The Senate

Legal and Constitutional Affairs Legislation Committee

Privacy and Other Legislation Amendment Bill 2024 [Provisions]

November 2024

ISBN 978-1-76093-745-4 (Printed version)

ISBN 978-1-76093-745-4 (HTML version)

Printed by the Senate Printing Unit, Canberra

Contents

Members

Chair

Senator Nita Green	ALP, QLD

Deputy Chair

Senator Paul Scarr	LP, QLD

Members

Senator Alex Antic	LP, SA
Senator Varun Ghosh	ALP, WA
Senator Helen Polley	ALP, TAS
Senator David Shoebridge	AG, NSW

Secretariat

Sophie Dunstone, Committee Secretary
Monika Sheppard, Principal Research Officer
Mervyn Piesse, Senior Research Officer
Grace McElholum, Research Officer
Jessica Brown, Administrative Officer
Jamison Eddington, Administrative Officer

Suite S1.61
Parliament House
Canberra ACT 2600

Telephone: (02) 6277 3560

Email: legcon.sen@aph.gov.au

List of recommendations

Recommendation 1

2.380 The committee recommends that the minimum consultation period for the Children's Online Privacy Code is extended to at least 60 days.

Recommendation 2

2.382 The committee recommends that the bill is amended to include a requirement for the Information Commissioner to consult with relevant industry bodies or organisations when developing the Children's Online Privacy Code.

Recommendation 3

2.384 The committee recommends the exclusion for media organisations from accessing personal information during declared emergencies is extended to exclude national broadcasters such as the ABC and Special Broadcasting Service.

Recommendation 4

2.386 The committee recommends that the bill is amended to empower the Information Commissioner to issue a discretionary notice to an entity to remedy an alleged breach of one or more of the provisions in section 13K before issuing an infringement notice.

Recommendation 5

2.388 The committee recommends that the Explanatory Memorandum to the bill is amended to make clear that the level of information required in privacy policies is not expected to compromise commercial-in-confidence information about automated decision-making systems.

Recommendation 6

2.390 The committee recommends that the Commonwealth government considers amending clause 7 of the bill to:

- **require a court to consider the matters of public interest that justify the invasion of the plaintiff's privacy;**
- **not require a defendant to adduce evidence of public interest in every case; and**
- **provide that 'artistic expression' is a form of freedom of expression.**

Recommendation 7

2.392 The committee recommends that the Commonwealth government considers amending Schedule 2 of the bill to ensure that the journalism exemption applies to a person involved in the publication, re-publication or distribution of journalistic material.

Recommendation 8

2.394 The committee recommends that Schedule 2 of the bill is amended to make clear that the concept of 'journalistic material' for the serious invasions of privacy tort includes 'editorial' material.

Recommendation 9

2.396 The committee recommends that Schedule 2 is amended to make clear that the power conferred on a court to issue an injunction is not limited to an 'interim' injunction.

Recommendation 10

2.397 Subject to the preceding recommendations, the committee recommends that the Senate passes the bill.

Chapter 1
Introduction

1.1 On 19 September 2024, the Senate referred the provisions of the Privacy and Other Legislation Amendment Bill 2024 (the bill) to the Legal and Constitutional Affairs Legislation Committee (the committee) for inquiry and report by 14 November 2024.[1]

1.2 The referral followed a recommendation of the Senate Standing Committee for the Selection of Bills. Appendix 4 to that committee's report suggested an inquiry would allow stakeholders to examine the new offences in the bill particularly in relation to doxxing reforms and the effect of regulatory changes on online platforms and social media.[2]

Conduct of the inquiry

1.3 In accordance with its usual practice, the committee advertised the inquiry on its website and wrote to relevant organisations and individuals inviting submissions by 11 October 2024. The committee received 75 submissions, which are listed at Appendix 1 and are available on the committee's website.

1.4 The committee held a public hearing in Canberra on 22 October 2024. A list of witnesses is provided at Appendix 2.

1.5 Answers to questions on notice and other material received by the committee are listed at Appendix 1. Submissions and the *Hansard* transcript of evidence may be accessed through the committee website.

1.6 The committee thanks the organisations and individuals who gave evidence at the public hearing as well as those who made written submissions.

Structure of the report

1.7 The report comprises two chapters as follows:

- Chapter 1 outlines the administrative details of the inquiry, background to the inquiry and the key provisions of the bill.
- Chapter 2 explores the key issues raised in evidence and provides the committee's views and recommendations in relation to the bill.

---

1 *Journals of the Senate*, No. 135, 19 September 2024, pp. 4076–4079.

2 Senate Standing Committee for the Selection of Bills, *Report No. 11 of 2024*, 19 September 2024, Appendix 4, pp. [13–16].

Note on references

1.8 References to *Committee Hansard* are to proof transcripts. Page numbers may vary between proof and official transcripts.

Purpose of the bill

1.9 The bill would enact a first tranche of reforms to the *Privacy Act 1988* (Privacy Act) agreed by the government in its Response to the Privacy Act Review. The bill would also introduce a new statutory tort for serious invasions of privacy and targeted criminal offences to respond to doxxing.[3]

Background

1.10 On 3 September 2014, the Australian Law Reform Commission (ALRC) released the final report for its inquiry into serious invasions of privacy in the digital era. In that report, the ALRC recommended the establishment of a statutory cause of action for serious invasions of privacy.[4]

1.11 In June 2019, the Australian Competition and Consumer Commission (ACCC) released the *Digital Platforms Inquiry* report (DPI report). That report recommended that the government undertake a review of the Privacy Act.[5]

1.12 The DPI report also recommended the introduction of a statutory tort for serious invasions of privacy.

Box 1.1 Recommendation 19 — Statutory tort for serious invasions of privacy

Introduce a statutory cause of action for serious invasions of privacy, as recommended by the Australian Law Reform Commission (ALRC). This cause of action provides protection for individuals against serious invasions of privacy that may not be captured within the scope of the Privacy Act. The cause of action should require privacy to be balanced against other public interests, such as freedom of expression and freedom of the media. This statutory cause of action will increase the accountability of businesses for their data practices and give consumers greater control over their personal information.[6]

---

3 Note: The Hon Mark Dreyfus KC MP, Attorney-General, has foreshadowed that the government will consult on a second tranche of reforms, see: *House of Representatives Proof Hansard*, 12 September 2024, p. 22.

4 Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era: Final Report*, 3 September 2014, p. 9.

5 Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry*, June 2019, pp. 34–36.

6 ACCC, *Digital Platforms Inquiry*, June 2019, p. 37.

1.13 On 16 February 2023, the Hon Mark Dreyfus KC MP, Attorney-General, released the *Privacy Act Review Report 2022* (Privacy Act Review). It recognised that technological advancements have had significant implications for the privacy of personal information since the passage of the Privacy Act. Since that time:

> Digitalisation and technological innovation have had a significant impact on the ways in which personal information is exchanged and used, as well as the volume of information handled. Our society is increasingly networked: decisions made by one individual about their personal information can impact the privacy of others. At the same time, the community expects that personal information will be protected.[7]

1.14 On 28 September 2023, the government released its response to the Privacy Act Review. That response acknowledged the implications that technological advancement has had for the privacy of Australians' information:

> The digital economy has led to innovation, advances in productivity and efficiency and a range of other benefits for Australians. However, the vast data flows underpinning digital ecosystems have also created the conditions for recent major data breaches affecting millions of Australians, with their sensitive personal information being exposed to the risk of identity fraud and scams. Strong privacy protections are critical to building the security, confidence and trust necessary to drive innovation and economic growth.[8]

1.15 The Privacy Act Review 'concluded that it is necessary to overhaul Australia's privacy laws, as many other countries have done, to ensure they remain fit-for-purpose in the digital age'.[9]

1.16 There is widespread public support for privacy reform. According to the 2023 Office of the Australian Information Commissioner Australian Community Attitudes to Privacy Survey:

> Three in five (62%) of Australians surveyed see the protection of their personal information as a major concern in their life, and 75% consider that data breaches are one of the biggest privacy risks they face today (increasing by 13% since 2020). Only 32% feel in control of their data privacy, and 84% want more control and choice over the collection and use of their personal information. 89% would like the Government to provide more legislation in this area.[10]

---

7 Attorney-General's Department (AGD), *Privacy Act Review Report 2022* (Privacy Act Review), February 2023, p. 18.

8 AGD, *Government Response to the Privacy Act Review Report* (Government Response), September 2023, p. 2.

9 AGD, Government Response, September 2023, p. 2.

10 AGD, Government Response, September 2023, p. 2.

1.17 According to the Explanatory Memorandum (EM), the Privacy Act is not fit-for-purpose in the digital age. It does not adequately protect Australians' data, particularly as the digital landscape has evolved. Privacy legislation:

> …has not kept pace with Australians' widespread adoption and reliance on digital technologies, which increases the risks that personal data will be subject to misuse or mishandling, including through data breaches, fraud and identity theft, unauthorised surveillance and other significant online harms.[11]

1.18 The EM defines doxxing as 'the intentional malicious exposure of an individual's personal data online'. The public release of that data may:

> …expose victims, including family members and associates of the individual whose data is released, to a wide range of harms including harassment and threats to their lives or physical safety, public embarrassment, humiliation or shaming, discrimination, stalking, identity theft and financial fraud.[12]

1.19 It further states that, once the data becomes publicly available, the risk of harm may be enduring. To address that risk:

> Victims of doxxing may be required to take significant steps, and incur significant cost and hardship…Doxxing can also cause psychological harms, both directly and as a result of the occurrence, or the fear of the occurrence, of the previously-mentioned harms.[13]

1.20 The victims of doxxing are exposed:

> …to physical threats, public embarrassment, humiliation or shaming, discrimination, identity theft and financial fraud, and other serious harms. These risks are magnified where the release of personal information involves women and children in the context of domestic and family violence.[14]

1.21 The Attorney-General's Department (AGD) reported that it:

> …received approximately 100 submissions through the public consultation process on doxxing. That was a process that we held between 11 to 20 March 2024. In addition to that, we convened a roundtable on doxxing and privacy reforms alongside the eSafety Commissioner.[15]

---

11 Explanatory memorandum (EM), p. 3.

12 EM, pp. 5–6.

13 EM, p. 6.

14 EM, p. 3.

15 Ms Elizabeth Brayshaw, Acting First Assistant Secretary, Integrity Frameworks Division, AGD, *Proof Committee Hansard*, 31 May 2024, p. 113.

1.22 The government agreed that an overhaul of the Privacy Act is required for multiple reasons, including to safeguard personal information and the competitiveness of Australian businesses:

> Australia can no longer afford to have inadequate privacy protections. Privacy uplift is needed to guard against identity fraud, scams and the risk to businesses of failing to manage personal information appropriately. Business sustainability relies on the ability to protect personal information. A failure to uplift Australia's privacy standards to more closely align with global standards also has the potential to adversely impact the international competitiveness of Australian businesses.[16]

1.23 The Privacy Act Review proposed 89 legislative changes. Of those proposed changes, the government 'agreed to 25 proposals, agreed in-principle to 56 and noted eight'. If it is passed, '[t]he bill would implement 23 of the 25 legislative proposals that were agreed in the Government Response to the Privacy Act Review'.[17]

1.24 In introducing the bill to the House of Representatives, the Attorney-General outlined its main provisions:

> Schedule 1 of the bill will amend the Privacy Act to enhance its effectiveness, strengthen the enforcement tools available to the privacy regulator and better facilitate safe overseas data flows. It will require the development of a children's online privacy code, streamline information-sharing in emergencies and following eligible data breaches, and increase transparency when entities are automating significant decisions which use personal information.
>
> Schedule 2 of the bill will introduce a new statutory tort to provide redress for serious invasions of privacy.
>
> Schedule 3 of the bill will amend the *Criminal Code Act 1995* to introduce new criminal offences to target the harmful practice of doxxing.[18]

Key provisions of the bill

1.25 The bill comprises the following three schedules:

- Schedule 1—Privacy reforms;
- Schedule 2—Serious invasions of privacy; and
- Schedule 3—Doxxing offences.

---

16 AGD, Government Response, September 2023, p. 2.

17 EM, p. 3.

18 The Hon. Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 22.

Schedule 1—Privacy reforms

1.26 The privacy reforms contained in Schedule 1 of the bill are divided into 15 parts. The key provisions of Schedule 1 raised by submitters are contained in the following parts:

- Part 2—Australian Privacy Principle (APP) codes;
- Part 3—Emergency declarations;
- Part 4—Children's privacy;
- Part 6—Overseas data flows;
- Part 8—Penalties for interference with privacy; and
- Part 15—Automated decisions and privacy policies.

Part 2—Australian Privacy Principle codes

1.27 The bill would amend the Privacy Act to allow the minister to direct the Information Commissioner to develop an APP code.[19] Before registering that code, the Information Commissioner would be required to make a draft of it publicly available and invite the public to make submissions about the draft over a period of at least 40 days.[20]

1.28 An APP code is:

> …a written code of practice for the handling of personal information…[that] sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code.[21]

1.29 The bill would also amend the Privacy Act to allow the minister to direct the Information Commissioner to develop a temporary APP code if there is an urgent need for such a code to be made.[22] A temporary APP code would not be able to operate for a period longer than 12 months.[23]

1.30 According to the EM:

> APP codes provide greater clarity and specificity about how the principles-based [APPs] are to be applied and complied with. The Bill enhances the right to privacy by promoting greater compliance and providing confidence to members of the community that their personal information will be handled appropriately. This is particularly important

---

19 Item 5 in Part 2 of Schedule 1 of the Privacy and Other Legislation Amendment Bill 2024 [Provisions] (the bill); proposed section 26GA of the bill.

20 Item 5 in Part 2 of Schedule 1 of the bill; proposed subsection 26GA(7) of the bill.

21 Office of the Australian Information Commissioner, *Privacy codes register*, no date, www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-codes-register (accessed 7 November 2024).

22 Item 5 in Part 2 of Schedule 1 of the bill; proposed section 26GB of the bill.

23 Item 5 in Part 2 of Schedule 1 of the bill; proposed subsection 26GB(7) of the bill.

> given the growing calls for APP codes to be developed in response to the privacy risks arising from new and emerging technologies.[24]

1.31 The establishment of temporary APP codes 'would promote the right to privacy by providing greater flexibility and efficiency to the APP code-making process'.[25] For example, during a pandemic emergency temporary APP codes could be developed:

> …to instruct APP entities on how to comply with APPs while collecting contact-tracing information, and give greater transparency to the community on how their personal information is being handled.[26]

1.32 Temporary APP codes are intended to only be in force during urgent situations:

> If it was proposed that the enforceable requirements within a temporary APP code would be extended beyond a 12-month period, these should be subject to the usual provisions for developing an APP code, including mandatory consultation on the code and tabling in Parliament.[27]

Part 3—Emergency declarations

1.33 The bill would amend the Privacy Act to require an emergency declaration to specify the kinds of personal information,[28] types of entities permitted to share personal information,[29] and the purposes for which that information may be shared.[30]

---

[24] EM, p. 10.

[25] EM, p. 10.

[26] EM, p. 33.

[27] EM, p. 34.

[28] Note: the EM suggests that the kinds of personal information would be specified in the declaration. The declaration could, for example, 'specify that only an individual's legal identity and identity documents may be handled', see: p. 36.

[29] Note: the EM suggests that the types of entities would be specified in the declaration. The declaration could, for example, 'specify that only health service providers may disclose personal information to entities who provide humanitarian aid', see: p. 36.

[30] Item 13 in Part 3 of Schedule 1 of the bill; proposed subsection 80KA(1) of the bill. Note: the types of entities that would be permitted to share personal information could include a state or territory authority. Such an entity must not be or include a media organisation, see: Item 13 in Part 3 of Schedule 1 of the bill; proposed subsection 80KA(2) of the bill. The EM suggests that the permitted purposes for sharing personal information would be specified in the declaration. The declaration could, for example, 'specify that entities may only handle personal information for the purposes of identifying individuals who are or may be, or at risk of, being injured, missing or dead', see: p. 36.

1.34 The permitted purposes for sharing that information would be required to relate to the Commonwealth's response to the emergency or disaster for which an emergency declaration is in force.[31]

1.35 During declared emergencies or disasters, those purposes may include:

- identifying individuals involved, or at risk of being involved;[32]
- assisting individuals affected, or at risk of being affected, to gain access to services;
- assisting law enforcement;
- coordinating or managing the response;
- ensuring that other persons responsible for those individuals affected, or at risk of being affected, are informed of matters related to those individuals.[33]

1.36 The emergency declarations provisions of the bill would 'authorise more targeted handling of personal information to assist individuals in emergency and disaster situations'.[34]

1.37 The Attorney-General explained that the bill would allow the sharing of personal information by permitted entities following disasters or emergencies. The sharing of that information would 'support response efforts, including to assist affected individuals'.[35]

Part 4—Children's privacy

1.38 The bill would require the Information Commissioner to develop an APP code about online privacy for children. That APP code would be known as the Children's Online Privacy Code (COP Code).[36]

1.39 According to the EM, '[t]he 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'.[37]

---

31 Item 13 in Part 3 of Schedule 1 of the bill; proposed subsection 80KA(3) of the bill. Note: according to the EM, this provision would 'limit the types of situations for which a declaration may authorise information handling', see: p. 37.

32 Note: those individuals include those who are, or are at risk of becoming, injured, missing or dead as a result of the emergency or disaster, see: Item 13 in Part 3 of Schedule 1 of the bill; proposed paragraph 80KA(4)(a) of the bill.

33 Item 13 in Part 3 of Schedule 1 of the bill; proposed subsection 80KA(4) of the bill. Note: the EM states this 'list is intended merely as a guide'. It should not limit the purposes for which information may be shared, see: p. 37.

34 EM, p. 35.

35 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 22.

36 Item 32 in Part 4 of Schedule 1 of the bill; proposed subsection 26GC(1) of the bill.

37 EM, p. 25.

1.40 An APP entity would be bound by the COP Code if:

- it provides a social media service, relevant electronic service or designated internet service within the meaning of the *Online Safety Act 2021*;
- children are likely to access the service; and
- it does not provide a health service;[38] or
- it is an APP entity, or is included in a class of APP entities, specified in the COP Code.[39]

1.41 The Information Commissioner must develop and register the COP Code within two years of the bill receiving Royal Assent.[40]

1.42 The COP Code would be required to set out how the APPs 'are to be applied or complied with in relation to the privacy of children'.[41] For example, the COP Code could set out how APP entities communicate their privacy policies and consent notices to children:

> …the COP Code may set out how regulated entities must meet requirements in APP 1 and 5 in relation to privacy policies and consent notices by ensuring that information addressed to a child is clearly expressed and understandable – such as through the use of graphics, video and audio content rather than relying solely on written communication.[42]

1.43 Providers of online services 'are expected to proactively assess the likelihood that their service is accessed by children, regardless of if the service is not explicitly targeted at children'.[43] To assist them in making that assessment, the Information Commissioner may provide written guidelines to assist entities in determining whether they provide a service that is likely to be accessed by children.[44]

---

38 Item 32 in Part 4 of Schedule 1 of the bill; proposed paragraph 26GC(5)(a) of the bill. Note: the EM indicates this provision would ensure 'the COP Code is not a barrier to providing essential services to children'. For the purposes of the bill, a health service 'can cover online health services such as counselling, advice and telehealth. However, more general health, fitness or wellbeing apps or services may be covered by the COP Code', see: pp. 41–42.

39 Item 32 in Part 4 of Schedule 1 of the bill; proposed paragraph 26GC(5)(b) of the bill.

40 Item 32 in Part 4 of Schedule 1 of the bill; proposed subsection 26GC(10) of the bill.

41 Item 32 in Part 4 of Schedule 1 of the bill; proposed subsection 26GC(3) of the bill.

42 EM, p. 40.

43 EM, p. 41. Note: the EM suggests that in assessing whether they provide a service that could be accessed by children, online service providers should consider: whether the nature and content of their service is likely to appeal to children; market research and user information related to their service or other similar services; and whether there are any measures in place that effectively prevent children from accessing the service, see: p. 41.

44 Item 32 in Part 4 of Schedule 1 of the bill; proposed subsection 26GC(11) of the bill.

1.44 The COP Code would differ from other APP codes as it must be developed by the Information Commissioner rather than 'by an APP code developer on their own initiative, or on request by the Information Commissioner'. The COP Code would be developed in this way as:

> There is a public interest and community expectation in ensuring that a COP Code is developed and registered, and is developed by the Information Commissioner who has particular expertise in privacy. This will avoid any potential industry regulatory biases, and conflicting commercial interests.[45]

1.45 The Attorney-General indicated that children are particularly vulnerable to online privacy risks. The extent of that risk is evident in the amount of data that is collected about them. According to the Attorney-General, 'by the time a child turns 13, around 72 million pieces of data will be collected about them'.[46]

1.46 Social media companies and other providers of online services accessed by children would be required to adhere to the COP Code. The code would 'specify how these entities must comply with privacy obligations in relation to children'. It would also align as closely as 'possible with similar codes in like-minded countries, such as the United Kingdom'.[47]

Part 6—Overseas data flows

1.47 The bill would amend the Privacy Act to introduce APP 8.3.[48] That APP would allow for countries, or binding schemes, that have data privacy laws that are 'substantially similar' to Australia's to be prescribed via regulation.[49]

1.48 The EM states that its introduction:

> …would enhance the free flow of information across national borders while ensuring the privacy of individuals is respected by providing greater certainty to disclosing entities about the standard of privacy protections in countries in which overseas recipients of personal information are located.[50]

1.49 In the globalised economy, the transnational flow of information 'is critical for international trade and services'. The bill would enable 'countries with substantially similar data privacy laws to Australia to be prescribed. Businesses and individuals will be able to have greater confidence that personal

---

45 EM, p. 40.

46 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 22.

47 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 22.

48 Item 38 in Part 6 of Schedule 1 of the bill; subcl. 8.3 of the bill.

49 Item 36 in Part 6 of Schedule 1 of the bill; proposed subsections 100(1A) and 100(1B) of the bill.

50 EM, p. 11.

information will be kept safe'. The provision would 'also reduce costs for business when entering into contracts and agreements with overseas entities'.[51]

Part 8—Penalties for interference with privacy

1.50 The bill would amend the Privacy Act to introduce civil penalty provisions for the serious interference with the privacy of an individual.[52]

1.51 To determine if an interference with the privacy of an individual is serious, the following factors may be taken into account:

(a) the particular kind or kinds of information involved in the interference with privacy;
(b) the sensitivity of the personal information of the individual;
(c) the consequences, or potential consequences of the interference with privacy for the individual;
(d) the number of individuals affected by the interference with privacy;
(e) whether the individual affected by the interference with privacy is a child or person experiencing vulnerability;
(f) whether the act was done, or the practice engaged in, repeatedly or continuously;
(g) whether the contravening entity failed to take steps to implement practices, procedures and systems to comply with their obligations in relation to privacy in a way that contributed to the interference with privacy; and
(h) any other relevant matter.[53]

1.52 The maximum penalty that would be applied to someone who is found to have seriously interfered with an individual's privacy would be 2000 penalty units (currently $626 000).[54] Alternatively, if the court finds that an individual's privacy has been interfered with, but not in a serious manner, it may make a pecuniary penalty order.[55]

1.53 The bill would allow a court to apply a civil penalty to an entity if it is found noncompliant with certain APPs. That penalty would not exceed 200 penalty units (currently $62 600).[56]

1.54 The EM states that the bill would introduce a tiered penalty regime that is 'commensurate with the seriousness of the interference with privacy'.[57]

---

51 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 23.

52 Item 50 in Part 8 of Schedule 1 of the bill; proposed subsection 13G(1) of the bill.

53 Item 51 in Part 8 of Schedule 1 of the bill; proposed subsection 13G(1B) of the bill.

54 Item 56 in Part 8 of Schedule 1 of the bill; proposed subsection 13H(3) of the bill.

55 Item 56 in Part 8 of Schedule 1 of the bill; proposed section 13J of the bill.

56 Item 56 in Part 8 of Schedule 1 of the bill; proposed section 13K of the bill.

57 EM, p. 12.

1.55 The Attorney-General argued the tiered civil penalty regime would assist in the enforcement of the Privacy Act.[58]

Part 15—Automated decisions and privacy policies

1.56 The bill would amend the Privacy Act to introduce APP 1.7.[59] That principle would apply to an APP entity if:

(a) the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making a decision;
(b) the decision could reasonably be expected to significantly affect the rights or interests of an individual; and
(c) 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.[60]

1.57 If APP 1.7 applies to an entity, the entity would be required to provide the following information in its privacy policy:

(a) the kinds of personal information used in the operation of such computer programs;
(b) the kinds of such decisions made solely by the operation of such computer programs; and
(c) the kinds of such decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.[61]

1.58 Automated decision-making processes 'have the potential to increase the efficiency, accuracy and consistency of decisions, and they present opportunities for improved outcomes in health, environment, defence and national security'.[62]

1.59 The bill would 'provide individuals with transparency about the use of their personal information in automated decisions which significantly affect their interests'. Any entity that makes automated decisions would be required 'to specify the kinds of personal information used in these sorts of decisions in their privacy policies'.[63]

Schedule 2—Serious invasions of privacy

1.60 Schedule 2 of the bill would insert a statutory tort for serious invasions of privacy into the Privacy Act.

---

58 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, pp. 22–23.

59 Item 87 in Part 15 of Schedule 1 of the bill; proposed subparagraph 13K(1)(b)(iia) of the bill.

60 Item 88 in Part 15 of Schedule 1 of the bill.

61 Item 88 in Part 15 of Schedule 1 of the bill.

62 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 23.

63 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 23.

1.61 The objects of Schedule 2 would be to:

(a) establish a cause of action for serious invasions of privacy;
(a) provide for defences, remedies and exemptions in respect of the cause of action;
(b) recognise that there is a public interest in protecting privacy;
(c) recognise that the public interest in protecting privacy is balanced with other public interests; and
(d) implement Australia's international obligations in relation to privacy.[64]

Cause of action

1.62 The bill would provide a plaintiff with a cause of action in tort against a defendant if:

(a) the defendant invaded the plaintiff's privacy by doing one or both of the following:

(i) intruding upon the plaintiff's seclusion;
(ii) misusing information that relates to the plaintiff; and

(b) a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances;
(c) the invasion of privacy was intentional or reckless; and
(d) the invasion of privacy was serious.[65]

1.63 Proof of damage would not be required to demonstrate that the defendant invaded the plaintiff's privacy.[66]

1.64 If the defendant argues that there was a public interest in invading the privacy of the plaintiff, the defendant would be required to provide evidence to demonstrate the public interest outweighed the protection of the plaintiff's privacy.[67]

1.65 Without restricting the kind of evidence that the defendant could present, the kind of evidence they could provide to meet the public interest test would include:

(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; or

---

64 Item 1 in Part 1 of Schedule 2 of the bill.

65 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(1) of the bill.

66 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(2) of the bill.

67 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(3) of the bill

(g) the prevention and detection of crime and fraud.[68]

1.66 In its consideration of whether the plaintiff had a reasonable expectation of privacy, the court may consider the following non-exhaustive matters:

- how the defendant invaded the plaintiff's privacy, including through the use of a device or technology;
- the defendant's reason for invading the plaintiff's privacy;
- the plaintiff's personal attributes, such as age, occupation or cultural background;
- whether the plaintiff 'invited publicity or manifested a desire for privacy';
- where the intrusion of the plaintiff's privacy occurred;
- the type of information that the defendant misused in their invasion of the plaintiff's privacy, how that information was obtained or shared by the defendant, and the extent to which that information was already in the public domain.[69]

1.67 To determine if the invasion of privacy was serious, the court may consider a range of matters not limited to:

(a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff;
(b) whether the defendant knew or ought to have known that the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff;
(c) if the invasion of privacy was intentional—whether the defendant was motivated by malice.[70]

1.68 The EM states that the statutory cause of action:

> …would implement the Australian Law Reform Commission's recommendation in its 2008 report For Your Information: Australian Privacy Law and Practice (ALRC Report 108). The model of the statutory tort set out in this Bill is informed by the ALRC's 2014 report Serious Invasions of Privacy in the Digital Era (ALRC Report 123).[71]

---

68 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(4) of the bill.

69 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(5) of the bill. Note: for the purpose of the bill, the information misused by the defendant in the course of invading the plaintiff's privacy may be true or false, see: Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(7).

