SUBMISSION

Senate Legal and Constitutional Affairs Committee – Inquiry on the Privacy and Other Legislation Amendment Bill 2024

11 October 2024

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2024/39

Senator Nita Green

Chair of the Senate Legal and Constitutional Affairs Committee

Parliament House

Canberra ACT 2600

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

11 October 2024

Dear Senator Green,

Senate Legal and Constitutional Affairs Committee – Inquiry on the Privacy and Other Legislation Amendment Bill 2024 (the Bill)

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to the Committee's consultation.

About ASFA

ASFA is a non-profit, non-partisan national organisation whose mission is to continuously improve the superannuation system, so all Australians can enjoy a comfortable and dignified retirement. We focus on the issues that affect the entire Australian superannuation system and its $3.9 trillion in retirement savings. Our membership is across all parts of the industry, including corporate, public sector, industry and retail superannuation funds, and associated service providers, representing over 90 per cent of the 17 million Australians with superannuation.

ASFA's Opening Comments

ASFA supports the Bill, noting that it amends the *Privacy Act 1988* (Cth)(the Privacy Act) in a manner consistent with a thorough process, flowing from the final Report of the Privacy Act Review, released on 16 February 2023. This extremely detailed report was 320-pages long and contained 116 separate proposals for reforms to Australia's privacy laws. [1]

ASFA strongly supports strengthening of Australia's privacy laws. We agree with the Attorney-General, the Hon. Mark Dreyfus KC MP – who said in his Second Reading Speech introducing this Bill:[2]

> *Strong privacy laws and protections are critical to building public trust and confidence in the digital economy, and driving the investments needed to keep people's data safe. The right to privacy is a fundamental human right.*

[1] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022).
[2] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 September 2024, 21 (The Hon. Mark Dreyfus KC MP)(Privacy and Other Legislation Amendment Bill 2024 – Second Reading Spech)

ASFA has consistently supported these reforms. We made a submission to the consultation on report on 31 March 2024.[3] There, while supporting the strengthening of Australia's privacy laws, we made the following comments:

1. We noted privacy principles can often have tensions with measures to measures to detect and prevent fraud and therefore Registrable Superannuation Entities (RSEs): 'must adopt a risk-based approach to manage and balance these competing concerns.'[4]

2. There is a need to balance 'the right to erasure' and the need for 'consents to be current' against with other record-keeping obligations imposed on RSEs by, inter alia, the *Corporations Act 2001* (Cth)(the Corporations Act), the *Superannnuation Industry Supervision Act 1993* (Cth)(the SIS Act) and the *Income Tax Assessment Act 1997* (Cth)(the ITAA).[5]

3. There are practical difficulties for RSEs verifying employee information provided to them by employers on behalf of their employees, given the volume of employers registering new employees and the lack of a pre-existing relationship with many employers.[6]

4. In our last submission, ASFA members sought clear timeframes in relation to the commencement of the proposals in the Privacy Act Review. [7] Greater clarity would be helpful in terms of when the proposals not dealt with by this legislation are intended to be implemented, noting ASFA estimates this legislation implements approximately 33 of the 116 proposals from the Review.[8] This means there are still 83 proposals outstanding from the Review.[9]

Consistent with ASFA's earlier submission on this issue, while strongly supporting the reform of Australia's privacy laws, this submission will observe where competing rights or legal obligations and administrative necessity may require that the implementation of the underlying objectives of the Privacy Act Review accounts for these additional considerations.[10]

In addition to our previous submission, ASFA would also like to draw the Committee's attention to two further initiatives which our members have proactively committed to, as a sign of our desire to work collaboratively with the Government to strengthen protections for personal information and combat financial crime. These are:

1. ASFA's Better Practice Guidance on Minimum Fraud Controls for Superannuation Funds (here), and
2. ASFA's Financial Crime Protection Initiative (FPCI), which seeks to help industry and consumers work together to fight financial crime through:
    - Enhancing collaboration and knowledge sharing between funds and critical service providers including custodians, administrators and tech providers
    - Developing industry-wide frameworks to combat financial and cybercrime
    - Connecting the superannuation sector, relevant government agencies and related financial services bodies
    - Helping make Australians aware of the actions they can take to protect their super and data from scammers.

