should be further consideration of the appropriateness of the phrase ‘likely to be accessed by children’. This would help to define the online services to which the Children’s Online Privacy Code would apply.
18. Section 26GC (5) (a) should be replaced with the following: ‘(a) the entity is a provider of a service that is likely to be accessed by children and is not a health service; or’
19. A new section 26GC (4) should be inserted: ‘To the extent possible, the Children’s Online Privacy Code must align with international approaches, including the UK Age Appropriate Design Code’
20. A new section 26GC (9) should be inserted: ‘(9) In developing the Children’s Online Privacy Code, the Commissioner must have regard to international approaches to children’s privacy, including the UK Age Appropriate Design Code’.
21. The definition of ‘child’ should be aligned with existing pieces of legislation and regulation such as the age of criminal responsibility or minimum working age.

## 3.4 Serious interference with privacy

The factors that a court may consider when determining an interference with privacy are skewed toward a conclusion that an interference is serious because they fail to include potentially relevant mitigating factors.

---

## Recommendation

---

22. Factors that a court may consider when determining an interference with privacy should be expanded to include factors such as whether the entity took steps to minimise damage suffered to the individual and whether actions by a third party contributed to the interference with privacy.

## 3.5 Public inquiries by the Information Commissioner

The Bill introduces broad new public inquiry powers for the Information Commissioner. In relation to instances where an APP entity is specified in a direction or approval, the Commissioner must give its written report on the inquiry to the APP entity mentioned in the direction or approval at the same time that it gives the report to the Minister. The Commissioner must also make the report publicly available, unless the Minister directs otherwise.

However, there are no express requirements on the OAIC to consult with affected APP entities who may be mentioned in a report prior to making the report public. This poses two potential issues:

- where an APP entity is not specified in the direction or approval, but it is still largely reported on, it will not be provided the report ahead of its tabling with parliament and subsequent publication, and
- regardless of whether an APP entity is provided with the report ahead of tabling with parliament or publication, APP entities discussed in the report do not have any mechanism through which to discuss or otherwise request that certain information is not published or redacted (including in respect of confidentiality concerns).

23. A mechanism should be developed whereby APP entities (in particular those who are specified in a direction or approval) can provide comments on sensitive aspects of reports that could impact an APP entity's protection of personal information, ahead of their tabling with parliament or publication.

## 4. Schedule 2 – Statutory tort for serious invasions of privacy

### 4.1 Overview

The implementation of this amendment would introduce a new statutory tort for serious invasions of privacy. Under the new proposed statutory tort, people affected by serious invasions of privacy – involving ‘intrusion of seclusion’ or ‘misuse of information’ – will have avenues for redress. Elements to be considered will include seriousness, a reasonable expectation of privacy, and recklessness or intention. A range of defences and exemptions are available.

The BCA recognises the policy objective in including the new statutory tort for a serious invasion of privacy but remains concerned with the drafting. The approach included in the Bill is applied too broadly and will result in a high degree of volatility in interpretation through case law. This will result in negative experiences for plaintiffs due to prohibitive costs and long court delays. It will also impose significant costs on companies that are required to defend legal proceedings, as well as on our already heavily burdened courts that will be required to adjudicate. We are also concerned that this may open new avenues for class action lawsuits, leading to a surge in claims while simultaneously creating a new and complex system to navigate.

### 4.2 Unreasonably broad

As drafted, the tort would apply to information much broader in scope than the personal information usually regulated in the purview of the Privacy Act. It would also bring in a broader range of organisations (such as small businesses).

### 4.3 Direct right of action

We are concerned by the government's decision to include this amendment without open consultation on the proposed drafting. We are also concerned that the government has not provided an implementation plan to outline whether it intends to separately pursue additional amendments to provide an additional direct right of action, and, if so, how these amendments would work together. Ensuring clarity in the options available, and that these are well scoped and targeted, is fundamental to promoting compliance.

### 4.4 Information that relates to a person

The scope of information captured by the tort is too broad when compared to the scope of information covered by the Privacy Act. The tort applies to the misuse of ‘information that relates to’ a person, whereas the Privacy Act applies to ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable’. There is no clear rationale for this distinction, which is likely to create unnecessary complexity. The BCA recommends that the tort should only apply to the misuse of ‘personal information’ as defined in the Privacy Act.

### 4.5 Misusing information

The definition of misuse of information is broad. Currently, the proposed reforms would define ‘misusing information’ as ‘collecting, using or disclosing information about the individual.’ By this standard, any interaction with data would de facto become misuse of information. BCA recommends that the definition of ‘misusing information’ should instead be limited to use, collection or disclosure that is improper or harmful.

### 4.6 Recklessness

The BCA has concerns about the use of ‘recklessness’ and suggests it be removed. Although it does have a specific meaning, it is subjective and involves a value judgement about what is a reasonable or unreasonable risk.

It increases the exposure to business, particularly where the tort is actionable without proof of loss. The ALRC Report suggests either referencing the criminal code standard of recklessness or

*‘Alternatively, the provision could state that a person is reckless if they are aware of a substantial risk that an invasion of privacy will occur, and acts regardless of, or with indifference to, that risk.’ (7.9)*

## 4.7 Serious harm

A serious harm threshold is not included. The Stage 1 and 2 Model Defamation Provision reforms provide for a serious harm threshold for actionable defamation, and a statutory exemption from liability for search engines.<sup>2</sup> The proposed statutory tort for serious invasions of privacy should incorporate a serious harm threshold, or at least requires plaintiffs to prove damage.