70 Item 7 in Part 2 of Schedule 2 of the bill; subcl. 7(6).

71 EM, p. 5. Also see: ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, 12 August 2008; ALRC, *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*, 3 September 2014.

1.69 The Attorney-General explained that the bill would address community expectations in relation to individual rights to seek legal recourse when reasonable expectations of privacy have been breached. He stated:

> There are parts of our lives that we reasonably expect to be able to keep to ourselves. The freedom to enjoy a private and family life, and express ourselves and our beliefs in safety, is critical to our wellbeing and dignity.
>
> Ensuring that individuals have a clear right to seek a legal remedy against people or entities who seriously invade their privacy is a key part of ensuring that our privacy laws keep pace with community expectations and advances in technology.[72]

Defences

1.70 It would be a defence to the cause of action if the:

- invasion of the plaintiff's 'privacy was required or authorised by or under an Australian law or court/tribunal order';
- plaintiff, or a person lawfully acting on their behalf, 'expressly or impliedly consented to the invasion of privacy';
- defendant had a reasonable belief that invading the plaintiff's 'privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person';
- invasion of the plaintiff's privacy was 'incidental to the exercise of a lawful right of defence of persons or property and proportionate, necessary and reasonable';
- defendant published defamatory information about the plaintiff and there is a related defence under Australian law that references the invasion of privacy.[73]

Interim injunctions

1.71 The bill would allow a court to 'grant an injunction restraining the defendant from invading the plaintiff's privacy'. In cases where the defendant invaded the plaintiff's privacy by publishing information related to them, 'the court must have particular regard to the public interest in the publication of the information when considering whether to grant the injunction'.[74]

---

[72] The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 23.

[73] Item 8 in Part 2 of Schedule 2 of the bill; cl. 8 of the bill.

[74] Item 9 in Part 2 of Schedule 2 of the bill; cl. 9 of the bill.

Damages

1.72 The bill would not allow a court to award aggravated damages. The court would be able to award damages for emotional distress. In exceptional circumstances, the court would be able to award exemplary or punitive damages.[75]

1.73 The sum of the damages awarded against the defendant would not exceed the greater of $478 550 and 'the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law'.[76]

1.74 When determining the amount of damages, the court may consider how the plaintiff and defendant engaged with each other after the invasion of privacy occurred. The matters it could consider could include, but not be limited to:

(a) whether the defendant apologised to the plaintiff;[77]
(b) if the defendant invaded the plaintiff's privacy by publishing information that relates to the plaintiff—whether the defendant published a correction;
(c) whether the plaintiff received or agreed to receive compensation in relation to the invasion of privacy;
(d) whether the plaintiff or the defendant took reasonable steps to settle the dispute;
(e) whether the defendant engaged in conduct after the invasion of privacy, including during the proceedings, that was unreasonable and subjected the plaintiff to particular or additional embarrassment, harm, distress or humiliation.[78]

1.75 The court would be able to grant other remedies instead of, or in addition to, awarding damages.[79]

Exemptions

1.76 If the invasion of privacy involved 'the collection, preparation for publication or publication of journalistic material', the cause of action would not apply to:

(a) a journalist;
(b) an employer of a journalist;
(c) a person assisting a journalist who is employed or engaged by the journalist's employer; or

---

75 Item 11 in Part 2 of Schedule 2 of the bill; cl. 11 of the bill.

76 Item 11 in Part 2 of Schedule 2 of the bill; subcl. 11(5) of the bill.

77 An apology would 'not constitute an express or implied admission of fault or liability by the defendant in connection with the invasion of privacy'. It would also not be 'relevant to the determination of fault or liability in connection with the invasion of privacy', see: Item 13 in Part 2 of Schedule 2 of the bill; cl. 13 of the bill.

78 Item 11 in Part 2 of Schedule 2 of the bill; subcl. 11(6) of the bill.

79 Item 12 in Part 2 of Schedule 2 of the bill; subcl. 12(1) of the bill.

(d) a person assisting a journalist in the person's professional capacity.[80]

1.77 The cause of action would also not apply to:

- enforcement bodies, provided 'that the invasion of privacy is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body';[81]
- intelligence agencies;[82]
- someone under the age of 18;[83] or
- a deceased person or a representative of that person.[84]

1.78 According to the Attorney-General, '[t]hese exemptions are important to protect press freedom, and ensure that legitimate activities of government can be delivered effectively'.[85]

Schedule 3—Doxxing offences

1.79 Schedule 3 of the bill would amend the *Criminal Code Act 1995* (Criminal Code) to create new doxxing offences.

1.80 For the purpose of the doxxing offences, the bill would define personal data as information that could enable an individual or group of individuals to be identified, contacted or located. That information would include any of the following details of an individual or group of individuals:

- their name or names;
- photographs or other images of them;
- their telephone number or numbers;
- their email address or addresses;
- details of an online account or accounts belonging to them;
- their residential address or addresses;
- their work or business address or addresses;
- a place or places of education attended by them; or
- a place or places of worship attended by them.[86]

---

80 Item 15 in Part 3 of Schedule 2 of the bill; subcl. 15(1) of the bill.

81 Item 16 in Part 3 of Schedule 2 of the bill; cl. 16 of the bill.

82 Item 17 in Part 3 of Schedule 2 of the bill; cl. 17 of the bill.

83 Item 18 in Part 3 of Schedule 2 of the bill; cl. 18 of the bill.

84 Item 20 in Part 4 of Schedule 2 of the bill; subcl. 20(1) of the bill.

85 The Hon Mark Dreyfus KC MP, Attorney-General, *House of Representatives Proof Hansard*, 12 September 2024, p. 24.

86 Item 1 in Schedule 3 of the bill; proposed subsections 474.17C(2) and 474.17D(2) of the bill.

Using a carriage service to make personal information publicly available

1.81 If a person uses a carriage service to share the personal data of one or more individuals in a menacing or harassing way, then that person would have committed an offence. The penalty for committing the offence would be imprisonment for six years.[87]

1.82 For example, if a person publishes an individual's name, image and telephone number on a website and encourages other people to harass that individual by leaving them violent or threatening messages that is an example of doxxing that would be covered by the bill.[88]

Using a carriage service to make personal information of one or more members of certain groups publicly available

1.83 A person would have committed an offence if they use a carriage service to share the personal information of one or more members of a group based on a belief that they have certain characteristics and share that information in a menacing or harassing way. The penalty for committing this offence would be imprisonment for seven years.[89]

1.84 For example, if a person publishes the name, image and residential address of one or more members of a private online religious discussion group on a website and encourages other people to attend those addresses, block entryways, or otherwise harass the members of the group that would be an example of doxxing that would be covered by the bill.[90]

Consideration by other parliamentary committees

1.85 When examining a bill, the committee takes into account any relevant comments published by the Senate Standing Committee for the Scrutiny of Bills (the Scrutiny Committee) and the Parliamentary Joint Committee on Human Rights (PJCHR).

---

87 Item 1 in Schedule 3 of the bill; proposed subsection 474.17C(1) of the bill.

88 Note to Item 1 in Schedule 3 of the bill; proposed subsection 474.17C(1) of the bill.

89 Item 1 in Schedule 3 of the bill; proposed subsection 474.17D(1) of the bill. Note: those characteristics include 'race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin'. Proposed subsection 474.17D(3) clarifies that 'it is immaterial whether the group is actually distinguished by' those characteristics.

90 Note to Item 1 in Schedule 3 of the bill; proposed subsection 474.17D(1) of the bill.

Senate Standing Committee for the Scrutiny of Bills

1.86 The Scrutiny Committee stressed that the exemption of legislative instruments from disallowance should only be permitted under 'exceptional circumstances'. There should be a full justification as to why legislation would be exempt from the usual disallowance process in the bill's EM.[91]

1.87 The Scrutiny Committee acknowledged that the EM explains the exemption is necessary 'to ensure that decisive action can be taken'. In emergency situations or in scenarios where events are quickly changing the exemption 'would establish an immediate, clear and certain legal basis for entities to handle personal information'.[92]

1.88 In the view of the Scrutiny Committee that could be achieved 'while allowing parliamentary oversight'. It did not consider this an appropriate basis for 'an exemption from disallowance'. The Scrutiny Committee left it for the Senate to determine the appropriateness of exempting the provisions from disallowance and drew the matter to the attention of the Senate Standing Committee for the Scrutiny of Delegated Legislation.[93]

1.89 In relation to the exemption of disallowance for the creation of temporary APP codes, the Australian Human Rights Commission considered 'the exemption from disallowance is – on balance – appropriate in these limited circumstances'.[94]

1.90 The AGD stated the provisions of the bill that would be exempt from disallowance relate to circumstances 'where prompt action and certainty is required'. For example, during declared emergencies and data breaches 'people would be able to rely on the contents of [the legislative instrument] immediately'.[95]

---

91 Senate Standing Committee for the Scrutiny of Bills (Scrutiny Committee), *Scrutiny Digest 13/24*, 9 October 2024, pp. 44–45.

92 Scrutiny Committee, *Scrutiny Digest 13/24*, 9 October 2024, pp. 45–46; EM, pp. 34–36 and 48–49.

93 Scrutiny Committee, *Scrutiny Digest 13/24*, 9 October 2024, p. 46.

94 Australian Human Rights Commission, Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024).

95 Ms Catherine Fitch, Assistant Secretary, Privacy Reform Taskforce, Integrity Frameworks Division, AGD, *Committee Hansard*, 22 October 2024, p. 66.

Chapter 2
Key issues

2.1 While most participants in the inquiry broadly supported the provisions of the Privacy and Other Legislation Amendment Bill 2024 (the bill), issues were mainly raised in relation to the provisions that related to the:

- Australian Privacy Principle (APP) codes;
- emergency declarations;
- Children's Online Privacy Code (COP Code);
- overseas data flows;
- penalties for interference with privacy;
- automated decision making (ADM) and privacy policies;
- statutory tort for serious invasions of privacy;
- doxxing offences; and
- future privacy reforms.

2.2 Speaking on behalf of several civil society organisations with an interest in digital technologies, Ms Elizabeth O'Shea, Chair, Digital Rights Watch (DRW), broadly reflected on the bill:

> Collectively, we welcome this bill and think that it is a good first step in the journey to improve and strengthen the *Privacy Act 1988* [Privacy Act]. The Privacy Act has not been meaningfully updated in nearly four decades and it's simply not capable of responding to the significant technological changes we've seen in this time.[1]

2.3 Reset.Tech Australia agreed with that assessment by stating 'Australia's privacy laws are substantially out-of-date and ineffective in the digital age'.[2]

2.4 The Attorney-General's Department (AGD) highlighted the importance of reform to Australian privacy laws:

> The rapid evolution of technology is transforming the way Australians engage with each other, providing significant benefits and opportunities. However, advances in technology are also facilitating harms, like scams, fraud and doxxing, and research indicates the law has not kept pace with community expectations.[3]

---

1 Ms Elizabeth O'Shea, Chair, Digital Rights Watch (DRW), *Committee Hansard*, 22 October 2024, p. 17.

2 Reset.Tech Australia, *Submission 3*, p. 1.

3 Attorney-General's Department (AGD), *Submission 31*, p. 2.

2.5 It is necessary to reform the Privacy Act to ensure that it is able to provide an appropriate level of protection to Australians in the digital age. As the AGD highlighted:

> Strong privacy protection reforms are critical to the Government's efforts across a range of areas to ensure technology is deployed for the benefit of Australians. The measures in this Bill and future privacy reforms will support initiatives to protect children and adults from online harms, uplift cyber security across the economy, prevent and address scam and other fraudulent activity, ensure the adoption of safe and responsible Artificial Intelligence [AI] and provide a comprehensive and consistent legal framework to support the use of automated decision-making by Government.[4]

Australian Privacy Principle codes

2.6 Access Now argued the ability for the Information Commissioner to develop APP codes in the public interest would 'provide a regulatory backstop in case industry initiatives are slow or inadequate'.[5]

2.7 The Human Rights Law Centre (HRLC) also welcomed the proposal to grant 'greater powers and flexibility' to the Information Commissioner. Allowing the commissioner to develop temporary APP codes would be 'particularly important' when there is a higher necessity to safeguard personal information in situations that are rapidly evolving or uncertain. It is appropriate that the safeguard to prevent the temporary APP code from being in force for longer than 12 months is included in the bill.[6]

2.8 The Internet Association of Australia (IAA) suggested the bill be amended to require the Information Commissioner to:

> …consult with entities that would be subject to the APP Code or temporary APP Code (as the case may be), and any other person the Commissioner considers appropriate in the development of APP Codes and temporary APP Codes.[7]

2.9 Mr Harry Godber, Head of Policy and Strategy, Tech Council of Australia, questioned the appropriateness of temporary APP codes for the technology industry. Given that they would only operate for up to 12 months:

> I would question whether a temporary 12-month code would reflect the reality of what is required for tech companies to comply, which typically, depending on the nature of the reform, could include restructuring the way

---

4 AGD, *Submission 31*, pp. 2–3.

5 Access Now, *Submission 55*, p. 3.

6 Human Rights Law Centre (HRLC), *Submission 60*, p. 11.

7 Internet Association of Australia (IAA), *Submission 29*, p. 2.

> that data is collected, managed and held. It would require systems reforms that would take potentially longer than 12 months to implement.[8]

2.10 The Business Council of Australia (BCA) opposed the provisions that would expand the Information Commissioner's power to make APP codes as it would increase their 'role through delegated legislation, and risks imposing confusing and misinformed compliance obligations on participants'.[9]

2.11 The BCA warned the bill 'does not specify what the Minister must consider in determining that the Commissioner should make a code'. It suggested that could lead to situations where the minister makes decisions about 'how industry should operate, without consideration of the experiences of those directly impacted'.[10]

2.12 The Law Council of Australia (Law Council) did not support the proposal in the Privacy Act Review Report that would enhance the Information Commissioner's code-making powers, which the provisions related to the APP code-making process are based upon. It argued that the proposal lacked 'sufficient clarity and, consequently, carried the potential for conflict and uncertainty'.[11]

2.13 The Law Council argued the Information Commissioner has significant 'knowledge of developments in the technological and privacy sphere…[and] is, therefore, well-placed to identify matters that need to be addressed by way of an APP code'.[12]

2.14 If the provisions that would enhance the Information Commissioner's code-making powers are to remain, the Law Council recommended the bill be amended:

> …to empower the Information Commissioner to advise the Minister of the necessity for an APP code (or temporary code), and so that the Minister is required to consider this request prior to issuing a direction under proposed sections 26GA and 26GB of the Privacy Act.[13]

2.15 The AGD argued the amendment proposed by the Law Council is unnecessary:

> The Information Commissioner already has advice-related functions as set out in section 28B of the Privacy Act which may be performed by the Information Commissioner on request or on the Commissioner's own initiative and include: Subsection (1)(a) providing advice to a Minister about any matter relevant to the operation of the Privacy Act, and Subsection (1)(c)

---

8 Mr Harry Godber, Head of Policy and Strategy, Tech Council of Australia, *Committee Hansard*, 22 October 2024, p. 14.

9 Business Council of Australia (BCA), *Submission 56*, p. 8.

10 BCA, *Submission 56*, p. 8.

11 Law Council of Australia (Law Council), *Submission 67*, p. 19.

12 Law Council, *Submission 67*, p. 19.

13 Law Council, *Submission 67*, p. 20.

> providing recommendations to the Minister in relation to any matter concerning the need for, or the desirability of, legislative or administrative action in the interests of the privacy of individuals.[14]

2.16 The AGD explained that 'APP codes provide entities with certainty on how to comply with their obligations and provide individuals with transparency about how their information will be handled'. The amendment to the APP code-making process would 'provide clarity on how new privacy obligations will apply in different circumstances, including in the context of new and emerging technologies'.[15]

2.17 The Office of the Australian Information Commissioner (OAIC) stated consultation with entities affected by an APP code 'is a critical component of any code development process'. That office also has guidelines for the development of APP codes, which includes consultation requirements. Those guidelines will be updated to reflect any amendments to the code making process if the relevant provisions of the bill are passed.[16]

Emergency declarations

2.18 The main issue raised in relation to the emergency declaration provisions of the bill related to a potential drafting error in the bill.

2.19 The ABC and the Special Broadcasting Service (SBS) alerted the committee to a potential drafting error in the bill. As the bill is currently drafted, it would permit the ABC and SBS to be provided with personal information during declared emergencies as they are 'national broadcasters' and not 'media organisations'.[17]

2.20 Ms Lyn Kemmis, Senior Legal Counsel, SBS, and Member, Australia's Right to Know (ARTK), queried why the national broadcasters could be provided with personal information during declared emergencies when commercial media outlets would not be privy to that information. Her understanding of the provision:

> …is about the provision of people's personal information in the case of an emergency, like a COVID outbreak. It is permitting government entities to

---

14 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

15 AGD, *Submission 31*, p. 4.

16 OAIC, Answer to spoken question on notice, 22 October 2024 (received 4 November 2024).

17 ABC, *Submission 38*, p. [1]; Special Broadcasting Service SBS, *Submission 40*, p. [1]; Mr Brett Farrell, Senior Privacy Officer and Privacy Champion, ABC; and Member, Australia's Right to Know (ARTK), *Committee Hansard*, 22 October 2024, p. 29; Ms Lyn Kemmis, Senior Legal Counsel, SBS; and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 29. Note: proposed paragraph 80KA(2)(b) of the bill would prevent media organisations from being provided with personal information during a declared emergency.

> quickly distribute information about individuals who might need to know their exposure. The media is not the way to do that.[18]

2.21 The AGD confirmed the national broadcasters were unintentionally excluded from the provisions of the bill. They should be treated in the same way as commercial broadcasters.[19]

2.22 The AGD explained the bill would 'enable emergency declarations to be more targeted'. Its provisions would require the kinds of personal information that would be shared during emergencies to 'be specified within the declaration, instead of allowing wide sharing of personal information in a declared emergency or disaster'. The amendment is intended to 'strike a better balance between protecting individuals' privacy, and enabling effective and coordinated responses to an emergency or disaster'.[20]

Children's Online Privacy Code

2.23 Most inquiry participants welcomed the development of a COP Code.[21]

2.24 ChildFund Australia emphasised 'the existing Privacy Act does not adequately address privacy and security challenges faced by children in the digital age'. It voiced concern 'about how children's personal data is collected, shared, and used by a range of actors, including technology companies'. There are potential life-long risks associated with inadequately protecting children's data.[22]

2.25 Those risks are associated with a wide range of potential online harms, many of which may not be immediately apparent. The Alannah and Madeline Foundation (AMF) suggested that the public conversation is focussed on the most visible risks associated with children's use of the digital environment. Personal information is collected by online platforms and monetised, often in

---

[18] Ms Lyn Kemmis, Senior Legal Counsel, SBS; and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 34.

[19] AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

[20] AGD, *Submission 31*, p. 4.

[21] See, for example: Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 5*, p. 1; Alcohol and Drug Foundation, *Submission 8*, p. 1; Children and Media Australia (CMA), *Submission 10*, p. 2; Australian Lawyers Alliance (ALA), *Submission 14*, p. 6; Queensland Council for Civil Liberties, *Submission 17*, p. 2; Law Council, *Submission 67*, p. 20; IAA, *Submission 29*, p. 2; Food for Health Alliance, *Submission 33*, p. 2; Dr Lisa Archbold et al, *Submission 34*, p. 6; Per Capita, Centre of the Public Square, *Submission 35*, p. 1; AHRC, *Submission 36*, p. [5]; Digital Industry Group Inc. (DIGI), *Submission 41*, p. 4; Tech Council of Australia, *Submission 49*, p. 1; DRW, *Submission 50*, p. [6]; HRLC, *Submission 60*, p. 7; Alannah and Madeline Foundation (AMF), *Submission 61*, p. 2; ChildFund Australia, *Submission 62*, p. [2]; UNICEF Australia (UNICEF), *Submission 63*, p. 4.

[22] ChildFund Australia, *Submission 61*, p. [2]–[3].

ways that adults let alone children struggle to understand. Depending on how it is developed, the COP Code 'would provide a strong foundation for change'.[23]

2.26 UNICEF Australia (UNICEF) referred to data as 'the currency of the online world, and children's data – where it's collected, traded and sold on mass scales – is considered big business'. It saw the proposal to develop the COP Code as an opportunity to:

> …ensure children's data is only collected and used in a way that serves their best interests and will provide them with the protections they are entitled to. It will hold tech companies accountable, ensuring they are transparent with how they use children's data, and that terms and conditions of apps are clear and straightforward.[24]

Scope of the Children's Online Privacy Code

2.27 UNICEF recommended that the COP Code apply 'to all online services likely to be accessed by children including educational technology providers, games and commercial health apps'.[25]

2.28 AMF agreed the COP Code should apply to a wide range of online services including 'apps, connected toys and devices, search engines, streaming services, online games and education products'. That approach would be consistent with the UK legislation upon which the COP Code is intended to be modelled.[26]

2.29 Reset.Tech Australia argued that the COP Code could be strengthened by expanding its application beyond 'social media, designated internet services and relevant electronic services'. For example, it suggested that it could be extended to 'EdTech and data brokers'. Learning from similar codes that have been developed in international jurisdictions could also improve the development of the Australian COP Code.[27]

2.30 Professor Elizabeth Handsley, President, Children and Media Australia (CMA), argued 'there is no justification' to exclude edtech from the COP Code. She alerted the committee to the situation in the United States where 'there has been a law firm set up…for the sole purpose of suing edtech companies for the way they treat children's data in that country'. In her view, 'the existence of a law firm solely dedicated to dealing with edtech's breaches of children's privacy tells

---

23 AMF, *Submission 61*, p. 2.

24 UNICEF, *Submission 63*, p. 3.

25 UNICEF, *Submission 63*, p. 3.

26 AMF, Answers to spoken questions on notice, 22 October 2024 (received 22 October 2024).

27 Reset.Tech Australia, *Submission 3*, p. 2.

you there is a major issue there that this legislation should really be addressing'.[28]

2.31 Additionally, children do not limit their online usage to child-specific platforms or services. For example:

> Instagram and TikTok are very popular among Australian teens and younger children, but more than 90% of Australian Instagram users and approx two-thirds of TikTok users are recorded as aged 18 and over. This could enable their providers to state, plausibly, that they do not provide 'children's services' and therefore are not in scope of a [COP Code].[29]

2.32 BCA indicated that determining the services that are 'likely to be accessed by children' would be difficult for 'business to assess'. Based on experience from the UK, organisations had 'found it difficult to operationalise' similar provisions.[30]

2.33 Meta outlined the services that are included in 'industry codes that have been and are being developed under the [*Online Safety Act 2021*]'. They include:

> …app stores, search engines, on-demand program services (e.g. some but not all streaming apps), third-party hosting services (cloud providers), ISPs and equipment makers and providers (for example, a company that makes phones or laptops).[31]

2.34 These services are regularly used by young people and should be included in the COP Code.[32]

2.35 The Food for Health Alliance argued that the term 'likely to be accessed by children' must be retained as the COP Code should apply 'to the services children use, not only those services designed for them'.[33]

2.36 Professor Handsley contended that '[i]f you're really serious about protecting children, you look at where they are, not at where people want them to be'. She explained:

> Children are curious and they do have a right to go online, find information and get experiences, and they need to be kept safe in all of those places. If we really are serious about keeping children safe, then we apply the legislation and regulations where the children are and we limit their

---

28 Professor Elizabeth Handsley, President, CMA, *Committee Hansard*, 22 October 2024, p. 6.

29 AMF, Answers to spoken questions on notice, 22 October 2024 (received 22 October 2024).

30 BCA, *Submission 56*, p. 9.

31 Meta, *Submission 57*, p. 3.

32 Meta, *Submission 57*, p. 3.

33 Food for Health Alliance, *Submission 33*, p. 2.

> exposure to the relevant risks, rather than cutting it down to be a matter of what the aim was in putting that information out.[34]

2.37 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church in Australia, Synod of Victoria and Tasmania, agreed that industry should not be left to regulate itself:

> Ideally in this space, you would want the regulator to almost be checking what kind of things children are accessing in reality. Just because a provider says, 'My content is targeted at adults', like it's an old game or whatever does not mean children are not accessing it. You'd almost want this checking to say, 'This is really a product that children are not accessing?', or in this case, 'Are they likely to be accessing?'.[35]

2.38 The Interactive Games and Entertainment Association (IGEA) and the Digital Industry Group Inc. (DIGI) suggested that international experiences of adopting similar children's privacy codes should be considered in the drafting of the COP Code.[36]

2.39 There should be alignment between the COP Code and international children's privacy codes. For example, the bill should be amended so that the COP Code applies to providers of social media services, relevant electronic services or designated internet services 'targeted at, or directed to, children'. Similar terminology is used in the US Children's Online Privacy Protection Act (COPPA).[37] The bill would provide greater clarity about which services are expected to adhere to the COP Code if it is aligned with the COPPA.[38]

2.40 Ms Jessie Mitchell, Advocacy Manager, AMF, stated the term 'likely to be accessed' is similar to the terminology used in the UK children's code:

> They say it's a digital environment where the probability of children accessing it is higher than the probability of them not accessing it, and they do provide some guidance to services as to how to make that assessment. I do agree it can be a challenging point for a service to assess, and that is a space where we'd want to see the regulator, the Office of the Australian Information Commissioner, being adequately resourced to provide that expert guidance.[39]

---

34 Professor Elizabeth Handsley, President, CMA, *Committee Hansard*, 22 October 2024, p. 5.

35 Dr Mark Zirnsak, Senior Social Justice Advocate, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 22 October 2024, p. 8.

36 Interactive Games and Entertainment Association, *Submission 18*, pp. 5–6; DIGI, *Submission 41*, p. 5.

37 Interactive Games and Entertainment Association, *Submission 18*, pp. 5–6.

38 IGEA, *Submission 18*, p. 6; DIGI, *Submission 41*, pp. 4–5.

39 Ms Jessie Mitchell, Advocacy Manager, Alannah and Madeline Foundation, *Committee Hansard*, 22 October 2024, p. 5.

2.41 The IAA cautioned against broadening the scope of the COP Code. It considered that the terms 'relevant electronic service' and 'designated internet service' are already 'extremely broad'.[40]

2.42 The OAIC indicated the range of online services likely to be accessed by children would include, 'but not [be] limited to, social media services, websites, apps, instant messaging services, and online gaming services'.

2.43 The COP Code would be required to 'set out how one or more of the APPs are to be applied or complied with in relation to children'. The code would be able to 'impose additional requirements provided those requirements are not inconsistent with the existing APPs. In this way, the requirements in the Code must be grounded in the APPS'. The COP Code could build upon the requirement for APP entities to have privacy policies and collection notices by:

> …set[ting] out how organisations should tailor privacy policies and collection notices for a child so that they are clear and easy to understand, for example, by using graphics, video and audio content, rather than relying solely on written communication.[41]

2.44 The COP Code would apply to APP entities 'that provide social media services, designated internet services or relevant electronic services that are likely to be accessed by children'. It would be developed as 'children merit special privacy protection as they may be less aware of the risks and consequences associated with the handling of their personal information, particularly online'.[42]

2.45 Regulated entities would be required 'to design their services in a manner that protects children from harm'. The government:

> …will consider additional proposals to increase privacy protections for children – including in relation to harmful targeting and trading in children's personal information, and requiring entities to have regard to the best interests of the child when handling their personal information.[43]

2.46 Ms Catherine Fitch, Assistant Secretary, Privacy Reform Taskforce, Integrity Frameworks Division, AGD, indicated the term 'likely to be accessed by children' was modelled on similar terminology used in the UK age-appropriate design code:

> The UK Information Commissioner's Office guidance outlines what is meant by 'likely to be accessed by children', and it provides some guidance that I think many organisations would be familiar with. In our bill currently the subject of this inquiry it also provides factors relevant to whether a service

---

40 Internet Association of Australia, *Submission 29*, p. 2.

41 OAIC, *Submission 23*, p. 3.

42 AGD, *Submission 31*, p. 4.

43 AGD, *Submission 31*, p. 4.

> is likely to be accessed by children, such as the nature and content of the service, whether it has a particular appeal and so on.[44]

Exclusion of health service providers

2.47 Ms Ariana Kurzeme, Director, Policy and Prevention, AMF agreed with the intent of the provision of the bill that would exclude health service providers from the COP Code. However, she stated her organisation is:

> …concerned about the proliferation of commercial platforms marketing health products and services of varying quality to children, including nominally free products, presumably based on handling personal data. We believe that protection should extend to all digital spaces where children's personal information is at risk of exploitation or misuse.[45]

2.48 The Law Council similarly queried why the bill would exempt health service providers from complying with the COP Code. As it is currently drafted, the exemption would:

> …exclude many APP entities that should be covered by the COP Code, given that 'health service' is broadly defined in section 6FB of the Privacy Act (and includes physical and psychological health). This exclusion is also much wider than entities providing 'preventative or counselling services', as was agreed to in the Government Response to Proposal 16.5, and would potentially exclude many digital providers whose tools are targeted at children.[46]

2.49 The Law Council was not certain that the blanket exemption for health service providers is necessary, given the bill would 'allow for the OAIC to specify within the COP Code itself which APP entities are, and are not, covered'. On that basis it recommended '[t]he breadth of the exclusion of health service providers…should be narrowed to exclude counselling services only, not health services more generally'.[47]

2.50 The OAIC clarified the COP Code would not apply to health service providers 'which ensures the code is not a barrier to providing essential services to children'. Health service providers would include entities 'such as online counselling and advice services, and telehealth'.[48]

2.51 The AGD similarly explained health service providers would be excluded 'to ensure the COP Code is not inadvertently a barrier to providing essential services to children, and allows more detail about the scope of the COP Code to

---

[44] Ms Catherine Fitch, Assistant Secretary, Privacy Reform Taskforce, Integrity Frameworks Division, AGD, *Committee Hansard*, 22 October 2024, p. 66.