[3] ASFA, Submission to AGD, Government's Response to the Privacy Act Review's Final Report (31 March 2024).
[4] Ibid, 2.
[5] ASFA, Submission to AGD, Government's Response to the Privacy Act Review's Final Report (31 March 2024), 2-3.
[6] Ibid, 3.
[7] Ibid, 3.
[8] See the Table in Attachment B of this submission.
[9] The Hon. Mark Dreyfus, KC MP (Attorney-General of Australia), *'Landmark Privacy Act Review Report Released*' (16 February 2023).
[10] ASFA, Submission to AGD, Government's Response to the Privacy Act Review's Final Report (31 March 2024).

ASFA also made a submission to Treasury on their recent consultation in relation to the Scams Prevention Framework draft legislation, which illustrates our commitment to robust consumer protections in these areas. There, we said:[11]

> *ASFA wishes to emphasise that our $3.9 trillion sector wants to assist the Government in dealing with scams. Our membership has been on the front foot in proactively seeking combat scams and issues related to other heinous forms of financial crime.*

We also note that strong privacy laws will be critical to combat the risks, which the Australian Competition and Consumer Commission (ACCC) estimates to have cost Australians $2.74 billion in 2023 alone.[12] We are strongly committed to fighting scams and welcome the Government's increased focus in the area, especially through the creation of the National Anti-Scam Centre and the allocation of an addition $67.5 million to fighting scams in the 2024-25 Budget.[13]

Our support for reforms to strengthen Australia's privacy laws, and our broader initiative to combat financial crime, indicate our deep desire to assist Government in improving the regulatory settings related to personal and sensitive information and data protection.

Given the volume of reforms in this package, ASFA's submission will focus only on the following changes:

1. the objects of the Act (Part 1)
2. the power to enable emergency declarations to authorise more targeted handling of personal information to assist individuals in emergency and disaster situations (Part 3)
3. the reforms in relation to children's privacy (Part 4)
4. clarifying that 'reasonable steps', in relation to Australian Privacy Principle 11 (APP 11), include technical and operational matters (Part 5)
5. regarding the sharing of personal information overseas (Part 6)
6. facilitating information sharing after an Eligible Data Breach (EDB) (Part 7)
7. the new civil penalty provision for 'serious invasions of privacy' (Parts 8 and 9)
8. the stricter requirements on automated decision-making and computer programs that interact with personal information (Part 15)
9. The creation of a new statutory cause of action, regarding serious invasions of privacy (Schedule 2).

Attachment A of this submission will first outline what is proposed by each of these reforms. It will then make ASFA's recommendations regarding each proposal.

Attachment B provides a useful summary of the underlying legislative objective of each aspect of the bill, and connects the legislative provisions to the relevant aspect of the following documents, which are key points of reference for this submission:

1. The legislation itself (here)
2. The Explanatory Memorandum (here)
3. The Privacy Act Review's Final Report (here), and
4. The Government's final response to the Privacy Act Review (here).

---

[11] ASFA, Submission to Treasury on the Scams Prevention Framework – Exposure Draft Legislation (4 October 2024).
[12] ACCC, 'Scam losses decline, but more work to do as Australians lose $2.7 billion' (28 April 2024).
[13] The Hon. Stephen Jones MP (Assistant Treasurer and Minister for Financial Services)(21 May 2024), Albanese Government continues crackdown on scammers.

We would welcome the opportunity to elaborate on our recommendations with you further.

Please feel free to reach out to ASFA Senior Policy Advisor, Sebastian Reinehr, at sreinehr@superannuation.asn.au or 0474 704 992, should you have any questions or wish to discuss these matters in detail.