## 4.8 Employee records

To ensure organisations can continue dealing with employee records as required to manage the employment relationship and their compliance obligations in respect of employees, the Bill should clarify that ‘employee records’ are exempt from the definition of ‘information’ in Schedule 2, s 7(1)(a)(ii). Urgent clarity must also be provided regarding the government’s intentions with respect to further amendment of the employee records exemption with the Act to understand the full impact and effect of the statutory tort on regulated entities.

## 4.9 A conciliation process

Additional steps must be put in place to provide a more effective system for redress and to limit the number of unmeritorious claims being made in courts. We recommend that the parties first be required to go through an Oaic conciliation process to try and address their concerns voluntarily before a claim can be made in court.

A voluntary and low-cost alternative dispute resolution here is best. In many instances, a well-resourced regulator would also provide a more effective way to achieve a complaint resolution than a court process. It may be that the Commissioner can agree for the matter to bypass that process in certain scenarios.

## 4.10 Vicarious liability

The BCA is concerned about the potential unfairness occasioned on employers held to be vicariously liable for the wrongful actions of their employees where they have taken appropriate steps to prevent their employees from invading individuals’ privacy.

At common law, an employer will be vicariously liable for the wrongful acts of their employees where the tortious act of the employee is committed in the course or scope of the employment.<sup>3</sup>

To address this, we recommend the common law approach to vicarious liability for employers be limited, such that where an employee or agent of a person does an act or acts that would breach s (7)(1), the employer is not liable for the wrongful acts of the employee or agent, if it is established that they took all reasonable steps to prevent the employee or agent from doing acts of the kind.<sup>4</sup>

## 4.11 Innocent dissemination

Digital intermediaries should have access to defences such as innocent dissemination and the digital intermediary defence with respect to the publication of information on its platform. This is to clarify that a digital intermediary should not be liable for the publication of information on its platform by a third party unless the digital intermediary has been notified of the information and has failed to remove it within a reasonable period of time.

A safe harbour defence for innocent dissemination has been introduced through Stage 1 and 2 Model Defamation Provision reforms.

<sup>2</sup> NSW Government, Communities and Justice, ‘Review of Model Defamation Provisions’, <https://dcj.nsw.gov.au/about-us/engage-with-us/public-consultations/statutory-reviews/review-model-defamation-provisions.html#:~:text=DWP%20to%20consider,-Background%20to%20the%20Model%20Defamation%20Provisions%20Reforms,approach%20to%20reform%20is%20essential>.

<sup>3</sup> *CCIG Investments Pty Ltd v Schokman* [2023] HCA 21; 97 ALJR 551

<sup>4</sup> Compare to s 106 of the *Sex Discrimination Act 1984* (Cth).

---

## Recommendations

---

24. The statutory tort for serious invasions of privacy should be limited to APP entities.
25. Government should consult on all direct rights of action proposed to implement via future tranches of amendments to the Act. Failing to do so risks creating systems that compound obligations.
26. Information in s7(1)(a)(ii) should be limited to 'personal information' as defined in the Act.
27. The definition of 'misusing information' should be limited to use, collection or disclosure that is improper or harmful.
28. The standard of intent should be limited to just 'intentional' (vs reckless). It should also include that the intention is to cause harm, damage or distress.
29. The proposed statutory tort for serious invasions of privacy should incorporate a serious harm threshold, or at least requires plaintiffs to prove damage. This would better align with the considered reforms in defamation.
30. The Bill should clarify that 'employee records' are exempt from the definition of 'information' in Schedule 2, s 7(1)(a)(ii).
31. Plaintiffs should first be required to go through an OAI conciliation process prior to taking action through the proposed statutory tort for serious invasions of privacy. Precedent for this approach can be found in a range of claims under the *Fair Work Act 2009* (Cth) for example in relation to unfair dismissal or dismissal-related general protections claims, and under anti-discrimination laws.
32. Employers should be exempted from vicarious liability for the tortious acts of their employees and agents done in the scope or course of employment if they have taken all reasonable steps to prevent wrongful acts.
33. Digital intermediaries should have access to defences such as innocent dissemination and the digital intermediary defence with respect to the publication of information on their platforms.

BUSINESS COUNCIL OF AUSTRALIA

GPO Box 1472, Melbourne 3001 T 03 8664 2664 F 03 8664 2666 [www.bca.com.au](http://www.bca.com.au)

© Copyright October 2024 Business Council of Australia ABN 75 008 483 216

All rights reserved. No part of this publication may be reproduced or used in any way without acknowledgement to the Business Council of Australia.

The Business Council of Australia has taken reasonable care in publishing the information contained in this publication but does not guarantee that the information is complete, accurate or current. In particular, the BCA is not responsible for the accuracy of information that has been provided by other parties. The information in this publication is not intended to be used as the basis for making any investment decision and must not be relied upon as investment advice. To the maximum extent permitted by law, the BCA disclaims all liability (including liability in negligence) to any person arising out of use or reliance on the information contained in this publication including for loss or damage which you or anyone else might suffer as a result of that use or reliance.

BCA

Business Council of Australia