[45] Ms Araina Kurzeme, Director, Policy and Prevention, AMF, Committee Hansard, 22 October 2024, p. 2.

[46] Law Council, Submission 67, pp. 20–21.

[47] Law Council, Submission 67, p. 21.

[48] OAIC, Submission 23, p. 3.

be determined through the code-making process', noting there is another provision in the bill that allows specified health service providers or types of health service providers to be bound by the COP Code.[49]

Consultation with stakeholders in the development of the Children's Online Privacy Code

2.52 The bill specifies that the Information Commissioner may consult with stakeholders when developing the COP Code. DIGI and Meta recommended the bill be amended to require the Information Commissioner to consult with stakeholders, including industry.[50]

2.53 DIGI agreed it is appropriate for the Information Commissioner to 'consult with children, children's welfare organisations, the eSafety Commissioner, and the National Children's Commissioner' when developing the COP Code. However, in addition to those stakeholders the bill should be amended to require the commissioner to 'consult with providers of Social Media Services, Relevant Electronic Services or Designated Internet Services'. That consultation would help to ensure the COP Code is 'fit for purpose and technically feasible'.[51]

2.54 Reset.Tech Australia welcomed the development of the COP Code by the OAIC seeing that office's involvement as 'critical to the initiative's success'.[52]

2.55 Based on survey data provided by Reset.Tech Australia, the Australian public overwhelmingly supports an independent regulator, such as the Information Commissioner, developing the COP Code (see Figure 2.1).[53]

---

49 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024). Also see: Explanatory Memorandum, pp. 87–88.

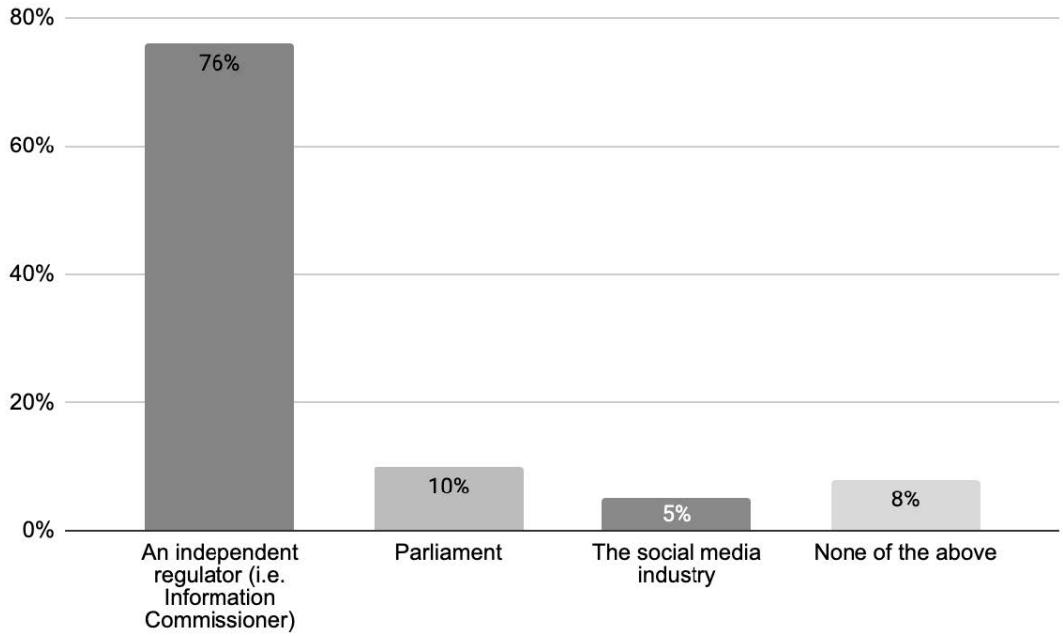
50 DIGI, *Submission 41*, p. 5; Meta, *Submission 57*, p. 13;

51 DIGI, *Submission 41*, pp. 5–6.

52 Reset.Tech Australia, *Submission 3*, p. 2.

53 Reset.Tech Australia, *Submission 3*, p. 5.

Figure 2.1 People's preference about who should write the codes for privacy safety for children (n=1508)



Source: Reset.Tech Australia, Submission 3, p. 5.

Note: Respondents were asked: If you had to choose, who would you most prefer to write the codes about online privacy for children?

2.56 Miss Alice Dawkins, Executive Director, Reset.Tech Australia, elaborated on this evidence by providing a case study demonstrating the potential shortcomings of having industry draft its own codes. In that case, 'where industry attempted to insert safety standards for young Australians, particularly privacy defaults…we saw some unacceptably low standards of protection'. She maintained that industry should not be permitted to draft the COP Code and 'it's excellent news that the commissioner is being empowered to do this'.[54]

2.57 UNICEF reflected on the importance of including children in the design of the COP Code and suggested they must be consulted in its design:

> Every child and young person under 18 has the right to participate and have their opinions included in decision-making processes that relate to their lives…Including the voices of children and young people in the development of policy isn't just the right thing to do, it's the smart thing to do – policies co-designed with children and young people are better placed to respond to their needs and deliver better outcomes.[55]

[54] Miss Alice Dawkins, Executive Director, Reset.Tech Australia, *Committee Hansard*, 22 October 2024, p. 24.

[55] UNICEF, *Submission 63*, p. 5.

2.58 As it can be difficult for children to understand privacy matters, AMF suggested the consultation period be extended from 40 days to a minimum of 60 days. A longer consultation period would allow for meaningful consultation with children about their privacy.[56]

2.59 The IGEA also argued the bill be amended to require the Information Commissioner to consult with industry on the development of the COP Code, rather than consult with them at their own discretion.[57]

2.60 To address its concerns, the IGEA recommended:

- As the Government has committed to developing the COP Code, the Code should be referring to services that are 'targeted at, or directed to, children', which is less ambiguous than the term 'likely to be accessed by children'.
- Should the OAIC be assigned with the responsibility for developing and consulting on the COP Code, the Bill should explicitly require the OAIC to meaningfully consult with relevant industry stakeholders who are directly impacted by the COP Code. Consultation should at least occur during the development and public consultation stages of the Code.[58]

2.61 According to the Australian Human Rights Commission (AHRC), the COP Code would 'significantly strengthen privacy protections for children and young people'. To ensure that the views of children and young people are taken into account during the drafting of the code, the AHRC recommended the bill be amended to specify the Information Commissioner must consult with children and other stakeholders.[59]

2.62 In developing the COP Code, the OAIC:

> …intend[s] to adopt a transparent and collaborative approach…and will consult widely with children, parents, child development experts, child welfare advocates, civil society, other regulators and across the online industry to ensure different voices are heard and represented throughout the process.[60]

---

56 AMF, *Submission 61*, p. 3.

57 IGEA, *Submission 18*, pp. 7–8.

58 IGEA, *Submission 18*, pp. 10.

59 Australian Human Rights Commission (AHRC), *Submission 36*, pp. [5]–[6]. Note: proposed subsection 26GC(8) of the bill stated the Information Commissioner 'may' consult children and other stakeholders while developing the COP Code. The AHRC recommended amending the proposed subsection to 'must'.

60 OAIC, *Submission 23*, p. 3.

Definition of a child

2.63 Some inquiry participants questioned the bill's definition of a child as an individual under the age of 18.[61]

2.64 BCA suggested the definition should be consistent with other legislation such as 'the age of criminal responsibility, minimum working age (which varies by State jurisdiction), and proposed definitions for social media platforms (and associated policies)'.[62]

2.65 Privacy 108 similarly discussed 'the ongoing debate around restricting children's access to social media and other digital platforms until they reach a certain age, likely between 14 and 16 years'. In its view, there should be a consistent definition in the Privacy Act and any other legislation that regulates children's use of technology.[63]

2.66 DIGI suggested a challenge associated with the COPPA is that it 'only applies to young people under the age of 13, where it is much easier to distinguish between material targeted to a child of that age vs an adult'. If the COP Code applies to anyone under the age of 18 'there will be challenges distinguishing between children under 18 and young adults'. The UK has provided guidance to regulated entities on this matter to assist them in determining if their service is likely to appeal to children.[64]

2.67 The Uniting Church in Australia, Synod of Victoria and Tasmania observed the internationally accepted definition of a child is someone under the age of 18. On that basis, it agreed with the definition included in the bill.[65]

2.68 It was suggested age restrictions may not be the most effective way of ensuring that online platforms protect children's data. For example:

> …if a platform can claim that children are not supposed to use their service due to age restrictions, it may avoid the additional legal obligations that would otherwise apply to protect children's data. This loophole allows companies to argue they are not "knowingly" collecting data from children, even though children may still access their platforms.[66]

2.69 That loophole is evident in other jurisdictions, including the United States, 'where some platforms avoid compliance by stating their service is not intended for children under 13'. To avoid this loophole, online platforms should be

---

61 Note: the bill would define a child as 'an individual who has not reached 18 years', see: Item 30 in Part 4 of Schedule 1 of the bill; proposed subsection 6(1) of the bill.

62 BCA, *Submission 56*, p. 10.

63 Privacy 108, *Submission 1*, p. 3.

64 DIGI, *Submission 41*, p. 5.

65 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 5*, p. 1;

66 Mx Trapani, *Submission 7*, p. [3].

required to 'adopt tailored privacy policies, and heightened security measures to ensure the privacy of children is genuinely protected'.[67]

2.70 AMF argued the international definition must be retained in the bill. That would align:

> …it with both the *Online Safety Act 2021* and the UN Convention on the Rights of the Child. This is crucial, as we've seen efforts by the tech industry to limit protections to younger age groups, for example, the first round of the industry codes under the Online Safety Act. We see these reforms as a once-in-a-generation opportunity to reduce the risk to children in digital environments, protect them from exploitation of their personal information and other intrusive practices, and uphold their rights.[68]

2.71 Ms Mitchell suggested that in instances where the definition of a child has been set at an age lower than 18 there have been 'lower default protections for children'. She cited the example of industry safety codes:

> These codes were drafted by industry and they introduced a definition of what they called a young Australian child, meaning a child under 16, and it was only for that category that social media services were put into the new code to introduce high privacy settings by default. That's a lower threshold of protection than a number of other countries have. We think that children up to 18 should have a right to these inbuilt protections for their personal information, because of the flow-on effects that has for their experience and safety.[69]

2.72 The Law Council cautioned that defining a child as an individual under the age of 18 years 'may lead to unintended consequences'. The insertion of that definition would make it applicable to all matters in the Privacy Act, which would 'erode many of the existing privacy-enhancing practices that respect the agency of young people under 18 years'.[70]

2.73 Additionally, the definition of 'child' proposed in the bill could introduce inconsistencies in relation to a child's capacity to consent in relation to their health and privacy.[71]

2.74 According to the Law Council, 'the generally accepted position regarding a child's capacity to consent' is as follows:

> …the Government agrees in-principle that the Privacy Act should codify the principle that valid consent must be given with capacity…The guidance provides sufficient flexibility by allowing entities to decide if an individual under the age of 18 has capacity to consent on a case-by-case basis. If that is

---

67 Mx Trapani, *Submission 7*, p. [3].

68 Ms Kurzeme, AMF, *Committee Hansard*, 22 October 2024, p. 2.

69 Ms Mitchell, AMF, *Committee Hansard*, 22 October 2024, p. 7.

70 Law Council, *Submission 67*, pp. 21–22.

71 Law Council, *Submission 67*, p. 22.

> not practical, as a general rule, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.[72]

2.75 To avoid those potential unintended consequences, the Law Council recommended 'the proposed definition of 'child' should be limited to the use of that term in the COP Code only'.[73]

2.76 The AGD responded directly to the concern raised by the Law Council, stating:

> The proposed definition of 'child' in the Bill will apply across the Privacy Act unless the contrary intention appears. The Law Council refers to the importance of respecting the agency of young people under 18 years and the issue of capacity to consent. Currently, the approach to capacity to consent under the Privacy Act is set out in [OAIC] guidance rather than in the legislation and specifies that an individual must have capacity to give consent. Proposal 16.2, which was agreed in principle in the Government Response to the Privacy Act Review Report would codify in the Act the principle that valid consent must be given with capacity. The proposed definition of child would not be determinative of capacity to consent where required under the Privacy Act.[74]

Overseas data flows

2.77 Submitters broadly agreed with the provisions that would simplify the regulation of overseas data flows.[75]

2.78 BSA | The Software Alliance (BSA) reminded the committee that overseas data transfers are already permitted under the Privacy Act. By prescribing countries that have 'substantially similar' privacy protections to Australia, the amendment would 'provide businesses with greater legal certainty and substantially reduce compliance burdens'.[76]

2.79 It was not clear to BSA 'what would constitute a "substantially similar" level of protection'. It was concerned a strict interpretation that would require foreign privacy laws 'to mirror, point-by-point, the APPs, would defeat the purpose of the mechanism'. To avoid that situation, BSA suggested that further consultation be undertaken 'on the process for, and factors involved in,

---

72 Law Council, *Submission 67*, p. 22. Also see: Attorney-General's Department, *Government Response: Privacy Act Review Report*, 28 September 2023, p. 13.

73 Law Council, *Submission 67*, p. 22.

74 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

75 See, for example: Privacy 108, *Submission 1*, p. 3; BSA | The Software Alliance (BSA), *Submission 6*, p. 2; Global Data Alliance, *Submission 9*, pp. 1–2; IGEA, *Submission 18*, p. 11; Australian Banking Association (ABA), *Submission 30*, p. 2; Association of Superannuation Funds of Australia (ASFA), *Submission 45*, p. 9; Access Now, *Submission 55*, p. 6; Law Council, *Submission 67*, p. 23;

76 BSA, *Submission 6*, p. 4. Also see: Global Data Alliance, *Submission 9*, p. 2.

determining whether a country or certification scheme offers the appropriate level of protection'.[77]

2.80 BSA and the Global Data Alliance suggested two certification schemes that Australia could consider prescribing for this purpose. Those schemes are:

- The Cross Border Privacy Rules; and
- International Standards Organization 27701.[78]

2.81 Some foreign privacy laws, including the *General Data Protection Regulation* (EU) 2016/679 (GDPR), have mechanisms that simplify the flow of data between countries. The Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University (Jeff Bleich Centre), considered the limited reforms contained in the bill could mean 'Australian privacy law may not meet the privacy standards of other countries and jurisdictions'. That limitation would 'represent a problem for data controllers or processors attempting to transfer data to Australia'. For example, it could 'act as an impediment for scientific research between Australia and European Union countries'.[79]

2.82 The Law Council submitted 'the Bill does not expressly harmonise with existing cross-border mechanisms widely used by many APP entities to address the requirements of the EU GDPR and APP 8'. For that reason:

> …the Bill should amend APP 8.2(a)—and the Privacy Regulation should also be amended—so as to expressly reference some of the mechanisms that are widely used by APP entities to address Article 46 of the EU GDPR ('transfers subject to appropriate safeguards'). Reference should particularly be made to safeguards, such Standard Contractual Clauses, adopted by the European Commission in accordance with the examination procedure referred in Article 92(2) of the EU GDPR.[80]

2.83 By expressly referring to those mechanisms, the bill would better 'avoid the unintended consequences of potentially conflicting measures being described, or adopted, by APP entities, especially if some countries may be added, or subsequently removed, by the regulations'.[81]

2.84 The AGD advised:

> APP 8.1 requires entities to take such steps as are reasonable to ensure that an overseas recipient of personal information does not breach the APPs in relation to the information. APP 8.2 provides that APP 8.1 does not apply where certain circumstances are established. One such circumstance is

---

77 BSA, *Submission 6*, p. 4. Also see: Global Data Alliance, *Submission 9*, p. 2.

78 BSA, *Submission 6*, p. 4; Global Data Alliance, *Submission 9*, p.

79 Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University (Jeff Bleich Centre), *Submission 19*, p. 5.

80 Law Council, *Submission 67*, p. 25.

81 Law Council, *Submission 67*, p. 25.

> where the entity reasonably believes that the recipient of the information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the APPs protect the information and there are mechanisms that the individual can access to take action to enforce the protection of the law or binding scheme (APP 8.2(a)). Schedule 1, subclause 37 introduces a mechanism to enable countries and certification schemes to be prescribed as providing substantially similar protection to the APPs under APP 8.2(a). Entities may still make their own assessment about whether countries or schemes that are not prescribed meet this test for the purposes of APP 8.2(a). The Government has also agreed in principle to progress Proposal 23.3 of the Privacy Act Review to make standard contractual clauses available to APP entities for transferring personal information overseas.[82]

2.85 The AGD submitted the intention of the amendment is to 'provide greater certainty to disclosing entities about the standard of privacy protections in prescribed countries enhancing the flow of information across national borders while ensuring privacy is respected'. Future reforms will consider how overseas data flows can be further enhanced.[83]

Penalties for interference with privacy

2.86 Submitters broadly agreed with the proposed amendments that would introduce tiered civil penalties for breaches of privacy.[84]

2.87 CHOICE argued a tiered approach would 'better protect people from breaches of privacy that do not fulfil the criteria for a "serious" interference, but which are nevertheless harmful and should be deterred'. It suggested the penalty provisions could be improved by:

> …allowing the courts to determine the penalty based on the value of the benefit resulting from the interference, or as a percentage of turnover. This would ensure that large businesses take the provision seriously.[85]

2.88 The IAA recommended the penalty provisions be accompanied by a 12-month education and awareness raising program to give industry and other stakeholders time to understand the compliance and enforcement approach.[86]

---

82 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

83 AGD, *Submission 31*, p. 5.

84 See, for example: Privacy 108, *Submission 1*, p. 4; Office of the Information Commissioner (Qld), *Submission 15*, p. 3; Queensland Council for Civil Liberties, *Submission 17*, p. 2; CHOICE, *Submission 21*, p. [2]; OAIC, *Submission 23*, p. 1; Tech Council of Australia, *Submission 49*, p. 4.

85 CHOICE, *Submission 21*, p. [2].

86 IAA, *Submission 29*, p. 3. Note: a similar approach was taken by the Department of Home Affairs and the Australian Signals Directorate in relation to the reform of the critical infrastructure framework.

2.89 Clubs Australia agreed that education and remediation should be applied to minor infractions or unintentional breaches of privacy. That approach 'would foster a culture of compliance and continuous improvement' and ensure that smaller organisations are not burdened with large fines.[87]

2.90 The Law Council submitted that the penalty provisions 'are broadly consistent with Proposals 25.1 and 25.2 of the Privacy Act Review Report, to which the Government agreed in its Response'.[88]

2.91 The Law Council generally supported the penalties for interference with privacy contained in the bill. It suggested that those penalties:

> …may not be appropriate if the Privacy Act is eventually extended to smaller organisations, noting that the Government agreed, in principle, to the removal of the small business exemption in its Response to the Privacy Act Review Report.[89]

2.92 The Law Council's main concern with the penalty provisions related to their clarity and proportionality to the offence. It queried whether the 'principles-based obligations [included in the bill]…are sufficiently prescriptive to enable certainty in compliance by entities'. The Law Council explained the civil penalties would apply to entities that have been found to have breached one or more of the APPs. Many of those APPs require entities to take ''reasonable' (as opposed to absolute) steps to address compliance. These are typically not prescriptive or binary matters that lend themselves to a simple determination of liability'.[90]

2.93 The provisions of the bill would allow the Information Commissioner to issue infringement notices without explaining how entities could better comply with their obligations under the Privacy Act. The Law Council suggested that 'may disincentivise—rather than promote—open and consultative communications with the OAIC'. The Law Council recommended the bill be amended so that the OAIC would be required to provide the entity with a 'notice that clearly outlines what is required to remedy the issue' before issuing an infringement notice.[91]

2.94 According to the AGD, the infringement notice power would be 'limited to specified provisions' and was designed in accordance with the AGD's *Guide to Framing Commonwealth Offences*. That guide:

> …states that an infringement notice scheme is appropriate for 'relatively minor offences, where a high volume of contraventions is expected, and

---

87 Clubs Australia, *Submission 37*, p. 4.

88 Law Council, *Submission 67*, p. 25.

89 Law Council, *Submission 67*, p. 26.

90 Law Council, *Submission 67*, p. 26.

91 Law Council, *Submission 67*, p. 28.

> where a penalty must be imposed immediately to be effective' and 'an enforcement officer can easily make an assessment of guilt or innocence'. The specified provisions were selected to align with this guidance. The provisions selected are similarly proscriptive to provisions subject to infringement notice powers of other regulators including the ACCC, ASIC and ACMA.[92]

2.95 By issuing infringement notices in the first instance, the Information Commissioner would be able 'to issue infringement notices in relation to alleged minor contraventions of the Act. This would allow the Commissioner to ensure compliance with privacy obligations without the need for protracted litigation'.[93]

2.96 The OAIC welcomed the proposed introduction of a new civil penalties regime for interference with privacy and saw it as a means to enhance the enforcement powers available to it:

> The enhanced civil penalty framework would provide more enforcement options to deter non-compliance and fill a gap where previously the Commissioner was only able to seek civil penalties for serious and repeated interferences with privacy, while the new infringement notice regime for administrative breaches of the Act would be a quick and cost-effective way for the OAIC to respond to non-compliant behaviour without the need for court proceedings.[94]

2.97 The AGD similarly explained that the tiered penalties regime would:

> …provide more enforcement options to the Information Commissioner to deter non-compliance and address a gap in the enforcement of privacy protections which allowed the Information Commissioner to seek civil penalties only for the most serious or egregious interferences with privacy. Lesser penalties and an infringement notice scheme for breaches of the Act that are less serious will allow the Information Commissioner to resolve matters more efficiently an proportionately.[95]

Automated decision making and privacy policies

2.98 The Tech Council of Australia raised concerns about the lack of clarity in the drafting of APPs 1.7-1.9. It suggested they will require 'substantial refinement for entities to interpret and apply consistently across the economy'. It may be appropriate to introduce the control/processor distinction to provide the necessary clarity.[96]

---

92 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

93 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

94 OAIC, *Submission 23*, p. 1.

95 AGD, *Submission 31*, p. 5.

96 Tech Council of Australia, *Submission 49*, p. 3.

2.99 It argued the ADM provisions should 'be carefully reconsidered'. As they are currently drafted, they are:

> …likely to inadvertently capture ADM activities that contribute positively to a safe and functioning internet, which includes automated decision-making systems to manage spam, scam, ADM systems that support vital cyber threat detection and security measures to combat hacking and fraud, as well as systems that assist in the moderation of harmful online content.[97]

2.100 The BCA similarly warned increased transparency 'about ADM processes could result in security risks'. For example, detailing how 'ADM processes are used to detect fraud…would tip off fraudsters and help them avoid detection'.[98]

2.101 The disclosure of information about ADM processes could also have implications for the protection of intellectual property and commercially sensitive information. A requirement to disclose that information could 'discourage or undermine business innovation'. The GDPR provides an exemption for 'trade secrets or intellectual property which, if disclosed, will adversely affect the rights or freedoms of others'.[99]

2.102 The Australian Chamber of Commerce and Industry (ACCI) agreed '[i]t will be important that information required to be disclosed by these [APP] entities is not commercially sensitive'.[100]

2.103 The Law Council argued there is insufficient clarity around some of the terms used in the provisions related to automated decision making:

> For instance, we are concerned that the Bill fails to provide certainty as to the meaning of 'automated decisions' and imposes an unnecessarily high bar with the proposed requirement for the computer program to 'make, or do a thing that is substantially and directly related to making, a decision'.[101]

2.104 The Law Council provided the following terminology related to automated decision making in the GDPR:

> …decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[102]

---

97 Tech Council of Australia, *Submission 49*, p. 4.

98 Business Council of Australia, *Submission 56*, p. 6.

99 Business Council of Australia, *Submission 56*, p. 7.

100 Australian Chamber of Commerce and Industry, *Submission 65*, p. 2.

101 Law Council, *Submission 67*, p. 29.

102 Law Council, *Submission 67*, p. 29. Also see: European Union, *General Data Protection Regulation* (EU) 2016/679, Article 22(1).

2.105 The EM provides the following meaning of 'computer program':

> The term 'computer program in APP 1.7(a) is intended to take its ordinary meaning and encompass a broad range of matters, including pre-programmed rule-based processes, artificial intelligence and machine learning processes to make a computer execute a task.[103]

2.106 These different definitions related to automated decision making may introduce limitations to the harmonisation and interoperability of the Privacy Act and the GDPR. In the Law Council's view:

> Alignment to existing frameworks is required to address the need for consistent practices and harmonisation with existing regimes that already regulate this field of activity and type of technology. This need for clarity is further reinforced by the fact that non-compliant disclosures will be the subject of new civil penalty provisions under the Bill.[104]

2.107 To ensure that the Privacy Act better aligns with existing legal regimes in foreign jurisdictions, the Law Council recommended:

> The terminology in Part 15 of Schedule 1 to the Bill should be aligned with Article 22 of the EU GDPR, which regulates 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her'.[105]

2.108 The Law Council also suggested that the bill appears to have been drafted with the understanding that automated decisions are made in relation to a single decision. It argued that, in some circumstances, ADM processes:

> …may be the result of several decisions that follow a series of 'decision trees'—some of which may include the use of computer programs in deciding what branch of the decision tree is taken next. This may be a complex process, potentially involving sensitive commercial-in-confidence information, that is not appropriate for disclosure in that entity's privacy policy.[106]

2.109 The Law Council was not certain about whether the bill was 'drafted to capture these circumstances'. To provide further clarity, the Law Council recommended the bill be amended to explain how entities are expected to comply with their new obligations 'in circumstances where a series of decisions are made, some of which may include the use of computer programs and commercial-in-confidence information'.[107]

---

103 Law Council, *Submission 67*, p. 29. Also see: EM, p. 77.

104 Law Council, *Submission 67*, p. 29.

105 Law Council, *Submission 67*, p. 30.

106 Law Council, *Submission 67*, p. 30.

107 Law Council, *Submission 67*, pp. 30–31.

2.110 If the bill is passed, it is possible that an entity required to disclose how personal information will be used in automated decision making processes will include generic statements in their privacy policy. Such a statement would fulfill the new obligation but may not provide any 'substantive information to meet the commendable objective of providing meaningful information to individuals'.[108]

2.111 The Law Council recommended the bill:

> …be amended to include a list of factors that must be considered by APP entities, prior to determining whether an automated decision may reasonably be expected to affect the rights or interests of an individual.[109]

2.112 To help individuals better understand how their personal data may be used in ADM processes, the Law Council recommended the bill 'be amended to provide for a right for individuals to request meaningful information about how substantially automated decisions with 'legal or similarly significant effect' are made'.[110]

2.113 The AHRC accepted the bill would generally improve transparency of ADM processes. However, that transparency 'may be limited due to the inaccessible nature of privacy policies, with people either not reading them or struggling to understand them'.[111]

2.114 The AGD explained the provisions related to ADM are intended to increase:

> …transparency about substantially automated decisions which significantly affect individuals' rights or interests. Entities will be required to include information in their privacy policy about the kinds of decisions and kinds of personal information used in these decisions. The use of the language 'rights or interests' is intended to have broad coverage. Rights do not have the same application in Australian law as in Europe which has more developed rights-based frameworks. Interests may include things that are not rights under the Australian law – for example the provision of benefits under an Act or denial of significant services or support.[112]

2.115 ADM has the potential to provide 'significant opportunities for enhancing productivity and facilitating economic growth, and improving outcomes for Australians across the areas of health, environment, defence and national security'. However, there are possible privacy risks associated with those potential benefits:

> …ADM systems may pose privacy risks as they can use personal information about individuals to assist or replace the judgement of human

---

108 Law Council, *Submission 67*, p. 31.

109 Law Council, *Submission 67*, p. 31.

110 Law Council, *Submission 67*, p. 32.

111 AHRC, *Submission 36*, p. [5].

112 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

> decision makers in ways which may have significant impact, with little transparency. Providing individuals with greater transparency on ADM allows them to understand how an entity handles their personal information and for what purposes, and allows them to take further action if there has been a breach of their personal privacy.[113]

2.116 If the bill passes, entities would be required:

> …to include information in privacy policies about the kinds of personal information used in, and types of decisions made by, computer programs that use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual.[114]

2.117 According to guidance materials provided by the OAIC, 'a privacy policy is general in nature, and focuses on the entity's information handling practices'. Privacy policies are 'not expected to involve any commercial-in-confidence information'.[115]

Information about the use of personal data

2.118 Some inquiry participants suggested that the bill take a stronger approach by providing individuals with information about how their personal data has been used in ADM.[116]

2.119 For example, the Jeff Bleich Centre agreed the bill would 'bring openness and transparency to the processing and use of personal information…[it] fails to bring Australian privacy law in line with other jurisdictions'.[117]

2.120 In the European Union, the GDPR:

- 'requires a data controller to inform a data subject whether their personal data will be processed as part of automated decision making';
- 'requires meaningful information about the logic used in processing'; and
- 'allows a person to opt out of automated decision making if it would produce legal effects that significantly affect this person'.[118]

---

113 AGD, *Submission 31*, p. 6.

114 AGD, *Submission 31*, p. 6.

115 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

116 See, for example: Mx Rebecca Trapani, *Submission 7*, p. [3]; Queensland Council for Civil Liberties, *Submission 17*, p. 2; Jeff Bleich Centre, *Submission 19*, p. 5; Law Council, *Submission 67*, pp. 28–29; Arca, *Submission 32*, p. [2]; Dr Lisa Archbold et al, *Submission 34*, p. 7; Per Capita, Centre of the Public Square, *Submission 35*, p. 1; Access Now, *Submission 55*, p. 5; HRLC, *Submission 60*, p. 11; Association for Data-driven Marketing and Advertising, *Submission 68*, p. [1].