Yours sincerely

James Koval

Head of Policy and Advocacy

Table of Contents

Attachment A – ASFA's Detailed Views on Specific Proposals

1. Amending the objects of the Act

Part 1 of the Bill amends the Privacy Act to add to indicate that the objects of the Act include:

> *(a) to promote the protection of the privacy of individuals with respect to their personal information; and*
> *(aa) to recognise the public interest in protecting privacy*

The Explanatory Memorandum states:[14]

> *These amendments would ensure that the Privacy Act is underpinned by a comprehensive understanding of the broad public benefits of strong privacy protections, which would guide the judiciary's interpretation of the Act.*

This implements Proposals 3.1 to 3.5 from the Privacy Act Review.[15]

1.1 ASFA's recommendation

ASFA supports this proposal. However, ASFA also notes that the right to privacy needs to be balanced against other legal rights and obligations. For example, there are instances where the right to privacy may come into conflict with other legitimate legal obligations imposed upon superannuation functions by other legislation, such as the AML/CTF Act or the SIS Act.[16]

Furthermore, ASFA notes that the insertion of these additional two new 'objects of the Act' does not detract from the 5 other 'objects' which will continue to exist in the Act. For example, section 2A(b) recognizes that another object of the Act is:

> *[T]o recognise that the protection of the privacy of individuals is **balanced with** the interests of entities in carrying out their functions or activities*

Therefore, ASFA recommends that it be made clear in the explanatory materials that the insertion of these objectives does not privilege them over the other objects of the Act, which balance other legitimate considerations.

2. The power to enable Ministerial emergency declarations to authorise more targeted handling of personal information to assist individuals in emergency and disaster situations

Part 3 of the Bill enables the Minister to make 'emergency declarations' in relation to certain situations, in accordance with clause 80KA.

The explanatory memorandum notes that the intention of this reform is:[17]

> *[To] promote the right to the enjoyment of the highest attainable standard of physical and mental health by seeking to prevent and mitigate harm caused by emergencies and disasters by facilitating information sharing when an emergency declaration is in place. These provisions allow both agencies and organisations to disclose personal information to state and territory authorities.*

---

[14] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 10[17].
[15] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 19-21.
[16] ASFA, Submission to AGD, Government's Response to the Privacy Act Review's Final Report (31 March 2024), 2-3.
[17] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 26[122].

This implements Proposals 5.1 to 5.3 of the Privacy Act Review.[18]

2.1 ASFA recommendation

ASFA recommends:

- Further clarification regarding if emergency declarations will extend to the handling of personal information by financial institutions, like super funds.
- For example, clause 80KA(4)(b) refers to:

> *[A]ssisting individuals involved in or affected by the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance.*

- ASFA seeks more information on what could be required of superannuation funds under an emergency declaration in such circumstances.

3. The reforms in relation to children's privacy.

Part 4 of the Bill makes certain recommendations in relation to the reform of laws regarding children's privacy. ASFA only wishes to comment on the aspects of the legislation related to the development of the Children's Online Privacy Code (the Code), as outlined in clause 26GC.

The Explanatory Memorandum states that this Code would be required to be developed and registered within two and a half years of the relevant provisions in the Bill.[19]

The Explanatory Memorandum further states that the purpose of this provision is as follows:[20]

> *[To] promotes the right to privacy for children by requiring the Information Commissioner to develop and register a COP Code. The COP Code would be an enforceable APP code that sets out how one or more of the APPs are to be applied or complied with in relation to the privacy of children.*
>
> *To date, details about how privacy protections under the Privacy Act should apply to children have been set out in guidance material from the Information Commissioner. Elevating protections into an enforceable APP code promotes the right to privacy of a child by imposing specific enforceable obligations with respect to privacy in the handling of children's personal information than would otherwise exist under prevailing law.*

3.1 ASFA's recommendations

ASFA recommends the following:

- Further detailed guidance on the content to which the Code will apply. For example, will it only apply to social media platforms and internet service providers. Or will it also apply to any entity that provides services to children over the internet. For example, a superannuation fund which may interact with 17-year-old employees who may be fund members? Greater guidance is needed here.
- There should be a separate public consultation to which industry can provide feedback on a draft version of the Code.
- The Code should be subject to the same parliamentary scrutiny and oversight mechanisms as ordinary apply pursuant to the *Legislation Act 2003* (Cth).