117 Jeff Bleich Centre, *Submission 19*, p. 5.

118 Jeff Bleich Centre, *Submission 19*, pp. 5–6.

2.121 The Jeff Bleich Centre recommended the bill be amended 'to reflect emerging regulatory practices and the need for openness and transparency in data processing'.[119]

2.122 Privacy policies do not limit the collection and use of personal information or generally inform consumers about how that information is collected and used.

2.123 Those policies are generally very lengthy, and it would take the average person 14 hours to read the privacy policies of all the sites and applications they use in a single day.[120] CHOICE argued:

> Rather than adding to the length of privacy policies nobody reads, a far more effective reform would be to introduce the fair and reasonable use test recommended by the Review. This would require that businesses limit their collection, use and disclosure of personal information (including in automated decision-making) to purposes in line with a reasonable person's expectations.[121]

2.124 The BCA agreed the provisions could increase 'information overload in a way that is less, not more, understandable to our customers'.[122]

2.125 The bill would also place a large burden on businesses as it would require them 'to review all decision-making processes in their business or organisation that rely on personal information'. They would then need:

> …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.[123]

2.126 Businesses would then need to update their privacy policies after the implementation of new ADM processes. In the process of doing that, businesses would be required to assess whether that new ADM process makes, or does 'a thing that is substantially and directly related to making, a decision'. In the BCA's understanding of the bill, that would include everything 'from basic use of spreadsheet formulas to complex AI systems'. In global privacy laws, similar requirements 'are typically limited to decisions that are 'solely' based on automated processing or are made without any meaningful human involvement'. For example, if an ADM process is used to provide a human decision-maker with data to make a decision, 'this could constitute an

---

119 Jeff Bleich Centre, *Submission 19*, p. 6.

120 Consumer Policy Research Centre (CPRC), *Submission 20*, p. 1.

121 CHOICE, *Submission 21*, p. [4].

122 BCA, *Submission 56*, p. 5.

123 BCA, *Submission 56*, p. 5.

'automated decision' under the Australian law but would not elsewhere in the world'.[124]

2.127 While the bill would increase transparency around the use of automated decision making in line with some of the recommendations of the Privacy Act Review, it would not incorporate Proposal 19 in its entirety. The bill does not include an associated accountability mechanism, which means that it 'do[es] not live up to the spirit of Proposal 19 as a whole'.[125]

2.128 Consumers should also have the 'right to request meaningful information about how substantially automated decisions with legal or similarly significant effects are made'. The introduction of that right would fulfil one of the recommendations made in the Review and complement new APP guidance on automated decisions. Without this right in the bill 'consumers [would be] aware that automated decision-making was used by a service, but without any idea how or to what effect'.[126]

2.129 CHOICE argued the right for consumers to be able to know how their data is being used:

> …is a baseline expectation…[B]usinesses should just say how they are using the data across the board. That's really the bare minimum. We think that businesses should be obliged to use it in a fair and safe way, and not just let consumers know how they are using it.[127]

2.130 Amending the bill to incorporate similar language to that used in the GDPR would assist in better incorporating Proposal 19:

> …the GDPR requires 'data controllers' to provide 'meaningful information about the logic involved in the decision-making, as well as the significance and the envisaged consequences of such processing for the data subject'.[128]

2.131 An amendment to APP 5 to require entities to specify the use of ADM, and include 'meaningful information about the personal information and logic used' would similarly satisfy the spirit of Proposal 19.[129]

2.132 The Insurance Council of Australia indicated the bill would 'apply to decisions that may affect an individual's interests as well as their rights'. That differs from the proposal put forward in the Privacy Act Review Report which only

---

124 BCA, *Submission 56*, p. 5.

125 Dr Lisa Archbold et al, *Submission 34*, pp. 7–8.

126 CHOICE, *Submission 21*, p. [4].

127 Mr Rafi Alam, Senior Campaigns and Policy Advisor, CHOICE, *Committee Hansard*, 22 October 2024, p. 49.

128 Dr Lisa Archbold et al, *Submission 34*, p. 8. Also see: *General Data Protection Regulation 2016/679* (EU), para. 13(2)(f).

129 Dr Lisa Archbold et al, *Submission 34*, p. 8.

mentioned individual's rights. The ICA argued that by including interests the bill would broaden:

> …the scenarios and use cases where organisations may have to disclose the use of ADMs. And given the penalties for non-compliance, this could perversely incentivise organisations to over-disclose information, leading to cognitive overload for customers.[130]

2.133 The ABA echoed that view:

> The focus on 'interests of an individual' is not a position that was previously contemplated, it introduces unnecessary ambiguity and broadens the application of the APP without any likely consumer benefit. Contrary to the intention of the reforms, inundating consumers with excessive and unnecessary disclosures could lead to general customer confusion.[131]

2.134 In its view, privacy policies should be required to outline the use of 'substantially automated decisions that have a legal or similarly significant effect on an individual's rights'.[132]

2.135 The Financial Advice Association of Australia recognised 'consumer rights, whilst vital in empowering individuals, cannot be a replacement for concerted and collective action by Government targeted at the misuse of information in this space'.[133]

2.136 For example, BSA argued that consumers should be able 'to know how their personal data is used and protected'. That right 'should be backstopped by strong legal obligations on companies that collect or process personal information'.[134]

2.137 The Human Technology Institute, University of Technology Sydney (HTI) submitted that while the requirement to include information about ADM in privacy policies 'would improve transparency regarding when automation is used in decision making, it is unlikely to have a significant practical impact'. The provision of additional information in a privacy policy that an individual would need to consent to prior to accessing a product or service would do little to support them in 'seeking a review of an adverse decision'.[135]

---

130 Insurance Council of Australia, *Submission 28*, p. 2.

131 ABA, *Submission 30*, p. 1.

132 Insurance Council of Australia, *Submission 28*, p. 2.

133 Financial Advice Association of Australia, *Submission 25*, p. 3.

134 BSA, *Submission 6*, p. 5.

135 Human Technology Institute, University of Technology Sydney (HTI), *Submission 13*, p. [13].

2.138 The HTI recommended:

> …the Bill should be amended to include a provision that would provide individuals with the right to request meaningful information about how substantially automated decisions with legal or similarly significant effects are made – as recommended by the Privacy Act Review report.[136]

2.139 Privacy 108 took a similar view, arguing that 'individuals must have stronger rights beyond transparency when AI is used', including:

- The right to human intervention in AI-driven decision-making processes;
- The right to refer AI uses to a specialist regulator for review based on fairness and the protection of broader human rights, particularly regarding their impact on individuals.[137]

2.140 Arca warned that the bill does not provide guidance on 'how specific the disclosures about automated decision making need to be'. A lack of guidance could result in entities 'making their disclosures as complete as possible'. In some instances, that would lead to very lengthy disclosures that are unlikely to be read by consumers. In other cases, some APP entities may disclose less information than others. Divergent approaches are likely to 'increase consumer confusion and uncertainty'.[138]

2.141 To overcome the limited guidance, Arca recommended either the:

- addition of a new subclause to explain 'that subclauses 1.7 and 1.8 do not require APP entities to set out every single piece of information used by a computer program, or the effect the information has on the decision'; or
- EM be amended to provide more guidance, specifically that APP 1.8 does not require 'very granular detail'.[139]

2.142 Ms Louise McGrath, Head of Industry Development and Policy, Australian Industry Group (Ai Group), suggested it would be difficult for businesses to comply with the proposed ADM provisions:

> Due to the generally commercial or proprietary nature of automated decision-making or other artificial intelligence tools, it will also be extremely difficult for most employers to be open and transparent in an APP privacy policy. A better approach would be to support our members in their adoption of these tools, including with reference to the 10 voluntary guardrails recently introduced by the government to support safe and responsible AI use.[140]

---

136 HTI, *Submission 13*, p. [14].

137 Privacy 108, *Submission 1*, pp. 7–8.

138 Arca, *Submission 32*, p. [2].

139 Arca, *Submission 32*, pp. [2]–[3].

140 Ms Louise McGrath, Head of Industry Development and Policy, Australian Industry Group (Ai Group), *Committee Hansard*, 22 October 2024, p. 37.

2.143 According to the AGD, future privacy reforms are expected to focus on:

> …measures to increase the transparency of ADM – including by providing individuals a right to request meaningful information about automated decisions that have a significant effect on an individual's rights or interests. This proposal will be further considered as part of a second package of privacy reform measures, and in the context of the [sic] developing a consistent legislative framework for the use of ADM in the delivery of government services to ensure consistency in approaches.[141]

2.144 Ms Virginia Jay, Director, Privacy Reform Taskforce, AGD, explained:

> The Privacy Act report proposed that privacy policies should set out the types of personal information that would be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights. That wording was drawn from similar wording used in the European Union's GDPR. The bill has applied that transparency requirement to decisions which could be reasonably expected to affect the rights or interests of an individual. The application of that transparency requirement to decisions with significant effect on an individual's interests, in addition to rights, was in recognition that rights do not have the same application in Australian law as in Europe, which has a more developed rights based framework. In Australian law, the concept of interests covered the types of similarly significant effects it was anticipated that the new requirement should cover—that is, the provision of benefits under an act or the denial of significant services or support.[142]

Use of artificial intelligence in automated decision making

2.145 Several submitters referred to the consultation underway by the Department of Industry, Science and Resources (DISR) on introducing mandatory guardrails for high-risk uses of AI.[143]

2.146 Some of those submitters suggested the ADM provisions in the bill be implemented after the other regulatory reforms related to AI and ADM are completed. Implementing the provisions prior to that could increase complexity, introduce conflicting requirements, add to compliance burdens, and lead to uncertainty.[144]

---

141 AGD, *Submission 31*, p. 6.

142 Ms Virginia Jay, Director, Privacy Reform Taskforce, AGD, *Committee Hansard*, 22 October 2024, p. 68.

143 See, for example: BSA, *Submission 6*, p. 6; Office of the Information Commissioner (Qld), *Submission 15*, p. 3; CHOICE, *Submission 21*, p. [4]; Insurance Council of Australia, *Submission 28*, p. 2; Australian Institute of Company Directors, *Submission 39*, pp. 1–2; BCA, *Submission 56*, p. 7; Meta, *Submission 57*, p. 3; HRLC, *Submission 60*, p. 12.

144 See, for example: BSA, *Submission 6*, p. 6; Insurance Council of Australia, *Submission 28*, p. 2; Australian Institute of Company Directors, *Submission 39*, pp. 1–2.

2.147 Dr Lisa Archbold et al disagreed with that perspective. In their view, 'the possibility of overlap with AI regulation is not a good reason to delay the implementation of Proposal 19.3'.[145]

2.148 Ms Celeste Moran, First Assistant Secretary, Integrity Frameworks Division, AGD, acknowledged the AGD is working with DISR on AI policy. The ADM provisions in the bill are designed to complement 'the work DISR are doing in relation to AI to ensure that safe and appropriate use of AI'.[146]

2.149 The government has agreed to implement Proposal 19.3 of the Privacy Act Review. According to the AGD:

> This proposal is proposed to be advanced in a further package of reforms, alongside other proposals to expand and introduce new individual rights. This would allow implementation of these reforms to be informed by the Government's work to develop guardrails for safe and responsible AI and a legal framework to support [ADM], consistent with the principles recommended by the Robodebt Royal Commission.[147]

Statutory tort for serious invasions of privacy

2.150 Most inquiry participants broadly supported the introduction of a statutory tort for serious invasions of privacy.[148]

2.151 There is wide community support for legal mechanisms that address invasions of privacy. According to research conducted by CHOICE, 85 per cent of Australian consumers 'believe in the right to sue a business that breaches their privacy'. CHOICE considered that as the proposed tort:

> …would only apply to intentional or reckless invasions of privacy…[the] impact on businesses would be minimal and would only impose a bare minimum standard that consumers should be able to expect of all businesses.[149]

---

145 Dr Lisa Archbold et al, *Submission 34*, p. 8.

146 Ms Celeste Moran, First Assistant Secretary, Integrity Frameworks Division, AGD, *Committee Hansard*, 22 October 2024, p. 68.

147 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

148 See, for example: Privacy 108, *Submission 1*, p. 8; Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 5*, p. 2; Mx Trapani, *Submission 7*, p. [2]; Professor Normann Witzleb, Professor Megan Richardson & Dr Damian Clifford, *Submission 12*, p. 3; ALA, *Submission 14*, p. 6; Queensland Council for Civil Liberties, *Submission 17*, p. 2; Jeff Bleich Centre, *Submission 19*, p. 6; CHOICE, *Submission 21*, p. [4]; Financial Advice Association of Australia, *Submission 25*, p. 3; Emeritus Professor Barbara McDonald and Professor David Rolph, *Submission 27*, p. 2; Dr Lisa Archbold et al, *Submission 34*, p. 10; Peter Clarke, *Submission 51*, p. 1; Access Now, *Submission 55*, p. 4; Meta, *Submission 57*, p. 16; HRLC, *Submission 60*, p. 9; Association for Data-driven Marketing and Advertising, *Submission 68*, p. [4];

149 CHOICE, *Submission 21*, p. [4].

2.152 The HTI submitted the introduction of a statutory tort for serious invasions of privacy would 'provide protection for individuals from some of the worst forms of privacy breach, and provide for a right to remedy for some people affected by such privacy violation'.[150]

2.153 The main concerns raised in relation to the statutory tort related to the:

- increased legal risk for certain professions and industries;
- fault element and whether it should be broadened to include negligent acts that lead to serious invasions of privacy;
- exemptions for journalists and enforcement bodies and whether a similar exemption should be included for businesses; and
- public interest test.

Increased legal risk

2.154 The ACCI and the Ai Group did not support the introduction of the statutory tort provisions as currently drafted.[151] The ACCI argued the provisions 'would create significant legal issues, incentivise class action lawfare, and is inconsistent with the approach taken by like-minded countries like New Zealand, the US and Canada'.[152]

2.155 The Australian Medical Association (AMA) was similarly concerned about the potential for the tort to expose 'healthcare providers and researchers to significant legal risks'. The tort would operate:

> …independently of the [APPs] and the rest of the Privacy Act, meaning an individual or organisation can be sued under Schedule 2, even if they have complied with the Privacy Act, or are not subject to its provisions. It also introduces a dual liability system, where medical professionals may face penalties under the Privacy Act and damages under Schedule 2 for the same act of collecting, using, or disclosing personal information.[153]

2.156 Uncertainty about what would be considered a 'reckless' or 'serious' invasion of privacy 'also creates ambiguity for medical professionals, hospitals, researchers and public health bodies who routinely handle sensitive personal data'. Healthcare providers are also protected by exemptions under the Privacy Act, which would not apply to the tort. If the tort provisions were passed, those providers would be put at increased risk of litigation for breaches of privacy.[154]

---

150 HTI, *Submission 13*, p. [4].

151 Ai Group, *Submission 42*, p. 7; ACCI, *Submission 65*, p. 9.

152 ACCI, *Submission 65*, p. 9.

153 Australian Medical Association (AMA), *Submission 26*, p. 1.

154 AMA, *Submission 26*, p. 1.

2.157 Some of those risks could arise from 'actions that are routine in medical practice', such as collecting family medical history or reports from other specialists without express consent. Medical professionals often engage in other practices that are necessary for them to comply with other legal obligations associated with their work or provide medical care and treatment. Some of those practices that could expose medical professionals to the tort include:

- 'disclosing health information to family members or authorities';
- 'raising concerns about colleagues'; and
- Undertaking 'medical research using personal data'.[155]

2.158 The AMA was also concerned about the lack of an exemption from the statutory tort for peer-reviewed scientific journals, including the *Medical Journal of Australia*. Without an exemption, 'the author, the editor, and potentially the directors and other senior officers' could be subject to the tort if they publish information about a person's financial links to a health product or service.[156]

2.159 The Justice and Equity Centre suggested the proposed tort and its defences contain provisions that would 'alleviate many of the concerns raised' by the AMA. As the tort would only apply 'in circumstances where a person has a 'reasonable expectation of privacy'', many of the AMA's concerns would not be subject to the tort. Furthermore, 'permitted health situations' are exempt from the APPs. The tort is also limited to the 'misuse of personal information'. In the Justice and Equity Centre's view, it is unlikely that the legitimate use of medical information would reasonably constitute such a misuse. The obligation of medical professionals to make mandatory reports to regulatory bodies, such as the Australian Health Practitioner Regulation Agency, 'would attract the lawful authority defence' contained in the bill.[157]

2.160 The AICD also queried whether a company that experienced a cyber attack involving the theft and misuse of personal information by a third party would be subject to the tort. It was concerned that such a company could take all reasonable steps to protect itself from a cyber attack and still find itself in a situation where personal information is misused.[158]

---

155 AMA, *Submission 26*, pp.1–3.

156 AMA, *Submission 26*, p. 3.

157 Justice and Equity Centre, Answer to spoken question on notice, 22 October 2024 (received 4 November 2024).

158 Australian Institute of Company Directors, Submission 39, pp. 4–5.

2.161 Google proposed 'an innocent dissemination defence' for digital platforms that have acted as an intermediary in the serious invasion of an individual's privacy. It argued '[i]t would be impractical for a digital intermediary to operate under any other premise'.[159]

2.162 Mr Harry Godber, Head of Policy and Strategy, Tech Council of Australia, raised similar concerns:

> …if a tort of privacy is introduced that is actionable per se that does not require demonstrated significant loss in order to be actionable, you would risk having large classes of action against any company at any tie where a data breach might have occurred. The crux of the proposed tort is that a serious breach has occurred¬¬—a serious invasion of privacy—but does not necessarily require an individual to have experienced any loss in order to pursue what would be nominal damages but in a class action environment could pose a significant threat to the just, quick and cheap operation of the legal system.[160]

2.163 The AGD explained the tort has several protections for the legitimate use of personal information:

> The tort already provides a number of safeguards to protect legitimate and necessary activities in the medical sector. The includes a public interest balancing element that requires a plaintiff to satisfy the court that the public interest in protecting their privacy outweighs any public interests the defendant may raise. The non-exhaustive list of public interests explicitly includes public health. The tort also includes a range of defences, including consent, and a necessity defence where the defendant reasonably believed that the invasion of privacy was reasonably necessary to prevent or lessen a serious threat to the life, health, or safety of a person. The model of the tort was deliberately crafted to ensure that privacy is balanced with other important public interests. This design of the tort should ensure that legitimate practices in the course of medical care or research do not attract liability under the tort.[161]

Fault element

2.164 The AHRC suggested the bill is too restrictive by limiting the cause of action to serious invasions of privacy that are caused by either intrusion upon seclusion or the misuse of private information. That 'approach is not responsive to a rapidly changing world where digital innovation has sometimes aimed to 'move fast and break things''. A more responsive approach would reflect the human

---

159 Google, *Submission 47*, p. 3.

160 Mr Harry Godber, Head of Policy and Strategy, Tech Council of Australia, *Committee Hansard*, 22 October 2024, p. 12.

161 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

right to privacy set out in the International Covenant on Civil and Political Rights (ICCPR).[162]

2.165 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp; and Member, ARTK, argued that approach would give primacy to the right to privacy and ignore the right of free speech that is also enshrined in the ICCPR. In her view, that would not be appropriate as '[b]oth of those rights actually have equivalence'.[163]

2.166 Emeritus Professor Barbara McDonald confirmed that the ALRC had 'no interest in preferring one [right] over the other' when it proposed the model statutory tort.[164]

2.167 According to the EM:

> The statutory tort for serious invasions of privacy is intended to operate similarly to other torts, in that it would be developed through jurisprudence. It is distinct from the regulatory regime established in the Privacy Act, which requires compliance with the APPs and is overseen by a regulator. As such, it is intended that courts would draw on key concepts from other torts, including privacy torts in other jurisdictions.[165]

2.168 The AGD stated there is broad public support for the introduction of the statutory tort, based on public consultation held in March 2024.[166]

2.169 The cause of action would only apply if an individual:

> …suffer[s] a serious invasion of their privacy, either by an intrusion into their seclusion or by misuse of information, in circumstances where a person in their position would have a reasonable expectation of privacy. Only intentional or reckless invasions are actionable. A mistake – such as an

---

[162] AHRC, *Submission 36*, p. [5]. Note: the International Covenant on Civil and Political Rights (ICCPR) states: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation', see: ICCPR, New York, 16 December 1966, entry into force 13 November 1980, [1980] ATS 23, Part III, Article 17(1).

[163] Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp; and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 35. Note: the ICCPR states: 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'. The ICCPR recognises there are limitations to the right to freedom of expression as it 'carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: For respect of the rights or reputations of others; [or] For the protection of national security or of public order, or of public health or morals', see: ICCPR, New York, 16 December 1966, entry into force 13 November 1980, [1980] ATS 23, Part III, Articles 19(2) and (3).

[164] Emeritus Professor Barbara McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 51.

[165] EM, p. 81.

[166] AGD, Submission 31, p. 2.

> accidental data breach – or mere negligence would not be sufficient. There is no requirement for a plaintiff to prove damage as a result of the invasion, however, the damage or harm a plaintiff suffers will be a relevant factor in assessing the seriousness of the invasion, and the remedies that may be awarded.[167]

2.170 The tort would balance the right to privacy against the public interest:

> Where there is evidence of a competing public interest, the plaintiff must satisfy the court that the public interest in protecting their privacy outweighs it. This balancing exercise is a key element of the cause of action, and recognises that a plaintiff should not be able to claim that a wrong has been committed where an invasion of privacy is justified in the public interest. For example, an individual's privacy may legitimately be invaded in the course of taking action to protect them from serious harm, for example in a bushfire or other emergency situation.[168]

Negligent acts

2.171 The HTI argued 'the tort imposes an appropriately high threshold; it does not, for example, include invasions that are negligent, but requires recklessness or intent to invade the plaintiff's seclusion or misuse of their information'.[169]

2.172 Emeritus Professor McDonald and Professor David Rolph argued:

> …it is appropriate, at this early stage, to limit the statutory tort to intentional and reckless conduct, for several reasons: the novelty of the cause of action in Australia; other available remedies for negligent conduct or for breaches of the Australian Privacy Principles and similar data protection legislation in the States and Territories; and the fact that intentional and reckless invasions of privacy comprise the most egregious forms of invasions of privacy. The recommended fault element underlies the recommendation that the cause of action be actionable without proof of damage.[170]

2.173 In their view, 'if the fault element were to be broadened to include negligence or abandoned in favour of strict liability' the cause of action without proof of damage should be rethought.[171]

2.174 The AICD argued 'it is critical that a statutory tort be confined to 'serious' invasions of privacy and require a fault element of 'intentionality or recklessness'. In its view:

> 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

---

167 AGD, *Submission 31*, p. 6.

168 AGD, Submission 31, pp. 6–7.

169 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [9].

170 Emeritus Professor Barbara McDonald and Professor David Rolph, *Submission 27*, p. 2.

171 Emeritus Professor Barbara McDonald and Professor David Rolph, *Submission 27*, p. 3.

> protection of data is unclear given the evolving nature of data governance and the dynamic threat environment.[172]

2.175 Confining the fault element to intentional or reckless acts 'would be consistent with comparable jurisdictions such as the UK, New Zealand and the US'.[173]

2.176 Google supported limiting the tort to serious invasions of privacy. If the bill was amended to require a plaintiff to prove damage, the legislation 'would be better aligned with the considered reforms in defamation and would strike a better balance between the efficient use of court resources and individuals' rights to privacy'.[174]

2.177 In contrast, Electronic Frontiers Australia recommended the bill be amended to include negligent acts in the tort.[175]

2.178 The AHRC suggested 'the fault element should also cover negligent acts'. It explained the fault element includes an entity conducting an intentional or reckless act that seriously infringes on an individual's privacy. The term 'reckless' is defined in the *Criminal Code Act 1995* and 'requires awareness of a substantial risk. In contrast negligence requires a 'great falling short of the standard of care that a reasonable person would exercise in the circumstances''.[176]

2.179 As the fault element would currently require 'a specific awareness of risk, it potentially rewards ignorance of privacy obligations and allows individuals to shield themselves from litigation by pleading ignorance'. The AHRC recommended the bill remove the fault element as it is 'too high'. If the fault element is retained, it should be redrafted 'to include negligent acts'.[177]

2.180 The ALRC considered including negligent acts in its model tort. Its report stated:

> 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.[178]

---

172 Australian Institute of Company Directors, Submission 39, p. 4.

173 Australian Institute of Company Directors, *Submission 39*, p. 4. Also see: ALRC Report 123, p. 94.

174 Google, *Submission 47*, p. 3.

175 Electronic Frontiers Australia, *Submission 44*, p. 7.

176 AHRC, Submission 36, p. [4].

177 AHRC, *Submission 36*, p. [4].

178 ALRC

2.181 Emeritus Professor McDonald suggested that expanding the definition beyond 'intentional or reckless invasions of privacy' to include negligent acts would require a re-examination of the whole statutory tort framework:

> …the design needs to be taken as a whole—particularly the point that it is 'actual damage' without proof of actual damage, as that is known in the law. 'Actual damage' means personal injury, psychiatric illness, property damage or economic loss. The law traditionally does not treat emotional distress as damage for the purposes of any negligence action. It was a contentious issue as to whether we should extend it to negligence. In our view, looking what has happened in other jurisdictions, the most egregious forms of invasions of privacy have been deliberate.
>
> …
>
> Extending it to negligence without requiring proof of actual damage flies in the face of negligence law generally.[179]

2.182 The tort 'is consistent with the model the ALRC recommended in that it doesn't include a serious harm threshold. It does only apply to serious invasions of privacy, though'. According to Ms Fitch:

> …this recognises that the harm suffered by a serious privacy invasion might often be emotional distress rather than actual damage. Requiring proof of actual damage would prevent damages being awarded for the significant distress and mental anguish which may be caused by a serious invasion of privacy but isn't generally considered under law as actual damage.[180]

Exemptions

2.183 Some inquiry participants highlighted the importance of achieving an appropriate balance between protecting privacy and ensuring that the public interest is not harmed. In their view, the bill should ensure there are safeguards for whistleblowers and journalists acting in the public interest.[181]

2.184 Google argued the bill should expressly address some additional exemptions. In its view, the tort should not apply to:

- any inadvertent capture of images of private activities by street photography, CCTV cameras, or drone usage;[182] and

---

[179] Emeritus Professor Barbara McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 53.