---

[18] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 50-1.

[19] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 10[4].

[20] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 25[116]-[117].

4. Clarifying that 'reasonable steps', in relation to Australian Privacy Principle 11 (APP 11), include technical and operational matters.

Part 5 of the Bill amends the Act to clarify that 'reasonable steps' under APP 11 'include technical and operational matters'.

The Explanatory Memorandum states:[21]

> *[This] would promote the right to privacy by clarifying the expected scope of measures that entities should consider when determining how they should protect the personal information. The reform would 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.*

This implements Proposal 21.1 from the Privacy Act Review.[22]

2.2 ASFA's recommendation

ASFA recommends that further detailed guidance should be provided by the Office of the Australian Information Commissioner (OAIC), on what meets the proposed 'reasonable steps' threshold in this provision. Guidance should be provided to aid firms in assessing what is required in relation to each of the elements mentioned above in the Explanatory Materials, including what would meet 'reasonable steps' regarding:

- the encryption of data
- securing access to systems and premises
- undertaking staff training
- other areas covered by APP 11.

ASFA further recommends that industry should be consulted on any proposed draft guidance from OAIC prior to it being finalised.

3. Reforms to the sharing of personal information overseas

Part 6 of the Bill changes the requirements of the Privacy Act in relation to the sharing of personal information overseas. This reform is designed to ensure that the relevant personal information which is shared with third parties overseas is subject to 'substantially similar' protection to that which is provided by the Australian Privacy Principles (APPs).[23]

Under the scheme, APP 8.1 provides that, before disclosing information to an overseas entity, entities subject to the APPs must take 'reasonable steps' to ensure that the overseas entity does not breach the APPs in relation to information.[24]

According to the Explanatory Memorandum, section 16C also provides that an APP entity which discloses personal information to an overseas recipient is:[25]

> *[A]ccountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.*

---

[21] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 11[23].
[22] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 222.
[23] See clause 101(1A)(a).
[24] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 44[104].
[25] Ibid.

There are exceptions to these requirements where an APP entity 'reasonably believes' the overseas recipient protects information in a way 'substantially similar' to the APPs.[26]

The Explanatory Memorandum indicates that the purpose of these exceptions to APP 8.2 is:

> *[T]o reduce the burden on APP entities in assessing whether an overseas recipient is subject to a substantially similar framework [to the APPs] and help establish Australia as a trusted trading partner and support Australian businesses to compete more effectively in international markets.*

This implements Proposal 23.1 to 23.6 from the Privacy Act Review.[27]

3.1 ASFA's recommendation

ASFA supports this proposal, insofar as it reflects the globally interconnected nature of how regulate entities do business in the modern digital economy. However, we seek further guidance from OAIC in relation to:

- What would constitute the taking of 'reasonable steps' under APP 8.1, to ensure APPs are not being breached.
- What constitutes 'substantially similar' protection to the APPs, including a list of countries and types of protection which, whilst not the 'same' as APPs, could be considered 'substantially similar' to the APP protections.
- What constitutes a 'reasonable belief' in relation to the exceptions, for cases where an APP entity 'reasonably believed' they had met the test.

ASFA further recommends that there should be a separate consultation prior to the finalization of any OAIC guidance on the topics listed above.

4. Facilitating information sharing after an Eligible Data Breach (EDB)

Part 7 of the Bill seeks to facilitate the sharing of information after an EDB.

EDBs are to be 'declared' by the Minister, in accordance with the requirements in clause 26X(1) of the Bill.

The amendments in the Bill clarify that in relation to EDBs:[28]

- regulated entities must provide a Notification Statement to the Information Commissioner if they are: 'aware that there are reasonable grounds to believe there has been an eligible data breach'.[29]
- the definition of what constitutes an EDB is in section 26WE of the existing Act, specifically it requires:
  - there is unauthorised access to or disclosure of personal information
  - or information is lost in circumstances where unauthorised access or disclosure is 'likely to occur'
  - this is likely to result in 'serious harm' to 'any of the individuals to whom the information relates'

In these circumstances, the Minister may make a declaration allowing the sharing of certain information to 'prevent or reduce a risk of harm arising from misuse of personal information'.[30]

[26] Ibid [105]-[106]
[27] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 237-43.
[28] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 46[121].
[29] Ibid.
[30] Ibid.

Clause 26X(5) of the Bill indicates that a non-exhaustive list of the kind of situations to which these information sharing provisions extend includes:[31]

(a) preventing a cyber security incident (within the meaning of the *Security of Critical Infrastructure Act 2018)*, fraud scam activity or identity theft
(b) responding to a cyber security incident, fraud, scam activity or identity theft
(c) responding to the consequences of a cyber security incident, fraud, scam activity, identity crime and misuse, financial loss, emotional and psychological harm, family violence and physical harm or intimidation
(d) addressing malicious cyber activity.

This implements Proposals 28.1 to 28.4 of the Privacy Act Review.[32]

4.2 ASFA's recommendations

ASFA supports this proposal to facilitate information sharing in response to financial crime and other malicious activity. It is consistent with our prior and ongoing advocacy to combat financial crime, as discussed in our opening comments.

ASFA further recommends the Committee should consider specifying other categories of activity for which declarations can be made, to further facilitate combating illegal activity. For example, a reasonable suspicion of breaches of the Commonwealth Criminal Code, the Criminal Code of a State, breach of the AML/CTF Act, should potentially be added to the list of categories for which the Minister may make a declaration to facilitate information sharing.

ASFA also recommends there need to be appropriate safeguards in place in relation to the sharing of information under this scheme. Therefore, we propose stricter protection than what is currently included in the bill, to allow for greater oversight. We specifically recommend:

- amending clause 26XA so the timeframes on Ministerial declarations under Part 6 should be more tightly defined, so that they either end at a specified date or have to be renewed every 6 months.
- removing clause 26X(10), so that declarations are subject to the normal oversight and disallowance provisions under the *Legislation Act 2003* (Cth).

ASFA requests further clarification around the new penalties for non-compliant data breach notification statements and failing to notify individuals 'as soon as practicable' of a data breach. Specifically, we seek detailed guidance and examples outlining how the term 'as soon as practicable' would apply to real world situations.[33]

5. The creation of a new civil penalty provision for 'serious invasions of privacy'

Part 8 and 9 specify stronger penalties and new orders that would be able to be made by the Federal Court in relation to offences under the Privacy Act. These include the following:[34]

- Clause 13G creates a new civil offence, for 'serious interference with the privacy of an individual'.[35] The maximum penalty for breach of this provision is $626,000.[36]
- Clause 13J allows the Federal Court to make 'alternative orders' if it is 'not satisfied that the interference with privacy is serious'.

[31] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 47-8[129].
[32] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 291-8.
[33] See the existing section 26WL of the Privacy Act and its interaction with the new proposed 13K(2). Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 44[104].
[34] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 52-7[162]-[190].
[35] See sections 13G and 13H.
[36] The equivalent of 2,000 penalty units at $313 as at 8 October 2024.

- Clause 13K allows the Federal Court to issue infringement notices for the breach of certain APPs, to a maximum of $62,600. While only listing certain APPs for which infringement notices may be issued, it allows for others to be 'prescribed by regulation'.[37]

Part 9 further broadens the Federal Court's discretion in these matters by noting under clause 80UA 'Powers of the court to make other orders', that in addition to the above, the Court may:[38]

- 'direct an entity to perform any reasonable act' or 'redress the loss or damage suffered or **likely to be suffered**' as a result of any contravention, and otherwise make any order it sees fit.