[180] Ms Fitch, AGD, *Committee Hansard*, 22 October 2024, p. 69.

[181] See, for example: Mr Greg Peak, *Submission 2*, p. [2];

[182] The Shopping Centre Council of Australia raised a similar issue about an exemption for footage captured by CCTV cameras. It indicated that CCTV is widely used by shopping centres 'for the purposes of public safety'. For example, 'shopping centre CCTV can be provided to law enforcement as part of investigations into alleged crimes. This can include incidences such as missing persons, theft, violence, and the use of weapons', see: *Submission 48*, p. [1].

- digital intermediaries associated with third party invasions of privacy of which they have no knowledge.[183]

2.185 The HTI recognised that while the tort is broadly based on a model developed by the ALRC, it differs from that 'model in some key respects'. In its view, 'the broad exemptions in the Bill will unnecessarily weaken the scope of the tort's application, and the effectiveness of the tort as a tool to address serious infringements of privacy'.[184]

2.186 The HTI explained:

> International human rights law, and rule of law principles, generally provide that any legal exemption or exception should flow from a specific, demonstrated justification based on the particular circumstance or activity in question, rather than merely the status of an organisation as operating within a context such as 'law enforcement,' 'intelligence' or 'journalism'.[185]

2.187 There are grounds to limit the right to privacy:

> …where the limitation is lawful and not arbitrary. In order for interferences not to be arbitrary, they must seek to achieve a legitimate aim (such as public interest, national security), and be reasonable, necessary and proportionate to achieving that aim.[186]

2.188 The AHRC similarly submitted that there are limitations to the right to freedom of expression:

> The right to freedom of expression has been described as constituting 'the foundation stone for every free and democratic society' and is enshrined in a range of international and regional human rights instruments. The right is not absolute and its exercise 'carries with it special duties and responsibilities'.[187]

2.189 Restrictions on the right to freedom of expression:

> …must be provided for by law and may only be imposed for 'respect of the rights or reputations of others' or 'for the protection of national security or of public order or of public health or morals'. Any such restrictions must also meet strict tests of necessity and proportionality. This requires that any proposed restriction pursues a legitimate aim, is proportionate to that aim, and is no more restrictive than is required for the achievement of that aim.[188]

---

183 Google, *Submission 47*, p. 2.

184 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [9].

185 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [9].

186 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [11].

187 AHRC, *Submission 36*, pp. [6]–[7].

188 AHRC, *Submission 36*, p. [7].

2.190 The AHRC explained:

> The proposed criminal offence of doxxing will limit the human right to freedom of expression by restricting certain forms of sharing information. The key issue is ensuring any offence is carefully tailored to meet the strict tests of necessity and proportionality and to avoid capturing reasonable online discourse about a person.[189]

2.191 The AHRC recognised there may be instances where there are legitimate public interest grounds to share or publicise personal information. It also suggested:

> While the sharing of information online in this way has the potential to enhance public safety, there is also a potential risk of digital vigilante activity, which may see individuals seek to enforce a 'parallel form of criminal justice', and can undermine rule of law protections.[190]

2.192 The doxxing offences could also 'unreasonably capture public interest whistleblowing and journalism'.[191]

2.193 The bill would:

> …guard against these risks by providing that the offences only apply where 'the person engages in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those individuals'. However, including a provision in the Bill which expressly protects the release of information for legitimate public interest purposes would help to further strengthen the protection of freedom of expression while still effectively addressing the harms caused by doxxing.[192]

2.194 To provide greater protection of freedom of expression, the AHRC recommended the bill include a provision that protects 'the release of information for legitimate public interest purposes'.[193]

2.195 The AGD explained the exemptions were included in the bill to save the time and resources of courts and litigants:

> The main rationale for including exemptions rather than relying on defences or the public interest balancing test itself is to that it makes it clearer at an earlier stage that, on the face of the act, for the tort a broad range of entities are not captured. That would be intended to indicate there's no need to begin an inquiry into these matters at all or for those entities to even raise a defence. That's ultimately directed at not wasting time and resources, either of the litigants or the courts.[194]

---

189 AHRC, *Submission 36*, p. [7].

190 AHRC, *Submission 36*, pp. [7]–[8].

191 AHRC, *Submission 36*, p. [8].

192 AHRC, *Submission 36*, p. [8].

193 AHRC, *Submission 36*, p. [8].

194 Ms Fitch, AGD, *Committee Hansard*, 22 October 2024, p. 69.

Exemption for journalistic activities

2.196 The bill's exemption for journalism was welcomed by some inquiry participants.

2.197 For example, the Queensland Council for Civil Liberties argued there should be an exemption for 'professional journalism'. The exemption should apply to journalistic material that is 'genuinely in the public interest'.[195]

2.198 The ABC reminded the committee that 'national broadcasters, as agencies, benefit from an exemption derived from the *Freedom of Information Act 1982*, which operates differently to the media organisation exemption'. The ABC strongly emphasised 'it is critical that the national broadcasters' exemptions continue to apply'.[196]

2.199 To ensure that the exemption for national broadcasters continues to apply, the ABC proposed 'that an additional exemption be created to align the privacy tort exemption regime' to the existing exemption in the Privacy Act.[197]

2.200 ARTK argued 'media organisations and those engaged in the activity of professional journalism should not be subject to the statutory tort either directly or indirectly'.[198]

2.201 The Free Speech Union of Australia (FSU) and Australian Christian Lobby suggested that those engaged in journalistic activities should include 'citizen journalists'.[199] Electronic Frontiers Australia Inc (EFA) agreed it is necessary to include citizen journalists to 'hold them accountable for any privacy harms that their reporting might cause individuals'.[200]

2.202 Per Capita, Centre of the Public Square argued the journalism exemption 'should be removed and replaced with a blanket public interest journalism defence. This would require journalists to prove that an invasion of privacy was in the public interest'.[201]

2.203 ARTK expressed a preference for an exemption for journalistic activity, rather than a defence. The exemption as currently drafted, however, would 'not be fully effective' as it:

---

195 Queensland Council for Civil Liberties, *Submission 17*, p. 2.

196 ABC, *Submission 38*, p. 1. Note: the ABC referred to the exemption in paragraph 7(1)(c) of the *Privacy Act 1988*. That exemption applies to the program material and datacasting content of the ABC, see: Division 1 in Part II of Schedule 2 of the *Freedom of Information Act 1982*.

197 ABC, *Submission 38*, p. 2. Also see: Special Broadcasting Service, *Submission 40*, p. [1].

198 Australia's Right to Know, *Submission 59*, p. 2.

199 Free Speech Union of Australia, *Submission 4*, p. 3; Australian Christian Lobby, *Submission 58*, pp. 7–8.

200 Electronic Frontiers Australia Inc, *Submission 44*, p. 7.

201 Per Capita, Centre of the Public Square, *Submission 35*, p. 5.

> …is a narrow exemption which is not adapted to the circumstances of the proposed cause of action. Many persons involved in journalism are not covered. It does not cover:
>
> - publishers who are not the employer of the journalist—the drafting assumes the publisher is the journalist's employer, but in modern news organisations the publisher is often a different entity to the employer entity;
> - publishers who are licensees of the original publisher;
> - publishers whose journalists are engaged as contractors or contributors, rather than as employees;
> - other involved in journalism/publishing who are not journalists but not limited to printers, distributors, retailers, production personnel;[202]
> - journalists' sources who are not acting in a "professional capacity.[203]

2.204 ARTK argued that these limitations to the proposed exemption would lead to 'a serious chilling of public accountability, as its operation will both indirectly and directly undermine journalism and curtail freedom of expression'. The exemption would hinder journalists from being able:

> …to investigate, gather information on and report stories of public interest, particularly where the reporting relates to a public figure or wealthy individual with the means to launch legal action to prevent publication of the story via an indirect injunction and/or pre action discovery.[204]

2.205 ARTK argued the term 'journalistic material' is defined too narrowly to adequately protect all aspects of journalism from the tort.[205]

2.206 The bill would define 'journalistic material' as any material that:

> (a) has the character of news, current affairs or a documentary; or
> (b) consists of commentary or opinion on, or analysis of, news, current affairs or a documentary.[206]

2.207 In ARTK's view, the term 'journalistic material' as defined in the bill only refers to:

> …one subset of journalism…Free speech should not be constrained by the 'character' or mode of expression by a journalist or the media as this imports an unnecessary and undesirable subjective element which inhibits that

---

202 Note: Emeritus Professor McDonald and Professor Rolph argued this suggestion is 'misconceived'. They explained '[l]iability can only be established if the defendant's conduct is intentional or reckless. Thus, a printer ordinarily could only be held liable for the statutory tort of serious invasion of privacy if the printer intentionally or recklessly invaded the plaintiff's privacy', see: Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024).

203 ARTK, *Submission 59*, p. 3.

204 ARTK, *Submission 59*, pp. 3–4.

205 ARTK, *Submission 59*, p. 5.

206 Item 15(3) in Part 3 of Schedule 2 of the bill.

> freedom. In contrast, it is all the activities of a free press which underpin the public's interest in the free flow of information. Those activities are matters of fundamental importance in a democratic society. Thus the proposed exemption should protect the activity of journalism.[207]

2.208 Ms Kiah Officer, Executive Counsel, Nine Entertainment Co, and Member, ARTK, maintained journalism plays an important role in Australian society and it should be properly protected:

> Journalism is a very wide range of services that professional media provide to the community. All of those services have importance. There is a public interest in freedom of discourse, freedom of expression and transparency, and we would say that those principles should certainly receive protection.[208]

2.209 The proposed exemption would not extend to a journalist's sources, which would further constrain the work of the media as those sources may be less willing to participate in journalistic activity:

> …the narrow scope of the exemption raises the prospect of sources being sued for the provision of the information to a journalist or media organisation. No doubt many people—sources— will be reluctant to assist in those circumstances and this also will have a considerable impact on the flow of information and reporting.[209]

2.210 Ms Officer, Nine and ARTK, opined that the lack of an exemption for sources would leave those sources 'potentially vulnerable to being sued under the tort'. Even sources who offer information confidentially might not be protected as they would not:

> …have the benefit of the shield law protections and whistleblower protections which we currently have under various jurisdictions and which are not necessarily adequate to provide a level of protection to those sources. We have not examined, nor are we certain about, the interplay between whatever current protections there may be, but we have concerns that the bill as currently drafted appears to create some exposure for confidential sources.[210]

2.211 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp, and Member, ARTK, argued there are similar frameworks internationally that protect freedom of speech and the media:

> …including article 10 of the European Convention on Human Rights, obviously, the First Amendment in the US and, of course, Australia's own

---

[207] ARTK, *Submission 59*, p. 5.

[208] Ms Kiah Officer, Executive Counsel, Nine Entertainment Co, and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 31.

[209] ARTK, *Submission 59*, p. 6.

[210] Ms Officer, Nine and ARTK, *Committee Hansard*, 22 October 2024, pp. 32–33.

> Privacy Act, which provides an exemption for journalism, as it currently stands.[211]

2.212 Ms Clare O'Neil, Director, Corporate Affairs, SBS, and Member, ARTK, added '[t]here is already a wide range of regulations and laws that govern anything that might be considered malicious or nefarious activity—things like the Surveillance Devices Act and defamation'.[212]

2.213 Mr Hamish Thomson, Head of Legal, Guardian Australia, and Member, ARTK, explained journalists are bound by professional codes and complaints processes that deter them from acting outside of the public interest:

> There is a very healthy claims lawyer industry…We are all organisations that are facing enormous financial pressures. The point of an exemption here is to avoid us getting into those preliminary, very costly and really inappropriate ways to deal with what is already something for which we have systems in place. Just to go to court, to have to prove a defence, to have to prove initial issues of serious harm, will have enough of a chilling effect on our journalists and on our editors to stop scrutinising the very people that are employing these kinds of lawyers—the wealthy, powerful people who are employing these lawyers.[213]

2.214 Ms Officer echoed that view:

> …international experience suggests that these are not laws utilised by everyday citizens to protect individual breaches of privacy. They very much become tools of celebrities, politicians and wealthy public figures to essentially stifle the publication of information that might be at odds with whatever public persona they seek to portray…This tort is unlikely to provide a remedy for individual citizens seeking to protect their privacy.[214]

2.215 She further argued that the serious harm test might not limit the number of cases that go before the courts as that has not been the experience with Australian defamation law:

> Protection of reputation is very well catered for in current Australian law. Even so, the legislature saw fit to introduce a serious harm test to defamation, to recognise that there is a threshold there, to try to minimise the number of claims before the courts and to limit those to only the most

---

211 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp; and Member, Australia's Right to Know, *Committee Hansard*, 22 October 2024, p. 30.

212 Ms Clare O'Neil, Director, Corporate Affairs, Special Broadcasting Service; and Member, Australia's Right to Know, *Committee Hansard*, 22 October 2024, p. 30.

213 Mr Hamish Thomson, Head of Legal, Guardian Australia; and Member, Australia's Right to Know, *Committee Hansard*, 22 October 2024, p. 30.

214 Ms Kiah Officer, Executive Counsel, Nine Entertainment Co; and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 31.

> serious cases. Even so, we still have a booming defamation industry. We would say that is a comparable test to apply.[215]

2.216 Ms Bridget Fair, Chief Executive Officer, Free TV Australia, and Member, ARTK, indicated there has been 'a complete explosion in the use of defamation claims as a means of trying to shut stories down'. The increase in defamation cases against media organisations:

> …in itself has a chilling effect on the ability of media organisations to report stories, both large and small. Boardrooms around the country, from small organisations to listed companies, are actively debating the amount of money they can put aside to fund legal actions that are brought speculatively because we a defamation claims industry in this country. We do not want to replicate that in the privacy arena.[216]

2.217 Ms Sarah Kruger, Chief Legal and Government Affairs Officer, Commercial Radio and Audio, and Member, ARTK, also highlighted the pressures experienced by the commercial radio industry that deter it from acting outside of the public interest:

> Any risk, whether that is in terms of additional administrative burden, financial burden, litigation or the risk of some kind of adverse consequence, will have a chilling effect because our stations simply cannot afford to go down a litigious route.[217]

2.218 Commercial Radio and Audio (CRA) posited that the exemption for journalistic activities would:

> …be developed through jurisprudence. This means that Australian media organisations, and individual journalists, will be subject to costly and protracted litigation to determine that scope. That threat of litigation, in itself, will have a chilling impact on freedom of speech and journalism.[218]

2.219 CRA suggested Australia has the opportunity to avoid the weaponisation of its proposed statutory tort, by:

> …ensur[ing] that journalism is entirely exempted from the tort. This will ensure the protection of journalism and free speech, as well as the public's right to be fully informed, which is essential in a democracy.[219]

---

[215] Ms Officer, Nine and ARTK, *Committee Hansard*, 22 October 2024, p. 31.

[216] Ms Bridget Fair, Chief Executive Officer, Free TV Australia; and Member, ARTK, *Committee Hansard*, 22 October 2024, p. 33.

[217] Ms Sarah Kruger, Chief Legal and Government Affairs Officer, Commercial Radio and Audio; and Member, Australia's Right to Know, *Committee Hansard*, 22 October 2024, p. 30.

[218] CRA, *Submission 43*, p. 2.

[219] CRA, *Submission 43*, p. 6.

2.220 That more fulsome exemption could include:

- a broader definition of the exempt journalist content, particularly to include other material of [public] interest…There is no need to link the definition to a particular class of persons such as journalists or their employers, as any defendant should be able to rely on this exemption in the event that proceedings are commenced against them in relation to exempt journalist content;
- an additional statutory right for defendants to apply for a claim to be struck out at an early stage of proceedings where the matter complained about relates to the collection, preparation for dissemination or dissemination of exempt journalist content; and
- if a defendant is successful in having the proceedings struck out then:
  - a Court may not order the defendant to pay the plaintiff's costs except where in the Court's view misconduct of the defendant in relation to the claim justifies such an order; and
  - the defendant will be entitled to indemnity costs relief, unless in the Court's view the defendant has engaged in misconduct.[220]

2.221 ARTK put forward two alternative options that would replace the journalism exemption in Item 15 of Part 3 in Schedule 2 of the bill. Its preferred option would broaden the exemption to include a wider definition of journalistic material:

> This Schedule does not apply to an invasion of privacy by any person engaged in activities related or incidental to the provision of information for, collection, preparation for publication, or other activities related or incidental to reporting news, presenting current affairs, expressing editorial or other content in news media or documentary media.[221]

2.222 The other alternative proposed by ARTK would add the underlined text to proposed clause 15(1):

> This Schedule does not apply to an invasion of privacy by any of the following, to the extent that the invasion of privacy involves the <u>provision of information for,</u> collection, preparation for publication, <u>communication or other activities related and incidental to reporting news, presenting current affairs, expressing editorial or other content in news media or documentary media:</u>
>
> (a) a journalist;
> (b) an employer of a journalist<u>, or person or organisation engaging a journalist</u>;
> (c) a person assisting a journalist who is employed or engaged by the journalist's employer <u>or person or organisation engaging a journalist</u>;

---

220 CRA, *Submission 43*, p. 6.

221 ARTK, *Submission 59*, p. 7. Note: this definition would replace the proposed amendments in Item 15 in Part 3 of Schedule 2 of the bill.

(d) a person assisting a journalist in the collection, consideration and or preparation for publication, or who otherwise assists in the provision of information for, preparation of or in the course of reporting news, presenting current affairs or expressing editorial or other content in news media.[222]

2.223 In contrast, several inquiry participants raised concerns about the exemption for journalistic activities.[223]

2.224 Peter Clarke suggested that instead of a blanket exemption, the bill should be redrafted to include '[r]obust defences in support of journalists properly undertaking their profession'. In his view, the exemption 'goes beyond free expression and supporting the legitimate exercise of journalism but provides a blanket coverage to the excesses committed by journalists which should not be tolerated'.[224]

2.225 Emeritus Professor McDonald & Professor Rolph, University of Sydney, submitted:

> The exemption for journalists in the bill is surprising, in that we know of no similar exemption anywhere else in the common law world, and particularly in its broadness. Once engaged, there is no limit on the exemption. Even if a journalist were to commit a crime in the serious invasion of the plaintiff's privacy the exemption would apply. We note that an exemption was neither proposed no recommended by the ALRC in its 2014 Discussion Paper or Report, nor has it been the subject of widespread public consultation before this Bill.[225]

2.226 Emeritus Professor McDonald argued that if the exemption is retained:

> …at the very least, the exemption should have limitations on it. At the moment it's absolute. The exemption applies even where the relevant parties committed a crime in invading someone's privacy.
>
> …
>
> But that's no help for the victim. The victim isn't able to take action. The victim relies on the law enforcement authorities being interested in pursuing that. There's no recompense for the victim. We could, for example, after every crime, every criminal provision, put in a provision that the court may, on application, provide compensation—for example, for breach of the Surveillance Devices Act or the Telecommunications Act and so on. We

---

222 ARTK, *Submission 59*, p. 7.

223 See, for example: Professor Normann Witzleb, Professor Megan Richardson & Dr Damian Clifford, *Submission 12*, p. 3–5; Dr Michael Douglas, *Submission 54*, p. [1];

224 Peter Clarke, *Submission 51*, pp. 8–9.

225 Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, p. 7.

> could give courts the power to grant compensation for that. That would fill some of the gaps that we have, rather than this wholesale new tort.[226]

2.227 The HTI raised the same point:

> …the journalism exemption would exclude any acts ostensibly done while developing 'journalistic material', regardless of the content or purpose of the journalism, including its merits as public interest journalism. This would exclude from coverage blatantly unlawful, even criminal, and unjustifiable infringements of privacy by journalists that are not in the public interest.[227]

2.228 The HTI provided the following examples of journalistic material that would not be covered by the tort:

- illegal phone hacking by a news corporation, as occurred during the *News of the World* phone hacking scandal in the United Kingdom; or 'upskirting' photos taken of celebrities by a tabloid.[228]
- a journalist maliciously publishing the home addresses and contact details of government officials. Doxxing would not fall within the scope of the tort if it occurred in the course of journalistic activities. However, doxing would be covered by the criminal provisions for doxxing offences in Schedule 3 of the Bill, where it meets the relevant criteria.[229]

2.229 The HTI recognised the importance of public interest journalism and suggested that the bill be amended to make it clear that the defences and exemptions for journalistic activities 'only applies to journalism that is in the public interest'.[230]

2.230 Professor Santow proposed that instead of a broad exemption for journalistic activities:

> …there should be a really strong focus on protecting public-interest journalism, and that would be by having a broad, robust defence for anyone who is accused of this statutory tort [inaudible] that they are engaging in public-interest journalism, not simply that they have the status of a journalist and so whatever they do cannot be impugned.[231]

---

226 Emeritus Professor McDonald, Private capacity, *Committee Hansard*, 22 October 2024, p. 52.

227 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

228 Note: Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp; and Member Australia's Right to Know, stated '[t]here has been no evidence of phone hacking in Australia. In the UK that happened a number of years ago. The UK laws have changed significantly since that time, to the detriment of reporting…There is no evidence of phone hacking in Australia', see: *Committee Hansard*, 22 October 2024, p. 33.

229 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

230 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [11].

231 Professor Santow, HTI, *Committee Hansard*, 22 October 2024, p. 27.

2.231 DRW endorsed Professor Santow's view and suggested there are other avenues available to protect public interest journalism:

> …there are also other court processes that exist, including the use of things like summary dismissal, striking out and the like that exist as part of normal court procedure and would assist media organisation where they've engaged in proper practices and engaged in public-interest journalism. I don't think there needs to be an exemption to still have the functionality of trying to deal with vexatious litigation. There are other processes that exist within court rules already that would provide for that. So I share HTI's concerns about the breadth of the exemption and its functionality. I think we'd better redraft it as a defence.[232]

2.232 There are other protections available in the tort that protect journalism:

> Apart from other defences available to defendants, the cause of action imposes a 'seriousness threshold' that operates in addition to the public interest balancing test, a construction which the ALRC acknowledges was intended to 'further ensure the new tort does not unduly burden competing interests such as freedom of speech'. This was recognised in the Privacy Act Review Report, which noted that the '[ALRC] model slightly preferences other public interests over the public interest in privacy as the test requires that privacy outweigh other interests'.[233]

2.233 The journalism exemption was viewed as unnecessary and unjustified as:

> Senior and lower courts across Australia, and indeed the common law world, have a demonstrated history of being able to balance the public interest in individual privacy protection against the broader public interest in journalistic activity. The proposed exemption is a clear outlier in that regard.[234]

2.234 The ABC indicated the bill may expose a third party that distributes or publishes national broadcaster content to the tort. It provided the example of 'an airline that shows news to passengers, will be vulnerable to the tort, whereas the news provider will not be'. There is a similar risk that if a national broadcaster sourced licensed content from a provider that was not protected by the exemption, the national broadcaster could be exposed to the tort. The ABC requested further clarity on these issues.[235]

---

232 Ms O'Shea, DRW, *Committee Hansard*, 22 October 2024, p. 27.

233 Professor Normann Witzleb, Professor Megan Richardson & Dr Damian Clifford, *Submission 12*, pp. 7–8.

234 Dr Lisa Archbold et al, *Submission 34*, p. 10.

235 ABC, *Submission 38*, p. 2.

2.235 The Law Council suggested that organisations involved in the publication of journalistic material may not be the employer of the journalist and, therefore, may not be exempt from liability. It explained 'that publishers often source material from self-employed journalists or other content providers'.[236]

2.236 There is also a possibility that the tort could 'have a chilling effect on legitimate free speech'. The Law Council argued:

> the exemption for journalists will not cover many journalists' sources, with the effect being that tortious action could be taken against a source instead of a journalist as a means of bypassing the exemption.[237]

2.237 In relation to the related matter of journalistic freedom, the Law Council opined:

> the definition of 'journalistic material' in proposed subclause 15(3) with reference to 'news, current affairs or a documentary' is unduly narrow in scope, despite the evolving nature of information transmission methods and delivery, and the broad range of topics they ay touch upon—thereby risking journalistic freedom to pursue matters of genuine public interest.[238]

2.238 The proposed definition of 'journalistic material' would also fail to provide an exemption for several:

> …other legitimate forms of free speech (for example, works including biographies or memoirs) or other media content that otherwise offers a valuable contribution to cultural and public life (for example, comedy, satire and other entertainment).[239]

2.239 The AGD explained the definition of journalistic material:

> …is intended to be 'platform neutral'; it covers those materials considered relevant for the additional protection provided by a journalism exemption – i.e. material that has the character of news, current affairs or a documentary, or consists of commentary, opinion on, or analysis of news, current affairs or a documentary. Material, activity or expression that does not meet the requirements of the exemption could potentially still be subject to the tort where the elements were established – including that the privacy invasion was serious, the plaintiff had a reasonable expectation of privacy, the defendant's conduct was intentional or reckless, and if the public interest balancing test were met.[240]

2.240 The exemption is not intended to extend to journalists' sources. The AGD indicated:

> …there are policy reasons for taking this approach. Whistleblower laws are intended to address concerns about liability in certain public interest

---

236 Law Council, *Submission 67*, pp. 35–36.

237 Law Council, *Submission 67*, p. 36.

238 Law Council, *Submission 67*, p. 36.

239 Law Council, *Submission 67*, p. 36.

240 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

> contexts in a consistent manner that extends beyond specific causes of action. Every Australian jurisdiction also has 'journalist shield' laws that prevent journalists from being required to disclose the identity of sources.[241]

2.241 The exemption also 'extends to journalists' employers. It is not clear the extent to which extending its application more broadly would satisfy the policy intent of protecting the beneficial role of journalism'.[242]

2.242 The AGD advised the exemption for journalistic activities:

> …recognises the important and beneficial role of journalism in a free and democratic society; it is intended to mitigate the risk that the mere prospect of litigation would have a chilling effect on reporting…Conduct that does not meet the requirements of the exemption could potentially still be subject to the tort where the elements were established—including that the privacy invasion was serious, the plaintiff had a reasonable expectation of privacy, and the defendant's conduct was intentional or reckless, as well as the public interest balancing element.[243]

Exemptions for enforcement bodies and intelligence agencies

2.243 The HTI submitted that enforcement bodies would be exempt from the tort. Those bodies would include:

> …agencies such as police, and a range of other bodies at the state, territory and federal level with powers to issue civil penalties or sanctions, ranging from the Department of Home Affairs to Sports Integrity Australia.[244]

2.244 An enforcement body is exempt from the tort when it 'reasonably believes that the invasion of privacy is reasonably necessary for one or more enforcement related activities'.[245] In the Human Technology Institute's view "[e]nforcement related activity' is another broad term, which includes pursuing minor civil fines, and the prevention of minor crimes, such as speeding'.[246]

2.245 The HTI suggested:

> The exemption for enforcement bodies could hypothetically cover unlawful actions by enforcement bodies, as long as the body 'reasonably believes the invasion of privacy is reasonably necessary'. This very low expectation of what the Bill deems to be proper behaviour by enforcement bodies, coupled with the extraordinary breadth of activities in respect of which enforcement bodies may claim this exemption, means that this exemption almost offers

---

241 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

242 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

243 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

244 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

245 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10]. Also see: item 16 in Part 3 of Schedule 2.

246 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

> carte blanche to those bodies to flout the privacy protection in this new statutory tort.[247]

2.246 It illustrated its point by explaining that the tort would not apply to an 'unlawful search and seizure by the Australian Tax Office, where it was 'reasonably believed it was reasonably necessary' to prevent potential tax avoidance'.[248]

2.247 The HTI indicated that 'any activity by intelligence agencies would be fully exempt from the scope of the tort, including activities conducted for malign or illegal purposes'.[249]

2.248 It suggested that the tort would not apply to 'illegal surveillance of Australian citizens by national security organisations due to their race, religion, sexuality or political beliefs'.[250]

2.249 Peter Clarke asserted that the exemption for 'enforcement bodies is too wide'. He indicated that enforcement bodies, including police services, 'have had a chronic problem of misusing information or abusing their positions. The exemption should not exist. There should be a defence available to enforcement bodies'.[251]

2.250 The HTI argued that the exemption provisions for enforcement bodies and intelligence agencies is unnecessary as they would be 'covered by the 'authorised by law' defence' elsewhere in the bill.[252] It suggested the proposed defence should be amended to make it clear that it would apply as follows:

- Enforcement bodies are covered by this defence if they are conducting lawful investigations in respect of serious crime, with independent authorisation. This wording would encompass authorisation through judicial warrants, and warrants issued by a judge or magistrate acting persona designate.
- Intelligence agencies are covered by this defence if they are conducting a lawful national security operation, with independent authorisation.[253]

2.251 The defence provisions should be further amended to make it clear that it would:

> …be restricted to invasions of privacy required or expressly authorised by law. This would prevent arguments claiming that privacy interferences

---

247 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

248 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

249 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [10].

250 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [11].

251 Peter Clarke, *Submission 51*, p. 9.

252 Human Technology Institute, University of Technology Sydney, *Submission 13*, pp. [11]–[12]. Also see: Item 8(1)(a) in Part 2 of Schedule 2 of the bill.

253 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [12].

> were merely impliedly authorised by law – for example, the use of spyware in devices that is not explicitly included in a warrant authorising some limited search activities.[254]

2.252 Emeritus Professor McDonald also saw the exemption for enforcement bodies and intelligence agencies as unnecessary:

> We didn't feel that was needed because we've got the lawful authority defence and also there can be no reasonable expectation of privacy for someone where the law enforcement bodies are lawfully pursuing their investigations. Obviously, we want our law enforcement bodies to investigate the commission of crimes and so on. That's what they are there for. It may be that, firstly, there's no reasonable expectation of privacy and, secondly, the lawful authority defence would apply.[255]

2.253 Emeritus Professor McDonald did not understand why the exemption had been included in the bill:

> …other than perhaps they feel there is some ancillary conduct. Take a case like Smethurst v Commissioner of Police, which went to the High Court a couple of years ago. There, a journalist's home was raided under an invalid warrant by the Australian Federal Police, who seized data from her phone, put it onto their own USB stick and then refused to give it back. In the end she couldn't get it back. She couldn't get a mandatory injunction for it to come back. The High Court stated many times in their judgements

2.254 The AGD explained the exemption for law enforcement bodies is intended to ensure:

> …these entities are not unduly restricted in carrying out their functions which may need to be privacy invasive. An invasion of privacy by an enforcement body is exempt only to the extent that an enforcement body reasonably believes it is reasonably necessary for one or more of the enforcement-related activities it is undertaking.[256]

2.255 The Australian Federal Police advised that the proposed exemption for law enforcement agencies 'is consistent with existing provisions in the Privacy Act'.[257]

Exemptions for businesses

2.256 The Council of Small Business Organisations Australia (COSBOA) and the Australian Industry Group (Ai Group) suggested there should be an exemption for small businesses.

---

254 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [12].

255 Emeritus Professor McDonald, Private capacity, *Committee Hansard*, 22 October 2024, p. 53.

256 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

257 Australian Federal Police, *Submission 71*, p. [1].

2.257 COSBOA, argued that without an exemption for small businesses:

> The introduction of the statutory tort will create a new risk of vicarious liability, potentially exposing small businesses of all sizes to legal responsibility for the actions of their employees or agents where the invasion of privacy occurred within the course of employment.[258]

2.258 Professor Santow was not aware of a similar small business exemption in any other comparable jurisdiction and that the position of COSBOA and the Ai Group is 'a very difficult position to maintain'. He explained the position is difficult to maintain as:

> The right to privacy is a human right. As just an ordinary member of the public, it is no less harmful to you if your right to privacy has been seriously invaded by a large company or a small company. It is just harmful if it's a small company. So I don't think it's helpful to focus on this idea of offering certain companies some sort of blanket exemption. Rather, it would be more helpful to focus on what the small business ombudsman has been calling for, which is really clear practical guidance for small- and medium-sized enterprises so that they really understand how they can stay on the right side of the law and some of the easy things that they can do to make sure that they don't inadvertently fall foul of this new law.[259]

2.259 The Business Council of Australia recommended there be an exemption in relation to employee records.

2.260 Ms Louise McGrath, Head of Industry Development and Policy, Ai Group, reminded the committee:

> …we have consistently pressed for the employee records and small business exemptions to be retained and for the government to instead pursue best practice outcomes for members' dealing with personal information. We maintain this position.[260]

2.261 She outlined that employers deal with the personal information of their employees:

> …for legitimate reasons and in the public interest. We ask the committee to consider that. This includes where employers manage their workers' conduct and performance to ensure compliance with their obligations under workplace laws and to keep people and property safe and free from injury or damage.[261]

---

258 Mrs Sutton, COSBOA, *Committee Hansard*, 22 October 2024, p. 38.

259 Professor Santow, HTI, *Committee Hansard*, 22 October 2024, p. 26.

260 Ms Louise McGrath, Head of Industry and Policy, Australian Industry Group, *Committee Hansard*, 22 October 2024, p. 37. Note: Ms McGrath clarified that in relation to the exemption for employee records, Ai Group sought an exemption for all businesses, not just small businesses, see: p. 42.

261 Ms McGrath, Ai Group, *Committee Hansard*, 22 October 2024, p. 37.

2.262 Ms Yoness Blackmore, Principal Advisor, Workplace Relations Policy, Ai Group, elaborated on the reasons that businesses might collect and store the personal information of their employees:

> …privacy can't be viewed in isolation, and there is a complex web of workplace relations laws. Employers must, and are entitled to, manage their workplace and run an efficient business. Part of doing so requires that they deal with data of their workers, too—for example, ensure that those workers work in a safe way, ensure that sexual harassment isn't happening in the workplace, and so forth.[262]

2.263 In her view there should be definitional consistency between the Privacy Act and the proposed tort:

> …both the small business exemption and the employee records exemption be applied to the statutory tort, because otherwise you would have the Privacy Act going along and then you would have the case law happening on the side. We would also propose that information in terms of the statutory tort should have the same definition as that applied under the Privacy Act. At the moment the Privacy Act has a definition of 'personal information' and 'health and sensitive information', but that is not the same as information under the statutory tort. Even on the grounds of consistency, we think that there needs to be alignment of those things.[263]

2.264 EFA argued employee records are treated no differently to 'the information organisations or government agencies collect about their customers or clients'. For that reason:

> There's no reason why the employee record exemption cannot be repealed and work equally well, amongst the new privacy principles, by way of any necessary minor exemptions that might need to be made to protect employers' positions in relation to legal claims.[264]

Public interest test

2.265 The bill would allow a defendant to adduce 'evidence that there was a public interest in the invasion of privacy'. To counter that evidence, a 'plaintiff must satisfy the court that that public interest was outweighed by the public interest in protecting the plaintiff's privacy'.[265]

2.266 Emeritus Professor McDonald and Professor Rolph, University of Sydney indicated this provision of the bill differed from the recommendation made by the ALRC as outlined in Table 2.1.

---

[262] Ms Yoness Blackmore, Principal Advisor, Workplace Relations Policy, Ai Group, *Committee Hansard*, 22 October 2024, p. 39.

[263] Ms Blackmore, Ai Group, *Committee Hansard*, 22 October 2024, p. 39.

[264] Mr Pane, EFA, *Committee Hansard*, 22 October 2024, pp. 27–28.

[265] Item 7(1) in Part 2 of Schedule 2 of the bill.

Table 2.1 Difference between ALRC recommendation and clause 7(3) of the bill

ALRC recommendation	Clause 7(3) of the bill
9.1 The Act should provide that, for the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest.	If the defendant adduces evidence that there was a public interest in the invasion of privacy, the plaintiff must satisfy the court that that public interest was outweighed by the public interest in protecting the plaintiff's privacy.
9.3 The Act should provide that the defendant has the burden of adducing evidence that suggests there is a countervailing public interest for the court to consider. The Act should also provide that the plaintiff has the legal onus to satisfy the court that the public interest in privacy outweighs any countervailing public interest that is raised in the proceedings.	
Suggested clause 7(3)	
The court may only determine that the plaintiff has a cause of action if the court is satisfied that the public interest in the plaintiff's privacy outweighs any countervailing public interest. A defendant may adduce evidence that there is a countervailing public interest that outweighs the plaintiff's interest in privacy. (These will probably need to be two separate sub-clauses).	

Source: Emeritus Professor Barbara McDonald and Professor David Rolph, University of Sydney, *Submission 27*, pp. 3-5.

2.267 In their view, the bill should require a court to 'consider the matters of public interest that justify the invasion of the plaintiff's privacy'. It should also clarify 'the onus/burden, if any, on a defendant to adduce evidence'.[266]

2.268 Emeritus Professor McDonald and Professor Rolph suggested there are cases where the public interest is self-evident without the adducing of evidence. For that reason:

> We do not think that defendants should be required to adduce evidence of public interest in every case before they might raise a countervailing public

[266] Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, p. 3.

> interest for the court to consider. So to require would unnecessarily increase the cost and complexity of litigation without any demonstrable public benefit. However, defendants should be permitted to adduce evidence relevant to public interest considerations if they think it is appropriate or necessary. The statutory cause of action should be redrafted to make it clear that the defendant may adduce evidence to establish public interest grounds to be balanced with the public interest in the plaintiff's privacy, but are not required to do so.[267]

2.269 Their suggested clause 7(3) would overcome this issue while:

> …also mak[ing] it abundantly clear that liability depends upon balancing competing interests, including any public interest ground identified or argued by the defendant, and that the public interest is not a defence, properly so called.[268]

2.270 The HTI endorsed that proposal 'recognising that it will not always be necessary or practical for the defendant to adduce evidence as to the public interest limb in every case'.[269]

2.271 Emeritus Professor McDonald argued against the inclusion of a public interest defence:

> …it is a matter of judgement as to whether something is in the public interest. How can you prove that it is in the public interest to reveal somebody's residential address, or something like that? We couldn't see how it could be a matter of proof on the balance of probabilities that more probably than not it was in the public interest. There are other contexts in which public interest is seen as a matter for judgement. For example, in sub judice contempt, where the court is considering whether the media have published information which would have a tendency or a likelihood of interfering with a fair trial, one of the issues will be whether or not there is sufficient public interest in the revelation of the material to outweigh any risk. So again, it is a judgement which the court brings.[270]

2.272 Emeritus Professor McDonald argued that, instead of a public interest defence, the onus of proof should include a public interest element:

> There was great concern, particularly amongst privacy advocates, that too much of a burden was being put on claimants or plaintiffs, and that the defendants could just sit back and leave it to the plaintiffs to show everything about their case—remembering that this hurdle of public interest is instead of a defence of public interest. It is something which we felt needed to be brought right up front. It would be quite appropriate that, if

---

[267] Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, p. 4.

[268] Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, p. 4.

[269] Human Technology Institute, University of Technology Sydney, Answers to spoken questions on notice, 22 October 2024 (received 29 October 2024).

[270] Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 54.

> there are facts which ought to be brought to the attention of the court, and if the plaintiff hasn't done so, then the defendant may bring those to the court. Perhaps that is obvious. It is just recognising that the defendant may bring those to the court; the defendant doesn't have to, or may not need to. It may be blindingly obvious that this is a matter of legitimate public interest.[271]

2.273 Emeritus Professor McDonald and Professor Rolph put forward a 'suggested compromise, which goes back to the ALRC recommendation'.[272] That compromise proposed:

> The court may only determine that the plaintiff has a cause of action if the court is satisfied that the public interest in the plaintiff's privacy outweighs any countervailing public interest. A defendant may adduce evidence that there is a countervailing public interest that outweighs the plaintiff's interest in privacy.[273]

2.274 Emeritus Professor McDonald contended that the tort should not:

> …be like a defamation case. In a defamation case, the plaintiff proves that they have been defamed; that's it. They are entitled to a remedy, although now there is a 'serious harm' requirement, which has modified that, importantly. They can say, 'I am entitled to success unless the defendant on the balance of probabilities can prove a defence.' In our design, the court must consider any countervailing public interest up front before the plaintiff can go ahead, or can succeed.[274]

2.275 She clarified:

> We don't say that the plaintiff must persuade the court. We say that the plaintiff only has a cause of action if the court is satisfied. So both parties will have to use persuasion to the court as to whether or not the public interest outweighs the privacy interest.[275]

2.276 In Emeritus Professor McDonald's view, the court should make this decision 'partly because the whole issue of onus is murky—whether you can have an onus about something which is a judgement'.[276]

2.277 If clause 7(3) is redrafted, clause 7(4) should also be redrafted to state that it is a non-exhaustive list of matters the court could take into consideration when considering the public interest test. Amending the bill in that way would bring the statutory tort closer to the model proposed by the ALRC:

---

271 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 54.

272 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 54.

273 Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, pp. 4–5.

274 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 54.

275 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 54.

276 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 22024, p. 55.

> …recommendation 9(3) of the Law Reform Commission report did say that the act should also provide that the plaintiff has the legal onus to satisfy the court that the public interest outweighs any countervailing public interest that is raised in the proceedings. I am departing from that in saying that I think a better way is to say that the court should be satisfied.[277]

2.278 Emeritus Professor McDonald indicated artistic expression should be one of the kinds of public interest that should be included in the bill. She saw 'no explanation' for not including it in the non-exhaustive list of public interests. Artistic expression is:

> …an important aspect of freedom of speech and freedom of expression in many different contexts: plays, films, novels, books and so on. There may be cases where there is sort of intrusion but it's something that has to be balanced.[278]

2.279 The bill would allow a court to grant an injunction that restrains the defendant from invading the plaintiff's privacy.[279] Emeritus Professor McDonald brought to the committee's attention that the section heading of clause 9 of Schedule 2 'is problematic and needs to be changed'. The provision would not limit the court's power 'to an interim injunction'. For that reason, '[t]he word "Interim" should be omitted' from the bill.[280]

2.280 The AGD contended '[t]he drafting of clause 7(3) was intended to give effect to the approach set out in recommendation 9.3 of the ALRC Report 123'. The public interest test:

> …is intended to allow judicial consideration of relevant countervailing public interests. It requires a plaintiff to satisfy the court that the public in their privacy outweighs any countervailing public interests in the invasion of privacy raised by the defendant. It provides that the defendant has the burden of adducing evidence that there is a countervailing public interest for the court to consider. It recognises that the public interest balancing element of the tort will not need to be satisfied in all cases; there may be matters in which competing public interests do not exist and the plaintiff should not need to prove the non-existence of public interests that have not been raised.[281]

2.281 The AGD advised the redrafted version of the clause proposed by Emeritus Professor McDonald and Professor Rolph:

> …removes the evidential burden from the defendant and requires the court to consider any/all countervailing public interests in determining whether

---

277 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, pp. 55–56.

278 Emeritus Professor McDonald, Personal capacity, *Committee Hansard*, 22 October 2024, p. 57.

279 Item 9 in Part 2 of Schedule 2 of the bill.

280 Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney, *Submission 27*, p. 6.

281 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

> the public interest balancing element of the cause of action is made out. The department is now considering how the proposed formulation in the suggested redraft would operate procedurally to ensure the plaintiff is aware of the case it must meet and the court is properly informed of the matters it must consider.[282]

2.282 In relation to the proposal to expressly include 'artistic expression' as a public interest, the AGD advised:

> These amendments could be made but arguably are not technically necessary. The Explanatory Memorandum to the Bill clarifies that freedom of expression includes (among other things) artistic expression and that the public interest in the freedom of the media pertains to the responsible investigation and reporting of matter of public concern and importance.[283]

Doxxing offences

2.283 Participants in the inquiry broadly supported the doxxing offences contained in the bill.[284]

2.284 The Australian Information Industry Association (AIIA), for example, submitted:

> The AIIA commends the government's efforts to address the escalating dangers associated with doxxing. However, while punitive measures such as the proposed statutory tort for serious invasions of privacy and amendments to the Criminal Code Act are a positive development, the focus must also include measures to mitigate harm to victims swiftly and effectively.[285]

2.285 Dr Zirnsak, Uniting Church, observed that the proposed doxxing offences fill a gap in the law and, for that reason, they should be passed:

> The risk always is the danger that somebody is being targeted for harmful behaviour and the legal team who are defending the perpetrator will try to argue the existing offences don't cover it. The more that we can make sure there aren't gaps in the law, the better it is. Our view is that this was filling gaps to make sure that, even if others want to argue you might possibly be able to use another law on some of this, this just makes it really crystal clear and ensures that on these matters of doxxing there will be a very clear and specific piece of law that will allow that behaviour to be addressed.[286]

---

282 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

283 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

284 See, for example: Privacy 108, *Submission 1*, p. 9; Mr Greg Peak, *Submission 2*, pp. [3]–[4]; Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 5*, p. 2; Financial Advice Association of Australia, *Submission 25*, p. 3.

285 Australian Information Industry Association, *Submission 22*, p. [3].

286 Dr Zirnsak, Uniting Church, *Committee Hansard*, 22 October 2024, p. 8.

2.286 The AFP contended that the criminalisation of doxxing 'may deter offenders and will provide a clear message to the community that this conduct is not tolerated'. In its view, '[t]he new offences complement existing offences in the *Criminal Code Act 1995* for using a carriage service to menace, harass or cause offence'.[287]

2.287 While ACCI was not opposed to the introduction of the doxxing offences, it was concerned they could have 'unintended consequences':

> …there may be good reasons to identify someone who is acting anonymously online. Anonymity facilitates a range of abuse and trolling on social media and the internet more broadly. People acting anonymously can bully and harass, issue death threats and threats of sexual abuse all without consequence. It may be that the Bill provides those persons with statutory protection to stay anonymous and continue their abuse of others. Additionally, "doxxing" may be in the public interest – many journalistic investigations have exposed political scandals and corruption by making public private text messages and other modes of communication.[288]

2.288 The Queensland Council for Civil Liberties argued that the doxxing offences should not be passed and should be subjected to 'substantial further consultation'. If the offences are introduced, they should only apply to cases of doxxing where the behaviour 'can be equated to harassment or stalking'.[289]

2.289 The FSU agreed that doxxing should be addressed as it 'can have a chilling effect on public discourse'. In its view, the doxxing provisions:

> …are remarkably expansive in their breadth. They would seemingly cover misgendering, dead-naming, and even pointing out which societies or organisations Politicians frequent…Such criminalisation is inappropriate in a democratic society. The Criminal law should be slow to regulate the dissemination of personal information, given the Freedom of Expression issues that arise.[290]

2.290 The Law Council took a similar stance in relation to the broadness of the term 'doxxing'. It acknowledged that while doxxing can be harmful and deleterious to the wellbeing of individuals:

> …there are instances in which doxxing behaviour is legitimate and should not be circumscribed. For example, doxxing can be part of public interest journalism where it involves the unveiling of private information that exposes contradictory, unethical, or illegal behaviour by public officials or business people.[291]

---

287 AFP, *Submission 71*, p. [1].

288 Australian Chamber of Commerce and Industry, *Submission 65*, p. 2.

289 Queensland Council for Civil Liberties, *Submission 17*, pp. 2–3.

290 Free Speech Union of Australia, *Submission 4*, pp. 1–2.

291 Law Council, *Submission 67*, p. 38.

2.291 To better ensure that the proposed offences are not misused, the Law Council suggested amending the bill to 'provide further guidance on what constitutes 'menacing' or 'harassing' behaviour'.[292]

2.292 The AGD indicated that the terms 'menacing' and 'harassing' are well defined in legislation and are understood by the courts:

> …the concept of menacing and harassing is well established in the Criminal Code, in existing section 474.17, which is 'use of a carriage service to menace or harass'. Those provisions have been in place since 2004. They are routinely prosecuted through the courts.[293]

2.293 Mr Parker Reeve, Assistant Secretary, High Tech Crime Branch, AGD, explained:

> To menace or harass involves conduct that is threatening or repeatedly vexatious to such an extent as to cause—and I think we've set this out in the explanatory memorandum—would cause a person to fear for their safety or limit their ability to go about their daily life. It is a serious threshold, as you would expect for a criminal offence attracting a high maximum penalty, and appropriately so.
>
> That goes to why we have not included a defence of the kind suggested in the offence. I think as we've set out in the explanatory memorandum, the objective requirement that a reasonable person would consider is the conduct to be menacing or harassing—that is, involving threats or vexatious behaviour et cetera—is such that legitimate conduct would not be captured by the offence, in the first instance, and the inclusion of a defence then would provide a permission, an authority, a licence, for people to engage in what is quite harmful behaviour.[294]

Personal data

2.294 Some inquiry participants commented on the definition of 'personal information' used in the Privacy Act and the term 'personal data' that would be introduced into the Criminal Code.[295]

2.295 Privacy 108 indicated that the bill would introduce the term 'personal data' into the Criminal Code. That term would be distinct from the term 'personal information' used in the Privacy Act. It argued in favour of consistency between the Criminal Code and the Privacy Act. The term 'personal information' should be consistently used and 'updated to reflect modern digital realities'. The updated definition should 'include metadata, geolocation data, and digital

---

[292] Law Council, *Submission 67*, p. 38.

[293] Mr Parker Reeve, Assistant Secretary, High Tech Crime Branch, AGD, *Committee Hansard*, 22 October 2024, p. 67.

[294] Mr Parker Reeve, Assistant Secretary, High Tech Crime Branch, AGD, *Committee Hansard*, 22 October 2024, p. 67.

[295] See, for example: Privacy 108, *Submission 1*, p. 9; Mx Rebecca Trapani, *Submission 7*, p. [2];

identifiers such as IP addresses, usernames, and other indirect identifiers, which are currently not comprehensively covered under the Privacy Act'.[296]

2.296 Those reforms 'would ensure clarity and consistency across Australian law'. They would also improve 'both privacy protection and the criminalisation of malicious online behaviours, including doxxing'.[297]

2.297 The FSU argued that the term 'private information' is 'unduly broad'. It argued the 'most appropriate approach' to the criminalisation of doxxing:

> …would be to have a small and complete list of categories. We would expect that residential addresses would cover most doxxing, and possibly home phone numbers. Indecent images are already covered by existing law, as is harassment using a carriage service.[298]

Penalties

2.298 The FSU considered the maximum penalty of seven years imprisonment to be 'disproportionate'. In its opinion, a maximum penalty of one year imprisonment would be more appropriate. It argued that the distribution of 'information that potentially enables an offence should not have a far higher penalty than the offence itself'.[299]

2.299 The application of the penalty should also not be predicated on 'harassment' which, in the FSU's view, 'is too broad for the offence'. Instead, the penalty should only be applied where there is 'a substantial risk of physical harm to an individual, which is the main legitimate concern with doxxing'.[300]

2.300 The AGD explained that the maximum penalty for using a carriage service to make personal data available would be six years' imprisonment. The penalty would be higher than that associated with using a carriage service to menace, harass or cause offence to reflect 'the serious harms caused by doxxing, the potentially enduring nature of these harms, and the significant steps that a victim may need to take to mitigate these harms'.[301]

2.301 Similarly, the proposed penalty for using a carriage service to make personal data available about members of certain groups would be seven years' imprisonment. The penalty would be higher to reflect:

> …the seriousness of such conduct. Doxxing persons because of a belief that they are part of a group that shares one or more protected attributes is

---

296 Privacy 108, *Submission 1*, p. 9.

297 Privacy 108, *Submission 1*, p. 9.

298 FSU, *Submission 4*, p. 2. Also see: Criminal Code s. 471.17 and 471.17A.

299 FSU, *Submission 4*, p. 2.

300 FSU, *Submission 4*, p. 2.

301 AGD, *Submission 31*, p. 8.

> particularly serious in nature, as it is likely to instil fear or anxiety in victims where there is a history of, or ongoing, persecution or prejudice and can encourage or incite other persons who share discriminatory views in relation to the protected group to engage in similar menacing or harassing conduct towards the victims.[302]

Future privacy reforms

2.302 Several inquiry participants highlighted the government's intention to introduce a second tranche of privacy reforms.[303]

2.303 Those participants mainly focused on the:

- timeline for future consultation and reform;
- small business exemption;
- fair and reasonable test;
- controller-processor distinction; and
- definition of personal information.

Timeline for future consultation and reform

2.304 Some participants in the inquiry suggested the government introduce the second tranche of privacy reforms as soon as possible or commit to a timeline for their introduction.

2.305 For example, the AIIA highlighted considerable concern within the digital technology industry about the time it has taken to introduce reforms to the Privacy Act:

> The government's apparent proposal to introduce two tranches of reforms, with the present Bill representing the first tranche, is a cautious step forward. However, we remain concerned that deferring critical reforms to a potential second tranche has fostered cynicism within the industry…[T]his approach has been viewed as timid and insufficient in addressing the pressing need for comprehensive privacy reforms. The delay in updating the Privacy Regime risks leaving Australian citizens vulnerable to privacy breaches, while businesses are left without clear guidance on their obligations.[304]

---

302 AGD, *Submission 31*, p. 8.

303 See, for example: BSA, *Submission 6*, pp. 6–7; Mx Trapani, *Submission 8*, pp [1]–[2]; Consumer Policy Research Centre, *Submission 20*, p. 1; CHOICE, *Submission 21*, p. [2]; Food for Health Alliance, *Submission 33*, p. 2; Dr Lisa Archbold et al, *Submission 34*, p. 1; Electronic Frontiers Australia, *Submission 44*, p. 2; DRW, *Submission 50*, p. [4]; Access Now, *Submission 55*, p. 2; HRLC, *Submission 60*, p. 13; Australian Communications Consumer Action Network, *Submission 64*, p. 3; Mr Angus Murray & Dr Monique Mann, *Submission 70*, p. [1].

304 Australian Information Industry Association, *Submission 22*, p. [2].

2.306 Reset.Tech Australia argued further reforms:

> …are vital to ensuring Australia's privacy framework is fit for the digital era, especially including the updates to the definition of personal data and the inclusion of the fair and reasonable test for processing data.[305]

2.307 Some of those reforms will also strengthen privacy protections for children and have 'the capacity to be far more protective for children than a children's code'.[306]

2.308 Reset.Tech Australia recognised that the first tranche of reforms would take 'some vital first steps that are necessary to updating Australia's privacy framework'. It did not see any 'reason to delay or impede the progress of these proposed reforms'.[307]

2.309 The HTI similarly viewed the bill 'as an important first step in reforming the Privacy Act. This reform is long overdue, and much more is needed to modernise Australia's privacy law for the 21st century'.[308]

2.310 The HTI encouraged the government:

> …to commit publicly to a clear and specific timeline for introducing the next bill. This timeline should be as expeditious as possible, noting that many of the reforms have been the subject of extensive public and broader stakeholder consultation – some going back almost two decades. Hence, this Committee should recommend that the Government commit to introducing the second reform bill to the Australian Parliament no later than six months after the forthcoming federal election.[309]

2.311 The next tranche of privacy reforms 'should incorporate the remaining recommendations that were agreed to, or agreed in principle, by the Government in its *Response to the Privacy Act Review Report*'.[310]

2.312 BSA recommended the publication of exposure drafts of future privacy bills to allow for public consultation ahead of their introduction to Parliament.[311]

2.313 Similarly, auDA - .au Domain Administration Ltd 'encourage[d] the Government to consider the need for certainty for Australian businesses on what future regulatory or legislative steps are planned'. Future consultation

---

305 Reset.Tech Australia, *Submission 3*, p. 6.

306 Reset.Tech Australia, *Submission 3*, p. 6.

307 Reset.Tech Australia, *Submission 3*, p. 6.

308 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [4].

309 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [7].