This implements Proposal 25.6 of the Privacy Act Review.[39]

5.1 ASFA's recommendations

ASFA supports-in-principle the creation of a civil provision for serious invasions of privacy. However, we make the following recommendations:

- The Explanatory Memorandum should provide detailed examples of what constitutes a 'serious' invasion of privacy, to clarify the distinction between serious misconduct and trivial misconduct.
- The Explanatory Memorandum should make clear that the definition of seriousness is in relation to a 'reasonable person' test. So that the threshold is an objective one and not a subjective one.
- In relation to clause 13K – subclause 13K(1)(x) should be removed, so only the APPs clearly listed in the legislation are operative. This provides greater clarity to regulated entities about their obligations, facilitating compliance.
- We seek clarification regarding how the proposed civil penalty provision in clause 13K(1)for breaching APP2.1 (failure to provide individuals the option to not identify themselves with dealing with an entity) would apply to super funds.
- ASFA requests further clarification around the new penalties for non-compliant data breach notification statements and failing to notify individuals 'as soon as practicable' of a data breach under 13K(2). Specifically, we seek detailed guidance and examples outlining how the term 'as soon as practicable' would apply to real world situations.[40]
- In relation to clause 80UA – all references to loss or damage 'likely to be suffered' should be removed. Orders should only be available for actual damage. Not hypothetical damage which has not crystallised.

6. The stricter requirements on automated decision-making and computer programs that interact with personal information

Part 15 of the Bill imposes stricter requirements on automated decision-making and computer programs that interact with personal information.

Specifically, the Bill includes the following provisions:

- Clause 13K(1)(b)(ii) – makes entities liable to the civil penalty provisions above if they fail to follow new requirements in APP 1.7 to contain information in their privacy policy about how they use personal information in automated decisions.[41]
- Under the new APP 1.7, privacy policies must contain the information outlined in APP 1.8, if the entity:[42]
  - has arranged for a computer program to make, or do a thing that is **substantially and directly** related to making a decision

[37] Clause 13K(1)(x).
[38] Clause 80UA(2)(a).
[39] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 265.
[40] See the existing section 26WL of the Privacy Act and its interaction with the new proposed 13K(2). Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 44[104].
[41] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77[332].
[42] Ibid 77[334]

- the decision could **reasonably be expected** to **significantly affect** the **rights or interests** of an individual
- personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is **substantially and directly** related to making the decision.

This implements Proposals 19.1 to 19.2 of the Privacy Act Review.[43]

6.1 ASFA's recommendations

ASFA makes the following comments and recommendations about this proposal.

First, there should be carveouts from requirement for disclosure of the use of automated decision-making processes, insofar as these could contain information which is – confidential, commercially sensitive, related to intellectual property rights, covered by contracts between the regulated entity and third parties or other subject to legal restrictions that need to be balanced against the desire to implement this proposal.

Secondly, given this proposal extends the civil penalty provision in clause 13K, to make civil penalties apply to breaches of the requirements in relation to automated decision making, the same recommendations which ASFA made above in relation to clause 13K apply equally to this proposal, that is:

- The Explanatory Memorandum should provide detailed examples of what constitutes a 'serious' invasion of privacy, specifically in the case of automated decision making, to clarify the distinction between serious misconduct and trivial misconduct.
- The Explanatory Memorandum should also make clear that the definition of seriousness is in relation to a 'reasonable person' test. So that the threshold is an objective one and not a subjective one.
- Similarly, per comments made above on clause 80UA – all references to loss or damage 'likely to be suffered' should be removed. Orders should only be available for actual damage. Not hypothetical damage which has not crystallised.

Thirdly, ASFA recommends that greater clarity of definition is required regarding the following terms in APP 1.7 as drafter in this Bill:

- A 'thing' that is 'substantially and directly related' to 'making a decision'.
- A decision that could be 'reasonably expected' to 'significantly affect' the 'rights or interests' of an individual.

The terms 'substantially and directly related', 'reasonably expected', 'significant affect' and 'rights or interests' are currently quite broad and vague. They would benefit from further clarity of definition. Through:

- Clearer and more explicit definition in the legislation.
- Deeper discussion in the Explanatory Memorandum, including the provision of detailed examples of different scenarios, especially in relation to artificial intelligence.
- Further guidance to be provided by OAIC once the scheme is effective.

7. The creation of a new statutory cause of action, regarding serious invasions of privacy

Clause 7 of Schedule 2 establishes a cause of action for the new statutory tort of serious invasions of privacy. The elements of this provision are as follows:

- the defendant 'intruded upon the plantiff's seclusion' OR 'misused information' about them AND
- the plaintiff would have had the 'reasonable expectation of privacy in all the circumstances'[44] AND
- the invasion of privacy was either 'intentional or reckless' AND

[43] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 191-3.
[44] The term 'reasonable expectation of privacy' is further defined in clause 7(5).

- the invasion of privacy was 'serious'[45]
- the tort is actionable without proof of damage.[46]

This cause of action is limited by considerations of the public interest, whereby if the defendant adduces evidence that the invasion of privacy was in the 'public interest' then the plaintiff must satisfy the Court that the public interest in was outweighed by the 'public interest in protecting the plaintiff's privacy'.[47] A non-exhaustive list of factors that may be considered regarding this public interest test include:[48]

(a) freedom of expression, including political communication
(b) freedom of the media;
(c) the proper administration of government;
(d) open justice;
(e) public health and safety;
(f) national security;
(g) the prevention and detection of crime and fraud.

Clause 7(7) renders it immaterial if the infromation related to the plaintiff was true or not.

Clause 8 summarises the defences to the cause of action, which include the following:

(a) the invasion of privacy was required by law or court order
(b) the plaintiff, or their lawful agent, expressly or impliedly consented
(c) the defendant reasonably believed the conduct was necessary to prevent or lessen a serious threat to the life, health or safety of a person
(d) the conduct was:
    i. incidental to the exercise of a lawful right of defence of persons or property; and
    ii. proportionate, necessary and reasonable.

There are also exceptions to liability under the cause of action for – journalists, enforcement bodies, intelligence agencies and persons under 18.[49]

This implements Proposals 27.1 of the Privacy Act Review.[50]

7.1 ASFA's recommendations

ASFA recommends the following:

- Careful consideration should be given to situations where the same conduct might constitute misconduct under both the statutory tort in Schedule 2 and the direct right of action for serious invasions of privacy in clause 13G. In such circumstances, care must be taken to avoid the risk of double jeopardy, whereby a wrongdoer is punished twice for susbtantially the same conduct.
- The same considerations should be given to avoid double jeopardy with respect to the statutory tort and infringement notices which can be issued under clause 13K.
- Proof of damage should be required in order to receive damages. Thus, clause 7(2) should be removed.
- The amount of damages which the Court may award for 'emotional distress' should be subject to a maximum cap, as well as a 'reasonable person' test, in order to provide certainty to litigants.

[45] The term 'seriousness' is further defined in clause 7(6).
[46] Schedule 2, clause 7(3).
[47] Clause 7(3).
[48] Clause 7(4).
[49] Clauses 15 to 18.
[50] Attorney-General's Department (AGD), *Privacy Act Review: Final Report* (2022) 287.