310 Human Technology Institute, University of Technology Sydney, *Submission 13*, p. [8].

311 BSA, *Submission 6*, p. 7.

should include multiple stakeholders and provide 'an adequate timeframe for consideration and response'.[312]

2.314 Professor Handsley, CMA, expressed concern about amending the bill to include tranche two reforms at this stage:

> I would have some slight concerns about the process of adding things in that would otherwise be tranche 2 that haven't been subject to the same consultation process these particular reforms have…[W]e wouldn't have had the opportunity to comment on them and we might not agree with precisely what the parliament was proposing to do.[313]

2.315 While it appreciated that incorporating additional reforms into the bill 'is likely to be practically difficult', the HTI proposed that the definition of personal information be expanded. The Privacy Act Review Report recommended that the term be expanded to make clear:

> …personal information is an expansive concept[314]

2.316 DRW stated that the second tranche of privacy reform should not impede passage of the bill:

> …there is a real urgency around privacy reform. In part, that's because the current act is so significantly out of date. We are out of line with comparable jurisdictions from a basic privacy rights perspective. Of course, the public largely support these measures to the extent they've been asked.[315]

2.317 Professor Santow, HTI, shared Ms O'Shea's view about passing the first tranche of privacy reforms as soon as possible:

> In a perfect world, of course, all 100-plus recommendations that the federal government has committed to should be in a single bill, but we don't live in a perfect world…The sad history of privacy reform in Australia, particularly over the last 19 years, has been that government has found it very, very difficult to progress to a bill, let alone to actually enact the bill, so I would treat stakeholders who are saying, 'We haven't been properly consulted. This has all been foisted upon us. It's all new information to us,' with some real scepticism.[316]

2.318 EFA opined that splitting the privacy reforms into tranches has potential benefits for the businesses that will need to implement compliance changes:

> …it's essential this bill pass. Understandably, from a business perspective, it's been put into two tranches, because the other approach would have been a big bang change—very expensive and very difficult for business to pass. So this is actually quite intelligent, from a business perspective, even

---

312 auDA - .au Domain Administration Ltd, *Submission 11*, p. 2.

313 Professor Elizabeth Handsley, President, CMA, *Committee Hansard*, 22 October 2024, p. 6.

314 Human Technology Institute, University of Technology Sydney, *Submission 13*, pp. [14]–[15].

315 Ms O'Shea, DRW, *Committee Hansard*, 22 October 2024, p. 25.

316 Professor Santow, HTI, *Committee Hansard*, 22 October 2024, p. 25.

> wearing my civil society hat. But it's critical that we get some promise from the current government to enact a bill within six months of the election or get some sort of promise around tranche 2 not going off into 2027 or something like that.[317]

2.319 While the Law Council was pleased there will be a second tranche of privacy reforms, it:

> …call[ed] for a roadmap, or strategy, to publicly detail how these reforms will be progressed—similar to the materials that the Government issued in 2023 for the *Security of Critical Infrastructure Act 2018*.[318]

2.320 That information would 'promote much-needed certainty for the multitude of sectors that expect to be impacted by these significant changes'.[319]

2.321 The AHRC welcomed the bill but indicated it failed to include 'many of the needed reforms'. It was particularly disappointed it did not 'include the 'fair and reasonable test', which would operate as a 'shield' against excessive data collection'.[320]

2.322 The AHRC recommended the government provide 'a clear timeline for when each 'agreed' and 'agreed in principle' amendment will be introduced in future tranches'.[321]

2.323 The OAIC agreed a second tranche of reforms is required and saw the bill as 'an important first step in strengthening Australia's privacy framework'.[322]

2.324 Ms Carly Kind, Privacy Commissioner, elaborated by explaining the bill would 'fundamentally contribute to the range of regulatory levers we have as an effective regulator and enable us to respond effectively to privacy harms and emerging threats in a strategic and proportionate way'.[323]

2.325 While Ms Kind argued that the bill should be passed, she suggested the next tranche of privacy reform should be developed urgently. Further reform is required quickly 'to keep ahead of the privacy threats and advancing skills of malicious cyberactors'.[324]

---

317 Mr Pane, EFA, *Committee Hansard*, 22 October 2024, pp. 25–26.

318 Law Council, *Submission 67*, p. 17.

319 Law Council, *Submission 67*, p. 17.

320 AHRC, *Submission 36*, p. [3].

321 AHRC, *Submission 36*, p. [3].

322 OAIC, *Submission 23*, p. 1.

323 Ms Carly Kind, Privacy Commissioner, OAIC, *Committee Hansard*, 22 October 2024, p. 60.

324 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, p. 60.

2.326 Ms Celeste Moran, First Assistant Secretary, Integrity Frameworks Division, AGD, stated:

> The government is implementing its privacy reform agenda in a measured and considered way.
>
> …
>
> The bill implements a first tranche of proposals from the government's response to the Privacy Act review ahead of further work towards the second package of reforms. The Attorney-General has stated publicly that the department will develop the next tranche of privacy reform for targeted consultation, including draft provisions in the coming months. We have commenced work towards this.[325]

2.327 The AGD similarly explained the importance of passing the bill prior to the introduction of further privacy reforms:

> The Bill provides individuals with greater protection, transparency and control over their privacy. These protections are vital to the Government's broader agenda to ensure Australian's personal information is safe and secure and is used responsibly and in the interests of the Australian community. The Government will continue advancing a further package of privacy reforms based on proposals from the Review that were agreed in-principle, through further targeted consultation with stakeholders on draft provisions.[326]

2.328 The AGD stated it:

> …will undertake targeted consultation on draft provisions to progress the outstanding legislative proposals from the Government response to the Review, which will ensure the details of an updated privacy framework for the digital age are appropriate and workable in a diverse range of contexts.[327]

2.329 The consultation would add to:

> …the extensive consultation to date with a broad range of stakeholders interested in protecting Australian's privacy and will ensure that the right balance is struck between protecting people's personal information, and allowing it to be used and shared in ways that benefit individuals, society and the economy. The targeted consultation will inform the Government's decision making on next steps in relation to Privacy reforms.[328]

2.330 Ms Moran indicated that consultation would be undertaken:

> …with entities including industry, tech organisations, small businesses, the media and civil society as well as experts in academia and peak bodies. This

---

[325] Ms Celeste Moran, First Assistant Secretary, Integrity Frameworks Division, AGD, *Committee Hansard*, 22 October 2024, pp. 59–60.

[326] AGD, *Submission 31*, p. 2.

[327] AGD, *Submission 31*, p. 9.

[328] AGD, *Submission 31*, p. 9.

> is intended to avoid unintended consequences and ensure the right balance is struck between protecting people's personal information and allowing it to be used and shared in ways that benefit individuals, society and the economy.[329]

2.331 The AGD anticipated beginning the consultation process on draft provisions before the end of 2024. However, '[t]he final make up and timing for any second package of reforms will be informed by this consultation and is ultimately a matter for the government'.[330]

Small business exemption

2.332 Some inquiry participants called for the removal of the small business exemption.[331]

2.333 Under the small business exemption, around 95 per cent of Australian businesses are not required to comply with the Privacy Act.[332] CHOICE indicated that includes 'high risk organisations like real estate firms'.[333]

2.334 Mr Rafi Alam, Senior Campaigns and Policy Advisor, CHOICE, shared the results of research conducted in December 2023:

> …our polling found that 65 per cent of consumers did not trust businesses to use their data responsibly and in their best interest; 78 per cent were concerned about businesses selling their personal information to data brokers; and 70 per cent were concerned about their data being used in automated decision-making. Sadly, this widespread lack of trust in businesses is warranted. Across many sectors, businesses have failed to demonstrate their ability to self-regulate and protect personal information, and consumers have paid the price.[334]

2.335 Mr Alam highlighted that there is broad consumer support for the repeal of the small business exemption. According to polling conducted by CHOICE, '83 per cent of people agreed that small businesses should be required to follow privacy laws'.[335]

---

329 Ms Moran, AGD, *Committee Hansard*, 22 October 2024, p. 60.

330 Ms Moran, AGD, *Committee Hansard*, 22 October 2024, p. 60.

331 See, for example: Mx Rebecca Trapani, *Submission 7*, p. [2]; Consumer Policy Research Centre (CPRC), *Submission 20*, p. 1; CHOICE, *Submission 21*, p. [1]; Per Capita, Centre of the Public Square, *Submission 35*, p. 2; Electronic Frontiers Australia, *Submission 44*, p. 5; Digital Rights Watch, *Submission 50*, p. [7]; Human Rights Law Centre, *Submission 60*, p. 13; Australian Communications Consumer Action Network, *Submission 64*, p. 3;

332 Mx Rebecca Trapani, *Submission 7*, p. [2]; CHOICE, *Submission 21*, p. [1].

333 CHOICE, *Submission 21*, p. [1].

334 Mr Rafi Alam, Senior Campaigns and Policy Advisor, CHOICE, *Committee Hansard*, 22 October 2024, p. 44.

335 Mr Alam, CHOICE, *Committee Hansard*, 22 October 2024, p. 45.

2.336 The Consumer Policy Research Centre argued the removal of the exemption 'would ensure all businesses who collect, share and use consumer data are held accountable to treat people's data with care and respect'.[336]

2.337 Ms Rosie Thomas, Director of Campaigns, CHOICE, referred to research that examines the privacy practices of 'the 'rent tech' sector; that is, third-party rental applications'. The research conducted by CHOICE found:

> Broadly, a large number of businesses there collect large amounts of data. We cannot definitively say whether they are small businesses; that is part of the challenge. From a consumer's perspective, they have no way to know whether the business that is collecting large amounts of their personal data for rental applications or for other reasons is subject to the Privacy Act. It is an example of a sector where it is likely that the Privacy Act is not always applying, yet they are dealing in large amounts of personal information.[337]

2.338 Ms Thomas reported that CHOICE 'supported a proportionate approach to regulation'. It:

> …would be open to calibrating the obligations in a way that is proportionate to the risk, while recognising that businesses might need time to transition, an appropriate transition period, and appropriate resourcing for the OAIC to be able to help and educate business on this journey. Fundamentally, it isn't acceptable that well over 90 per cent of the businesses in the country are not captured by the Privacy Act at the moment.[338]

2.339 Mr Jordan Carter, Internet Governance and Policy Director, auDA, indicated that the vast majority of small businesses surveyed by his organisation support stronger privacy regulations.[339]

2.340 Ms Elizabeth O'Shea, Chair, DRW, argued that the exemption can be damaging to small businesses. She explained that while there are some small businesses that do not treat their customers privacy carefully:

> …there's a lot of small businesses who I think want to do the right thing by their customers and actually end up being sold substandard products form a cybersecurity perspective because they don't have that requirement to comply with the Privacy Act, and I would say there is significant benefit that would come to small business from an elevation in the standards of handling personal information that would improve the experience. It would mean off-the-shelf products sold to small business and purchased by them which they use on daily basis would adhere to a higher standard of privacy protection, which is a good thing. We shouldn't be creating a situation where small business has to contend with substandard products because the people selling them know the standards are low, so I think there's a lot of

---

336 CPRC, *Submission 20*, p. 1.

337 Ms Rosie Thomas, Director of Campaigns, CHOICE, *Committee Hansard*, 22 October 2024, pp. 45–46.

338 Ms Thomas, CHOICE, *Committee Hansard*, 22 October 2024, p. 49.

339 Mr Jordan Carter, Internet Governance and Policy Director, .au Domain Administration Ltd, *Committee Hansard*, 22 October 2024, p. 15.

> benefit that would come from the removal of that exemption. It's not all downsides.[340]

2.341 The AIIA acknowledged 'that all businesses, regardless of size, should be held accountable for protecting the privacy of Australians and their personal and sensitive information'. The small business exemption:

> …not only heightens the risk to individuals but also overlooks the significant role these businesses play in the broader digital economy, forming 97% of businesses in Australia and contributing approximately one-third of Australia's [gross domestic product].[341]

2.342 Mr John Pane, Chair, EFA, supported the removal of the small business exemption arguing it is an anachronistic measure that does not align with privacy legislation overseas. In all privacy legislation that has developed since the 1990s:

> …there is no similar or equivalent exception for small businesses. In fact GDPR also applies to small businesses. Small businesses have adapted, and with regard to economic and other impacts there has not been any significant negative reporting. Time have changed, particularly since the year 2000, when the national privacy principles were first drafted. We now have digitally enabled businesses that don't have a shopfront. They're all online, and so is our data. That's why it's important to ensure that the data is protected, that Australians have rights in relation to their data and that small businesses who process and collect that data have obligations to manage it and protect it.[342]

2.343 COSBOA assured the committee:

> Small businesses of all sizes already actively process data with appropriate care and concern, many of which already have a turnover of over $3 million and are therefore already subject to the Act.[343]

2.344 If small businesses with an annual turnover of less than $3 million were required to comply with all APPs it would undermine 'the viability of those businesses already facing a laundry list of increased red tape and regulation'.[344]

2.345 Mrs Adele Sutton, Head of Policy and Advocacy, COSBOA, explained the small business 'exemption was introduced as recognition of the significant additional compliance burden facing small businesses without the extensive resources available to large companies'. She observed that 'small businesses with turnovers between three and $10 million are required to comply with the

---

340 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 22 October 2024, p. 24.

341 Australian Information Industry Association, *Submission 22*, p. [2].

342 Mr John Pane, Chair, Electronic Frontiers Australia, *Committee Hansard*, 22 October 2024, p. 23.

343 Council of Small Business Organisations Australia (COSBOA), *Submission 46*, p. 1.

344 COSBOA, *Submission 46*, p. 1.

Privacy Act'. If the proposed amendments are passed, those small businesses will be required to comply with them.[345]

2.346 Exemptions for small businesses exist in similar legislation in foreign jurisdictions. For example:

> …under the GDPR, although it applies to small business, there are specific exemptions within that European legislation from certain types of principles. For example, I don't believe that businesses with less than 250 employees necessarily need a data protection officer.[346]

2.347 Mrs Sutton clarified the GDPR does not contain an exemption for small businesses, but there are exemptions for small businesses from compliance with some of its provisions. In the Australian context:

> For a small business, particularly a sole trader, without guidance as to what they need and what they can practically do to comply—and we haven't got the figures as to how much compliance with all 13 [APPs] would cost—what does this look like? Our understanding is that it is cost prohibitive to comply with such a broad brush of [APPs] without assistance and guidance.[347]

2.348 Mrs Sutton, stated:

> …COSBOA is relieved that small businesses with turnovers under $3 million, including 1.1 million sole traders, appear to have been spared further complexity due to the government's decision not to proceed with the removal of the small business exemption from the Privacy Act.[348]

2.349 The Financial Advice Association of Australia urged caution on proposals to increase the regulation of businesses, particularly those engaged in the provision of financial advice.[349]

2.350 The AIIA proposed a middle course between rescinding the small business exemption and maintaining the status quo. It argued small and medium enterprises (SMEs) do not necessarily have to comply with the same legislative requirements as large businesses. The AIIA proposed 'penalties could be tailored for SMEs, providing them with a longer implementation timeframe to ensure compliance'.[350]

---

345 Mrs Adele Sutton, Head of Policy and Advocacy, Council of Small Business Organisations Australia (COSBOA), *Committee Hansard*, 22 October 2024, pp. 37–38.

346 Mrs Sutton, COSBOA, *Committee Hansard*, 22 October 2024, p. 38.

347 Mrs Sutton, COSBOA, *Committee Hansard*, 22 October 2024, p. 41.

348 Mrs Adele Sutton, Head of Policy and Advocacy, Council of Small Business Organisations Australia, *Committee Hansard*, 22 October 2024, p. 37.

349 Financial Advice Association of Australia, *Submission 25*, p. 1.

350 Australian Information Industry Association, *Submission 22*, p. [2].

2.351 Small businesses with an annual turnover of $3 million or less are exempt from the Privacy Act. It was considered that extending the Privacy Act to these businesses would place an unreasonable burden on them that is not proportionate to the privacy risk these businesses pose. The government agreed in-principle that the small business exemption should be rescinded. However, further consultation with affected stakeholders is required before that occurs.[351]

Controller-processor distinction

2.352 Some inquiry participants expressed disappointment that the bill did not include provisions that address the controller-processor distinction.[352]

2.353 BSA suggested the bill be amended to introduce the controller-processor distinction. If it is not possible to make that amendment, it 'strongly urge[d] any subsequent tranches of reform to prioritise introducing this distinction due to how fundamental it is to the function and structure of a privacy law'.[353]

2.354 The Tech Council stated the introduction of the distinction should be prioritised. It explained the difference between controllers and processors:

> Controllers own the end-user relationships and are generally the first point of contact for individuals who wish to exercise their rights. They have the primary responsibility for ensuring compliance with privacy laws. This includes obtaining valid consent and responding to individual requests…[P]rocessors have responsibilities to comply with controller instructions, implement appropriate security measures, and ensure that any sub-processors are also in compliance with applicable privacy laws.[354]

2.355 BSA explained the controller-processor 'distinction has existed for more than 40 years and is foundational to privacy laws worldwide'. Privacy frameworks in foreign jurisdictions reflect 'the different roles of controllers (which decide how and why to process personal data) and processors (which handle personal data on behalf of other companies and pursuant to their instructions)'.[355] By distinguishing between controllers and processors 'a privacy law can better craft obligations that fit both types of organisations'.[356]

---

351 Attorney-General's Department, *Government Response Privacy Act Review Report*, September 2023, p. 6.

352 See, for example: BSA | The Software Alliance (BSA), *Submission 6*, pp. 1–2; Australian Information Industry Association, *Submission 22*, p. [2]; Tech Council of Australia, *Submission 49*, p. 3;

353 See, for example: BSA, *Submission 6*, pp 6–7.

354 Tech Council of Australia, *Submission 49*, pp. 3–4.

355 Note: the privacy frameworks from foreign jurisdictions include: the European Union's General Data Protection Regulation, the Californian Consumer Privacy Act, the Japanese Act on the Protection of Personal Information, and the Singaporean Personal Data Protection Act, see: BSA, *Submission 6*, p. 3.

356 BSA, *Submission 6*, p. 3.

2.356 Ms Erika Ly, Policy Manager, Tech Council of Australia, further explained the helpfulness of making a distinction between data controllers and processors:

> When we're starting to think about how we may necessarily apply privacy obligations in the context of automated decision-making, being able to clarify the roles of controller and processor folks who are operating across the technology stack becomes very important, because it clarifies the appropriate entity that then will apply the disclosure notices for automated decision-making. At the moment in terms of our read of those particular provisions, it is fairly unclear.[357]

2.357 The inclusion of that distinction in the Privacy Act would 'not only align Australia's privacy law with other international laws and frameworks, but also, provide much-needed clarity for businesses and consumers'.[358]

2.358 Introducing the distinction into legislation:

> …would increase the efficiency of the Privacy Act by allocating responsibilities relating to notification, consent, and security. The clear separation between controllers and processors forms a fundamental aspect of effective privacy frameworks worldwide, including the European Union's GDPR. The AIIA cautions that a failure to provide a clear delineation between these concepts would result in an inability to clearly define responsibilities in the management of personal data.[359]

2.359 Mr Godber understood that the controller/processor distinction:

> …would apply to the tranche 2 provisions, which we also understand are reasonably advanced. The introduction of a controller and processor distinction is just one of a number of fundamental reforms that we are expecting in tranche 2 that critically will make Australia's privacy regime interoperable with key regimes overseas.[360]

2.360 In its response to the Privacy Act Review Report, the government stated:

> Complexity and regulatory burden for entities acting as 'processors' would likely increase following reforms proposed in the Report. To recognise that different entities have differing degrees of control over the handling of personal information, the Government agrees in-principle that a distinction between controllers and processors of personal information should be introduced into the Privacy Act (proposal 22.1). This will bring Australia into line with other jurisdictions, reflect the operational reality of modern

---

357 Ms Erika Ly, Policy Manager, Tech Council of Australia, *Committee Hansard*, 22 October 2024, p. 11.

358 BSA, *Submission 6*, p. 2.

359 Australian Information Industry Association, *Submission 22*, p. [2].

360 Mr Harry Godber, Head of Policy and Strategy, Tech Council of Australia, *Committee Hansard*, 22 October 2024, p. 11.

> business relationships, and reduce the compliance burden for entities acting as processors.[361]

Updating the definition of personal information

2.361 Some inquiry participants called for an updated definition of 'personal information'.

2.362 EFA argued the definition of 'personal information has not kept pace with technological advances'. To remain relevant and protect people's identity, it needs 'to include online tracking technologies, individuation, the use of location data, face and voice recognition, and other emerging methods of identifying individuals'.[362]

2.363 Ms Chandni Gupta, Deputy Chief Executive Officer and Digital Policy Director, CPRC, argued privacy reform should include an update to the kinds of data that are included in 'personal information'. She gave the example of location data:

> We haven't specifically had anything from government about why or why not, or what is included or not included. However, we do believe it is those points of data, such as location data, that are very much personal to you. If you think about it, your journey and your different locations that you visit across a day are very much specific to you, and there is probably no other person that follows your pathway in the same way.[363]

2.364 CPRC argued that this kind of data, even if it is anonymised or not associated with your name in any way, would be 'easy to re-identify because of how unique our map is. You do not need to know who the person is. Businesses can very easily single you out'. The definition of personal information that was drafted in 1988:

> …would have been enough to protect us, but it's not 1988. At that time there had only been one data breach, which was the Morris Worm, and we know now that there are multiple data breaches every year. We are living in a very different time.[364]

2.365 For that reason, the definition of 'personal information' should be modernised.[365]

---

361 Attorney-General's Department, *Government Response: Privacy Act Review Report*, 28 September 2023, p. 15.

362 Electronic Frontiers Australia, *Submission 44*, p. 4.

363 Ms Chandni Gupta, Deputy Chief Executive Officer and Digital Policy Director, CPRC, *Committee Hansard*, 22 October 2024, p. 48.

364 Ms Chandni Gupta, Deputy Chief Executive Officer and Digital Policy Director, CPRC, *Committee Hansard*, 22 October 2024, p. 48.

365 Ms Chandni Gupta, Deputy Chief Executive Officer and Digital Policy Director, CPRC, *Committee Hansard*, 22 October 2024, p. 48.

2.366 Professor Santow, HTI, called for a broadening of the term 'personal information'. He suggested the term should include information such as IP addresses, device identifiers, and geolocation data. That information 'should fall within that subset of personal information known as sensitive information' as it has the potential 'to cause quite serious harm'. The Privacy Act already makes a distinction between personal and sensitive information.[366]

2.367 Ms O'Shea, DRW, argued that the technology industry should not be surprised by reform to the definition of personal information:

> Industry have been involved in this consultation process. They've had their say and they've participated in this throughout. This is not a novel proposal. They are also, I think, on notice that they require a social licence to operate, and, at present, polling surveys of the Australian public show support for stronger privacy protections over their personal information. The element of surprise is not there, I think, from the perspective of this process or in general, in terms of social attitudes to privacy.[367]

2.368 Mrs Lorraine Finlay, Human Rights Commissioner, expressed the AHRC's disappointment that the bill did not include more of the reforms from the Privacy Review that the government had agreed, or agreed in principle, to where not included in the bill. The bill should have included 'a fair and reasonable test which would serve to strengthen privacy protections in the modern era'.[368]

2.369 Ms Kind, OAIC, agreed that the introduction of a fair and reasonable test and an updated definition of personal information should be prioritised. Broadening the definition of personal information 'would greatly expand our ability to be an effective regulator'.[369]

2.370 She suggested there is legal uncertainty about the definition of 'personal information':

> …there has been some legal uncertainty for some time in the aftermath of a case, Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4, which has left some legal uncertainty about the definition of 'personal information'.[370]

---

366 Professor Edward Santow, Co-Director, Human Technology Institute, University of Technology Sydney, *Committee Hansard*, 22 October 2024, pp. 21–22.

367 Ms O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 22 October 2024, p. 22.

368 Mrs Lorraine Finlay, Human Rights Commissioner, AHRC, *Committee Hansard*, 22 October 2024, p. 60.

369 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, p. 60.

370 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, pp. 69–70.

2.371 Broadening the definition and making it clearer would:

> …take away that uncertainty, aid the regulated community in being clear about what their obligations are and aid our office in unqualified enforcement with respect to the kinds of personal information that might not instinctively be classified as personal information but which would relate to an individual as that broader definition proposes.[371]

2.372 Ms Kind also argued the introduction of a fair and reasonable test would provide:

> …a way to raise the general standard of personal information handling across the economy, and would address the current power imbalance inherent in the existing framework by shifting the responsibility to businesses and organisations to proactively consider the impact that their data-handling practices may have on individuals.[372]

2.373 The introduction of that test would modernise Australian privacy legislation in line with community expectations as it:

> …would change and also level up the nature of the obligations in the Privacy Act, commensurate with the kinds of harms and challenges we see, particularly in the digital economy. At the moment, the Privacy Act regime really focuses on the collection of personal information as the relevant process to regulate and control. What the fair and reasonable test gives us is a way to also try to ensure that the ways in which personal information are being used are consistent with community expectations and the interests of the individuals. We think that that's really the linchpin of bringing Australia's privacy regime into the 21st century.[373]

2.374 Mrs Finlay argued there is no reason to delay the introduction of these reforms:

> …while public policy requires consultation, there has been consultation on this point…[I]t is something that has been discussed for a lengthy period of time. While we certainly understand the need to proceed in a measured and considered way, we would say there is also a need to proceed in a timely way, and we would like to see a clear timetable in terms of when that reform and others will be progressed.[374]

2.375 Ms Catherine Fitch, Assistant Secretary, Privacy Reform Taskforce, Integrity Frameworks Division, stated the AGD understands the importance of revisiting the definition of personal information and introducing a fair and reasonable test. In the AGD's view:

> …they both clearly do assist in providing an upgraded baseline standard for personal information. The government at this stage has committed to

---

371 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, p. 70.

372 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, p. 61.

373 Ms Kind, OAIC, *Committee Hansard*, 22 October 2024, p. 70.

374 Mrs Finlay, AHRC, *Committee Hansard*, 22 October 2024, p. 61.

> progressing the remaining agreed-in-principle proposals, of which those were two, in a second package.

2.376 The rationale for introducing the reforms in two tranches was based on stakeholder feedback during the consultation phase. As Ms Fitch explained:

> …this first tranche bill was really intended to address areas where reform had been identified as urgent and can be progressed largely without a direct or significant regulatory impact on entities. The reason for that I think is that the government's seeking to balance an uplift in privacy protection with a reasonable and proportional impact on entities. In our consultations to date, several stakeholders have made clear that they would welcome the things that directly impact them being progressed in one group.
>
> …
>
> …the government has made clear that it does seek to do another tranche of reform and, in certain cases, that requires further consultation on the detail of the draft proposals.[375]

Committee view

2.377 The bill would enact a first tranche of reforms to the *Privacy Act 1988* agreed by the government in its Response to the Privacy Act Review. The bill would also introduce a new statutory tort for serious invasions of privacy and targeted criminal offences to respond to doxxing.

2.378 Multiple civil society organisations told the committee that privacy reform is overdue. They did not support delaying the bill to incorporate further reforms.

2.379 The committee heard evidence from children's advocacy organisations. They highlighted the importance of including children's views in the design of the Children's Online Privacy Code. Given the logistical difficulties associated with consulting children, the committee considers that the 40-day consultation period is insufficient. To gain meaningful input from children, the committee recommends the Information Commissioner consult stakeholders over a minimum of 60 days.

Recommendation 1

2.380 The committee recommends that the minimum consultation period for the Children's Online Privacy Code is extended to at least 60 days.

2.381 The committee received evidence from representatives of a broad range of industries. Many of them indicated a strong desire to engage in the development of the Children's Online Privacy Code. While the bill would allow the Information Commissioner to consult with industry on the development of that code, the committee is of the view that the commissioner should be required to engage in that consultation to ensure that all relevant stakeholders are consulted

---

375 Ms Fitch, AGD, *Committee Hansard*, 22 October 2024, p. 61.

on the design of the code. Input from a wide range of stakeholders would help to ensure the COP Code is fit for purpose and technically feasible.

Recommendation 2

2.382 The committee recommends that the bill is amended to include a requirement for the Information Commissioner to consult with relevant industry bodies or organisations when developing the Children's Online Privacy Code.

2.383 The ABC and the Special Broadcasting Service drew the committee's attention to a possible drafting error in the bill. The Attorney-General's Department confirmed the provision that would permit national broadcasters, such as the ABC and Special Broadcasting Service, to access personal information during declared emergencies was a drafting error. On that basis, the committee recommends that the error is rectified.

Recommendation 3

2.384 The committee recommends the exclusion for media organisations from accessing personal information during declared emergencies is extended to exclude national broadcasters such as the ABC and Special Broadcasting Service.

2.385 The bill would provide the Information Commissioner with the power to issue infringement notices to entities subject to the Australian Privacy Principles that have not complied with their obligations. The committee understands these provisions would not necessarily explain to the affected entity what steps could be taken to remedy their breach of the principles. The committee is concerned that without the power to issue a discretionary notice in the first instance, the bill could disincentivise entities from engaging in open and consultative dialogue with the Office of the Information Commissioner.