Attachment B – ASFA's Summary of the Proposed Reforms

Changes to Privacy Laws in the Bill				
Proposal	**Bill**	**Explanatory Memo**	**Privacy Act Review**	**Government Response**
Commencement provisions	Pages 1-3	Pages 28-29	N/A	
Changing the objects of the Act to including 'to promote the protection of the privacy of individuals with respect to their personal information' and 'to recognise the public interest in protecting privacy'	Part 1 - Page 4	Pages 30	Proposals 3.1 – 3.2 on Page 5	Page 21
Outlines the circumstances in which the Commissioner may, at the direction of the Minister, develop a Code which relates to an Australian Privacy Principle (APP)	Part 2 – Page 5-8	Page 30-5	Proposals 5.1 – 5.2 on Page 6	Page 22
The purpose of Part 3 of this Bill is to enable emergency declarations to authorise more targeted handling of personal information to assist individuals in emergency and disaster situations to and to ensure that declarations may be made in relation to ongoing or extended emergencies or disasters.	Part 3 - Page 8-14	Page 35-9	Proposals 5.3 to 5.5 on Page 6	Page 23
Makes certain amendments in relation to children's privacy	Part 4 – Page 14-8	Page 39-43	Proposals 16.1 to 16.5 on Page 10	Page 29-30
Clarifying the 'reasonable steps' required of entities to protect information in Australian Privacy Principle 11 include technical and organisational measures	Part 5 - Page 18	Page 43-4	Proposal 21.1 on Page 13	Page 33

Providing greater certainty about when personal information can be disclosed overseas and increasing mechanisms to facilitate free flow of information across national borders while ensuring privacy of individuals is respected	Part 6 - Page 19-20	Page 44-45	Proposals 23.1 to 23.6 on Page 14	Page 34-5
Facilitating information sharing after an Eligible Data Breach of an entity, to prevent or reduce risk of harm arising from misuse of personal information	Part 7 - Page 21-30	Page 45-52	Proposals 28.1 to 28.4 on Page 15-6	Page 37
Introducing new penalties for breaches of the Privacy Act	Part 8 - Page 31-36	Pages 52-57	Proposals 25.1 to 25.3 on Pages 14	Page 35
Introducing stronger enforcement powers and a range of new orders that can be made by federal courts regarding privacy	Part 9 – Page 37-8	Page 57-8	Proposals 25.6 on Page 15	Page 36
Allowing the Information Commissioner to conduct public inquiries on privacy	Part 10 – Page 39-42	Page 58-62	Proposal 25.4 on Page 14	Page 36
The Information Commissioner has the power to make a determination under section 52 after investigating a complaint or after an Information Commissioner-initiated investigation. The determination may include a declaration requiring the respondent to take steps or perform certain actions, including to perform any reasonable act or course of conduct to redress any loss or damage suffered as a result of an interference with privacy or breach.	Part 11 – Page 43	Page 63	Proposal 25.5 on Page 14	Page 36
Procedural changes to the annual reporting requirements of the Commissioner	Part 12 – Page 44	Page 63-4	Proposals 25.9 – 25.10 on Page 15	Page 36
Grants broader discretion to the Commissioner to dismiss privacy complaints in certain circumstances	Part 13 – Page 45	Page 64	Proposal 25.11 on Page 15	Page 36
The Commissioner has a range of monitoring, assessment and investigation powers under the Privacy Act. This includes the power in section 68 enabling an authorised person to enter premises occupied by an agency, organisation, file number recipient, credit	Part 14 – Page 46-56	Page 64-77	N/A	N/A

reporting body or credit provider to inspect any documents that are kept at those premises and are relevant to the performance of the Information Commissioner's functions under the Privacy Act				
Requiring entities to include information in privacy policies about automated decisions that significantly affect rights or interests of an individual Introducing disclosure requirements about the use of computer programs that use personal information to make decisions that could reasonably be expected to significantly affect rights or interests of an individual	Part 15 – Page 57-8	Page 77-9	Proposals 19.1 to 19.2 on Page 12	Page 32
Introducing a new statutory cause of action to address serious invasions of privacy.	Schedule 2 – Pages 58-74	Pages 79-97	Proposal 27 on Page 15	Page 36
A new offence in relation to 'doxxing' – the publishing of personal data on personal information about an individual	Schedule 3 – Pages 75-81	Page 93-103	N/A	N/A