Recommendation 4

2.386 The committee recommends that the bill is amended to empower the Information Commissioner to issue a discretionary notice to an entity to remedy an alleged breach of one or more of the provisions in section 13K before issuing an infringement notice.

2.387 The bill would require Australian Privacy Principle entities to include information in their privacy policies about how personal information is used in automated decision making processes. The committee received evidence that the provision could compromise sensitive business information and potentially stifle innovation. The committee considers it appropriate that sensitive commercial information is protected.

Recommendation 5

2.388 The committee recommends that the Explanatory Memorandum to the bill is amended to make clear that the level of information required in privacy policies is not expected to compromise commercial-in-confidence information about automated decision-making systems.

2.389 The committee acknowledges concerns raised about the public interest test outlined in clause 7 of the bill, particularly those discussed by Emeritus Professor Barbara McDonald and Professor David Rolph. The committee is of the view that a defendant should not be required to adduce evidence of a public interest in every case and that the court should be required to consider countervailing public interests in determining whether the statutory tort cause of action is made out. The committee also considers that the bill should make clear that 'artistic expression' is a form of freedom of expression.

Recommendation 6

2.390 The committee recommends that the Commonwealth government considers amending clause 7 of the bill to:

- **require a court to consider the matters of public interest that justify the invasion of the plaintiff's privacy;**
- **not require a defendant to adduce evidence of public interest in every case; and**
- **provide that 'artistic expression' is a form of freedom of expression.**

2.391 The committee received evidence that the journalism exemption from the statutory tort for serious invasions of privacy should be broadened to include a wider range of journalistic activities. In the committee's view, individuals involved in the publication, re-publication or distribution of journalistic material should also be exempt from the tort.

Recommendation 7

2.392 The committee recommends that the Commonwealth government considers amending Schedule 2 of the bill to ensure that the journalism exemption applies to a person involved in the publication, re-publication or distribution of journalistic material.

2.393 The bill would exempt journalism that comprises commentary or opinion on, or analysis of, news, current affairs or a documentary from the statutory tort for serious invasions of privacy. The committee is concerned that the bill would not provide adequate certainty that editorials are a form of journalistic material. In the committee's view, editorials are journalistic material and should therefore be exempt from the tort.

Recommendation 8

2.394 The committee recommends that Schedule 2 of the bill is amended to make clear that the concept of 'journalistic material' for the serious invasions of privacy tort includes 'editorial' material.

2.395 Clause 9(1) of the bill would allow a court to grant an injunction restraining the defendant from invading the plaintiff's privacy. That power is not limited to interim injunctions as the section title suggests. The bill should be amended to make it clear that this power is not limited to the issuance of an interim injunction.

Recommendation 9

2.396 The committee recommends that Schedule 2 is amended to make clear that the power conferred on a court to issue an injunction is not limited to an 'interim' injunction.

Recommendation 10

2.397 Subject to the preceding recommendations, the committee recommends that the Senate passes the bill.

Senator Nita Green
Chair

Additional comments by Deputy Chair Senator Paul Scarr

Introduction

1.1 The bill deals with three discrete issues; namely:

- Privacy reforms implementing various amendments following the Privacy Act Review (Schedule 1);
- Enactment of a statutory tort for serious invasions of privacy into the *Privacy Act 1988* (Privacy Act) (Schedule 2); and
- Introduction into the *Criminal Code Act 1995* (Criminal Code) of a criminal offence for so-called doxxing offences (Schedule 3).

1.2 Prior to providing comments on the bill, there are a number of legislative process issues which (once again) require comment.

Deficiencies in legislative process

Preliminary remarks

1.3 Followers of the work of the committee will note the similarity of many of the below comments to those made in previous inquiry reports.

1.4 As I have done on previous occasions, I note that the comments I make in this regard are not intended to be a reflection on the Chair or other government members on the committee. In all the circumstances, including the inappropriately abbreviated timeline, the committee has acted (once again) in a collegiate manner and has done its best to deal with the timeline imposed upon it.

1.5 I note that inappropriately abbreviated timelines place a great workload upon the secretariat; especially when multiple bills dealing with important matters are required to be dealt with contemporaneously.

1.6 In this case, the committee was required to report on two bills on the day prior to the tabling of this report; namely, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 (a very significant bill which generated an inquiry report of 94 pages with additional comments from a number of Senators) and the Criminal Code Amendment (Genocide, Crimes Against Humanity and War Crimes) Bill 2024, a private senator's bill dealing with matters of great importance and sensitivity.

1.7 It is a great credit to the staff of the secretariat that they manage to navigate the pressures of such a workload. However, their ability to do so, should not be taken as an open invitation to government to continue to impose such demands.

1.8 It should also be recognised that relevant staff in the Attorney-General's Department (AGD) put great effort into engaging meaningfully with the inquiry process. This included processing a large number of questions on notice in a timely fashion. Whilst it is not possible in the time available to canvass all of these matters, it will suffice to comment that the prompt and thorough nature of the responses resolved a number of issues for me which would have otherwise been of concern.

1.9 Lastly, I thank all submitters who engaged with the inquiry. Again, given the abbreviated time available, it is not practical to respond to all of the issues raised. However, I found the submissions most useful and of great assistance in formulating my views with respect to the legislation. I am sure that Senate colleagues will find that the submissions provide a very useful resource in formulating their views in relation to the legislation.

Inappropriate consolidation of matters into a single bill

1.10 As noted above, the bill deals with a number of discrete policy areas where: (a) it could be reasonably anticipated that there would be divergent views in the Parliament; and (b) different scrutiny concerns are raised.

1.11 Obviously, the executive may choose to consolidate matters for political reasons. However, this does not enhance the objective of discerning the will of the Parliament with respect to contentious matters. **By including three schedules dealing with disparate matters in a single bill, senators will be forced to decide whether or not to support the bill in circumstances where they may agree to one or two schedules, but not all schedules. This is not best practice (if the goal is not to 'wedge' political opponents).**

1.12 The additional complication with respect to this bill is that Schedule 3 deals with amendments to a different act. Schedules 1 and 2 deal with amendments to the Privacy Act (noting it is certainly highly questionable as to whether consideration of introduction of a statutory tort should be dealt with in the same bill as that which deals with less controversial reforms of the nature contained in Schedule 1). However, Schedule 3 deals with doxxing offences to be introduced into the Criminal Code.

1.13 Given that Schedule 3 deals with issues relating to the criminal law, it should have been dealt with in a separate bill.

Inadequate time for stakeholders to engage in the committee process

1.14 Once again, inadequate time has been provided to those impacted by the proposed law to comment upon the bill.

1.15 As previously commented upon, the Law Council of Australia (Law Council) has repeatedly raised its concern (this is the sixth occasion) with the abbreviated inquiry processes that have occurred during this Parliament.[1] In its submission, the Law Council referred to the committee's '**lamentably short inquiry timeframe**'.[2]

1.16 The Law Council submitted:

> **The truncated Committee inquiry timeframe is also disappointing, given the significance of the proposed reforms to Australia's approach to privacy and data law, and the fact that an exposure draft of the Bill was not subject to public consultation.**
>
> Whilst the comprehensive Privacy Act Review Report was welcome after a long review process, the adaptation of many of its high-level proposals into the Bill necessitates close scrutiny to ensure that—as drafted, and in practice—these measures will achieve their policy intention and will not give rise to unintended consequences.
>
> The Bill was referred to the Committee for inquiry on 19 September 2024, with a reporting date of 14 November 2024. This reporting date has resulted in a period of approximately three weeks for submissions to be provided. This timeframe has heavily impeded the ability of the Law Council, its Business Law Section, and its Constituent Bodies, to engage at a detailed level with the legislative and explanatory materials (184 pages in total).
>
> In addition, several of our Constituent Bodies were unable to contribute to this submission, despite having a strong interest in these reforms. As a result, we have been unable to ascertain the views of the legal profession on a range of features in the Bill, nor have we had an opportunity to conduct a comprehensive analysis of the entirety of the proposals.
>
> **This truncated process is highly problematic from the perspective of broader public scrutiny of the making of Australia's laws, as part of a democratic process. This is a regrettable—and increasingly prevalent—consequence of the Parliamentary inquiry timeframes during this Parliament.** This trend also undermines the Law Council's role as a membership-based peak organisation, in which we have an obligation to consult with our Constituent Bodies, Sections, and advisory committees on matters of policy.[3]

1.17 In this context, concern was also raised in relation to the conjunction of the period of inquiry into this bill with other consultation processes requiring the detailed engagement of key stakeholders.

---

1 Refer to my comments in previous committee reports citing the concerns of the Law Council of Australia in relation to each of the following five bills: Administrative Review Tribunal Bill 2023; Migration Amendment (Removal and Other Measures) Bill 2024; Identification Verification Services Bill 2023; Criminal Code Amendment (Deepfake Sexual Material) Bill 2024, and Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024.

2 Law Council of Australia (Law Council), *Submission 67*, p. 5.

3 Law Council, *Submission 67*, p. 16.

1.18 The Digital Industry Group Inc. (DIGI) is a non-profit industry association that represents the interests of the digital industry in Australia (including Apple, Discord, Google, Meta, TikTok, X and others). It submitted:

Failure to provide exposure draft of the bill

1.19 A number of stakeholders also registered their dissatisfaction that the Labor Government had not released an exposure draft of the bill for consultation prior to the introduction of the bill. This was notwithstanding the fact that a number of key stakeholders specifically requested the Labor Government to release an exposure draft.

1.20 The Law Council submitted:

> In our April 2023 submission to the Department, we stated:
>
> The Law Council is supportive, at least in principle, of many of the proposals in the Report. However, it calls for and recommends that additional details be provided to give the proposals more certainty. To that end, the Law Council would welcome an opportunity to review an exposure draft bill with a view to providing further comment on legal issues raised… Further, given the high-level nature of the various proposals, it may be that there are further issues which are identified during the legislative process that the Law Council has not identified during this limited consultation process … Therefore, early and reasonable consultation with civil society, regulators and other interested parties and stakeholders on any exposure draft legislation will be critical.
>
> Similarly, in our April 2024 submission to the Department in response to its consultation on civil remedies to address doxxing, we stated:
>
> The Law Council reiterates its call for careful and considered consultation of any draft legislation introducing a statutory tort (for serious invasions of privacy) and other reforms designed to strengthen individual protection, to ensure that measures reflect community expectations and that the courts are empowered to weigh up the public interest in privacy against any other countervailing interests that may arise.
>
> **However, the Department did not provide us with an opportunity to review, or provide feedback on, an exposure draft of the Bill or any preliminary materials during its development.**
>
> **This is disappointing, given the legal profession's significant ongoing interest in these reforms, as evidenced by our detailed submissions to the Department in the course of the Privacy Act Review, and our subsequent offers to the Department to be consulted directly during its development of the Bill.**[4]

[4] Law Council, *Submission 67*, pp. 15–16.

1.21 BSA | The Software Alliance (BSA), the leading advocate for the global software industry, submitted:

> BSA notes that the AGD did not release an exposure draft of the Privacy Bill before introducing it into Parliament, despite multiple requests from various industry stakeholders.
>
> As a matter of good practice, releasing an exposure draft of a bill for public consultation would allow industry to engage on draft legislative text and comment on any potential concerns or ambiguities before it is submitted to Parliament. We find this practice invaluable in helping to create more widely supported and effective legislation.[5]

1.22 I agree. The number of issues raised by stakeholders during this inquiry evidence the benefits which would have arisen from the circulation of an exposure draft of the bill.

Failure of the Labor Government to make public the Cost Benefit Analysis undertaken by ACIL Allen

1.23 It is noted that the majority report does not refer to the failure by the Labor Government to release the Cost Benefit Analysis undertaken by ACIL Allen (the Cost Benefit Analysis). This is a material oversight.

1.24 The failure of the Labor Government to make public the Cost Benefit Analysis either before or during the inquiry into the bill was pursued (rightly) during the public hearing by my fellow committee member, Senator Shoebridge. The AGD responded to questions on notice in relation to this matter as follows:

> The Cost Benefit Analysis undertaken by ACIL Allen was commissioned for the purpose of informing decision-making processes about the impact of potential reforms, the release of which could, or might reasonably be expected to, disclose the deliberations of the Cabinet. Those processes are still underway. Standard government processes provide for an impact analysis, and accompanying assessment, to be published on the Office of Impact Analysis website when a final decision has been taken and announced.[6]

1.25 The importance of such analysis has been highlighted in a recent inquiry undertaken by this committee into the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024. The impact analysis undertaken by the AGD in that case informed the committee's deliberations into the impact of the bill upon small businesses (lawyers, accountants and real estate agents) and their clients.

---

5 BSA | The Software Alliance (BSA), *Submission 6*, p. 7.

6 AGD, Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024).

1.26 The Cost Benefit Analysis is not just being requested by senators. The Council of Small Business Associations of Australia (COSBOA) submitted:

> COSBOA also requests that the Attorney-General's office grants public access to the Cost Benefit Analysis so continued consideration can be given to the benefits of maintaining and perhaps expanding the small business exemption to the small businesses between $3 million and $10 million that face the same significant challenges in complying with the full breadth of all 13 Australian Privacy Principles.[7]

1.27 It is regrettable that the Labor Government has elected to deprive the Senate and relevant stakeholders the opportunity to consider the Cost Benefit Analysis in considering the bill.

Roadmap of future reform

1.28 When expressing their concerns with respect to the legislative process, a number of stakeholders (including significant representative bodies) submitted that there should be a road map of future amendments to the Privacy Act.

1.29 BSA submitted:

> In the Attorney-General's media release on the Privacy Bill, he stated that the Privacy Bill 'implements a first tranche of agreed recommendations from the Privacy Act'. However, there was no indication as to which recommendations will be implemented next, and when they will be introduced.
>
> Without a clear roadmap or timeframe, there is significant uncertainty regarding how and when businesses will need to adjust their privacy practices to comply with the evolving landscape.
>
> In the circumstances, we urge the Committee to encourage the AGD to provide a roadmap of future amendments to the Privacy Act. This roadmap should clearly set out which agreed recommendations the AGD will implement next, and when stakeholders can expect these agreed recommendations to be presented in a bill for public consultation.[8]

1.30 Digital Rights Watch submitted:

> If the Attorney-General's office intends on introducing these reforms in 'tranches', as is suggested, we expect to see a detailed roadmap and timeline for the introduction of the remaining tranche(s), else we risk the remaining reforms being delayed indefinitely. We concur with many other civil society organisations in calling on the government to implement the remaining reforms within six months of taking office, should they win the next election. We also call on the opposition to make a similar commitment should they win office.[9]

---

7 Council of Small Business Organisations Australia (COSBOA), *Submission 46*, p. 3.

8 BSA, *Submission 6*, p. 6.

9 Digital Rights Watch, *Submission 50*, p. 4.

1.31 Similarly, the Law Council submitted:

> Whilst it is pleasing that the Government intends to continue this significant reform work, we call for a roadmap, or strategy, to publicly detail how these reforms will be progressed—similar to the materials that the Government issued in 2023 for the Security of Critical Infrastructure Act 2018 (Cth). The proactive provision of clear details (i.e., what proposals will be addressed in each tranche of reform) will promote much-needed certainty for the multitude of sectors that expect to be impacted by these significant changes.[10]

Commentary

1.32 If the Senate is to perform its function as a house of review, there needs to be adequate time for those impacted by proposed legislation (and their representative bodies), to engage in the Senate committee process. The failure to provide such time is a detriment to the law-making process.

1.33 With all due respect, it is embarrassing that the Law Council has on six occasions had to register its dissatisfaction with inquiry processes in relation to legislation introduced by the AGD. This should be a cause for deep reflection on the part of the Labor Government.

Recommendation 1

1.34 It is recommended that the Senate note the inappropriateness of the abbreviated timeline for consideration of the Privacy and Other Legislation Amendment Bill 2024 [Provisions]; especially given:

a) the importance of the legislation;
b) the failure of the government to circulate an exposure draft of the bill; and
c) the concurrent examination of other legislation in the same policy area making it difficult for stakeholders to engage in depth.

Recommendation 2

1.35 It is recommended that the Senate call for the release of the ACIL Allen Cost Benefit Analysis prior to debate on the bill with a view to ensuring that the Senate has the benefit of all relevant analysis undertaken in relation to the subject matter of the bill prior to voting on the bill.

---

[10] Law Council, *Submission 67*, p. 17.

Recommendation 3

1.36 It is recommended that the Senate note the inappropriateness of including in the same bill, provisions which amend different acts and/or deal with different policy areas in circumstances where senators may reasonably be expected to have different views (in good faith) as to whether the provisions in different schedules should be supported and be passed into law.

Recommendation 4

1.37 It is recommended that the Senate consider each schedule separately and that the government do all things reasonably necessary to facilitate such consideration.

Recommendation 5

1.38 It is recommended that, as requested by a range of key stakeholders, the government provide a road map, or strategy, regarding how future reforms will be progressed.

Amendments to the Privacy Act (Schedule 1)

Overview

1.39 Schedule 1 of the bill deals with matters which have been the subject of consideration by the Privacy Act Review. The majority report provides a very detailed overview of the issues raised during the inquiry. Given the limited time available to prepare these comments I focus upon areas which, in my view, warrant further consideration.

Response to recommendations proposed in the majority report

1.40 I support:

- the minimum consultation period for the Children's Online Privacy Code being extended to at least 60 days (recommendation 1);
- the bill being amended to require the Information Commissioner to consult with relevant industry bodies or organisations when developing the Children's Online Privacy Code (recommendation 2);
- the rectification of the drafting error in the proposed new paragraph 80KA(2)(b) to ensure that the ABC and the Special Broadcasting Service fall within the ambit of 'media organisations' (recommendation 3);
- the bill being amended to empower the Information Commissioner to issue a discretionary notice to an entity to remedy an alleged breach of one or more of the provisions in section of the bill before issuing an infringement notice (recommendation 4); and
- amending the Explanatory Memorandum to make clear the level of information required in privacy policies is not expected to compromise

commercial-in-confidence information about automated-decision making systems (recommendation 5).

1.41 In summary, I support recommendations 1 to 5 in the majority report for the reasons outlined therein.

Scrutiny concerns

1.42 The Scrutiny of Bills Committee raised concerns with the exemption from disallowance for a temporary Australian Privacy Principle (APP) code if the minister is satisfied that it is in the public interest for the code to be developed, for the Information Commissioner to develop the code, and that the code should be developed urgently.

1.43 In commenting upon the relevant principles, the Scrutiny of Bills Committee commented:

> The committee notes that disallowance is the primary means by which the Parliament exercises control over the legislative power that it has delegated to the Executive. Exempting an instrument from disallowance therefore has significant implications for parliamentary scrutiny. In June 2021, the Senate acknowledged these implications and resolved that delegated legislation should be subject to disallowance unless exceptional circumstances can be shown which would justify an exemption. In addition, the Senate resolved that any claim the circumstances justify an exemption will be subject to rigorous scrutiny, with the expectation that the claim will only be justified in rare cases.[11]

1.44 In considering the arguments made for exemption from disallowance in this case, the Scrutiny of Bills Committee concluded:

> Whilst the committee acknowledges the necessity of an immediate, clear and certain legal basis for entities to know their obligations, the committee consider this is achievable while allowing parliamentary oversight. The committee notes that a legislative instrument has effect from the day of commencement, which may be the day of registration, thereby establishing an immediate legal basis, and will continue to have effect unless it is disallowed within the disallowance period. The committee does not consider the need for certainty in this context to be an indication of exception circumstance that warrant an exemption from disallowance.[12]

1.45 The oversight power of Parliament in the context of laws promulgated during emergencies is of great importance. On one view, the importance of that oversight role can be even more important in an emergency context.

---

11 Scrutiny of Bills Committee, *Scrutiny Digest 13/24*, 9 October 2024, pp. 44–45.

12 Scrutiny of Bills Committee, Scrutiny Digest 13/24, 9 October 2024, p. 46.

1.46 In relation to this issue, the Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University submitted:

> The authors note that caution should be exercised with respect to proposed ss 26 GB(8), 80J(3), and 80K(3) that exclude the operation of section 42 of the Legislation Act (Cth).
>
> Unless exceptions circumstances apply, Parliament should retain ultimate oversight over the exercise of legislative or quasi-legislative power. The proposed ss 26 GB(8), 80J(3), and 80K(3) would undermine the ability for the Parliament to review decision making with respect to delegated legislation.[13]

1.47 It is further noted that the Scrutiny of Legislation Committee also made requests in relation to the making of addendums to the Explanatory Memorandum to address scrutiny issues in relation to: (a) provisions reversing the burden of proof (with respect to disclosure of information in certain circumstances);[14] and (b) the justification to include significant matters in delegated legislation (in relation to new exceptions for APP entities in assessing overseas recipients prior to releasing personal information to said recipients).[15]

1.48 For completeness, it should be noted that I raised the issue with Human Rights Commissioner Finlay of the Australian Human Rights Commission who opined as follows:

> In respect of the Privacy Amendment Bill, the Explanatory Memorandum sets out why the creation of the temporary APP codes should not be subject to disallowance under the Legislation Act 2003 (Cth). For the reasons set out in the Explanatory Memorandum, the exemption from disallowance is – on balance – appropriate in these limited circumstance.[16]

1.49 I respectfully disagree. Given that any temporary APP code would be in effect from the time promulgated and it should be reasonably assumed that the Senate would only exercise its power to disallow in extreme cases (following a period of consultation with the minister which may address any scrutiny concerns, as is usually the case), there is insufficient justification to remove the Parliament's oversight function in this context.

---

13 Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University, *Submission 19*, p. 4.

14 Scrutiny of Bills Committee, Scrutiny Digest 13/24, 9 October 2024, p. 48.

15 Scrutiny of Bills Committee, Scrutiny Digest 13/24, 9 October 2024, p. 50.

16 Australian Human Rights Commission, Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024).

Recommendation 6

1.50 It is recommended that the Senate as a whole consider the scrutiny issues raised by the Scrutiny of Legislation Committee with respect to the appropriateness of exempting temporary Australian Privacy Principles Codes and emergency declarations from disallowance given that such codes would have immediate effect and would only be disallowed following consultation undertaken by the Scrutiny of Delegated Legislation Committee with the minister.

Recommendation 7

1.51 It is recommended the government make addendums to the Explanatory Memorandum of the bill as requested by the Scrutiny of Legislation Committee.

Importance of facilitating cross-border data transfers

1.52 A number of stakeholders raised the importance of facilitating cross-border data transfers.

1.53 I quote from the Global Data Alliance (GDA) submission in depth:

> The GDA strongly supports the importance of facilitating cross-border data transfers. As explained in the Memo, companies can already transfer data to overseas recipients through a variety of methods consistent with the Australian Privacy Act 1988 (Privacy Act).
>
> These include disclosing data pursuant to APP 8.1, which adopts the accountability model and requires companies to meet certain obligations before transferring data to an overseas recipient, most notably the requirement to "take reasonable steps" to ensure the overseas recipient does not breach the APPs in relation to the information.
>
> Separately, companies can also transfer data under APP 8.2 to an overseas recipient that is subject to a "substantially similar" privacy law or binding scheme, without adopting the obligations imposed in APP 8.1.
>
> The proposed mechanism under the Privacy Act would prescribe the countries and certification schemes that provide "substantially similar protection" under APP 8.2(a).
>
> The new mechanism would therefore make it easier for companies to transfer data under APP 8.2(a) by identifying countries that have "substantially similar protections," rather than requiring companies to assess for themselves which countries have such protections.
>
> Crucially, GDA notes that the new scheme would not limit companies from transferring data under the accountability model reflected in APP 8.1 or pursuant to any of the other grounds for transfers recognised in APP 8.2(b)-(f).
>
> In the circumstances, GDA supports the introduction of this proposed mechanism, as it will provide businesses with greater legal certainty and substantially reduce compliance burdens. However, GDA also observed

that neither the Privacy Bill nor the Memo explained what would constitute a "substantially similar" level of protection.

If the mechanism establishes an unnecessarily strict interpretation of "substantially similar", it would be counterproductive to the policy objective of increasing certainty for companies transferring data internationally. For example, to the extent a new mechanism applies the term "substantially similar" to mean a standard akin to the European Union's "essentially equivalent" standard, it may unnecessarily restrict transfers conducted under APP 8.2(a)…

Relatedly, GDA recalls that the AGD's Privacy Act Review Report 2022 (AGD Report) suggested that Australia could prescribe the Cross Border Privacy Rules (CBPR) system under APP 8.2(a) as a binding scheme that provides a "substantially similar" level of protection to the APPs.

In this regard, we reiterate our support for recognising internationally recognised certifications and standards such as the Global CBPR system. Similarly, the Act could also recognise compliance with ISO 27701 as creating "substantially similar" protections…

Finally, we also observe that Australia – and many of its closest trading partners – have reflected their commitment to the protection of personal data from governmental overreach in the context of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.

The Global CBPR Forum and the OECD Declaration on Government Access to Personal Data Held By Private Sector Entities are specifically designed to bring together governments with a substantially similar view of the importance of personal data protection in a cross-border data policy context. We encourage Australia to consider presumptively deeming the signatories of these mechanisms to meet the "substantially similar" standard under the APPs.

Recommendations:

GDA supports the introduction of a mechanism to prescribe countries and binding schemes that provide substantially similar privacy protections to the APPs. However, we recommend that that the Privacy Bill specify what constitutes "substantially similar" privacy protections and conducts further consultations on the process for, and factors involved in, determining whether a country or certification scheme offers the appropriate level of protection.

We also encourage the Australian Government to take account of the longstanding efforts of Australia and its allies to improve cross-border data privacy interoperability by presumptively deeming the signatories of the Global CBPR Forum and OECD Declaration on Government Access to Personal Data Held By Private Sector Entities to meet the "substantially similar" standard under the APPs.[17]

[17] Global Data Alliance, *Submission 9*, pp. 1–2.

1.54 The Interactive Gaming and Entertainment Association recommended:

> While not in the scope of this Bill, the Australian Government should continue to work on a path towards an adequacy decision to facilitate overseas data flows between Australian and the EU.
>
> The EU's General Data Protection Regulation be prioritised at the first opportunity, in accordance with the overseas data flows provision of the Bill.
>
> The Australian Government (via the relevant Minister) should favourably consider 'whitelisting' countries that already have an adequacy decision with the EU, where the GovernorGeneral could then make regulations to prescribe that these countries provide substantially similar protections to the APPs, in accordance with section 100(1A) of the Bill e.g. the United Kingdom and Japan.
>
> The Bill should also clarify Australia's position on 'onward transfers', where personal information that was first transferred from Australia to a whitelisted country (Country A), is further transferred from Country A to another country (Country B).
>
> The Government should reconsider whether 'substantially similar' is the best term to use as the certification threshold for establishing overseas data flows between Australia and a given country. We would prefer the term 'adequate' or 'similar'.[18]

Recommendation 8

1.55 It is recommended that the government and relevant agencies consider the recommendations made by industry leaders with respect to providing greater clarity with respect to which countries have 'substantially similar' privacy protections, including through prescribing relevant countries and systems as soon as reasonably practicable to provide clarity to business in relation to cross-border data transfers.

Additional matters

1.56 There are a range of additional matters raised in the submissions, including issues which are very technical in nature. There are practical suggestions with respect to implementation. There are also requests with respect to progressing the next stage of reforms. All of these should be considered by the government. In the time provided for this inquiry it is not practical to do justice to all of the recommendations and suggestions made by stakeholders.

---

[18] Interactive Gaming and Entertainment Association, *Submission 18*, pp. 4–5.

Recommendation 9

1.57 It is recommended that the government:

a) systematically review the submissions made to the inquiry;
b) consider any further amendments to Schedule 1 which would enhance the bill and provide further clarity; and
c) consider the submissions made in this inquiry in relation to both implementing the reforms contained in Schedule 1 and progressing the next stage of reforms.

Introduction of a statutory tort for serious invasions of privacy (Schedule 2)

Overview

1.58 Schedule 2 of the bill would introduce a statutory tort for serious invasion of privacy. This was first recommended by the Australian Law Reform Commission in 2014.

Concerns raised by key stakeholders

1.59 Whilst there is support for the introduction of the statutory tort for serious invasions of privacy from a range of stakeholders, there are also material concerns. This includes with respect to unintended consequences.

Small business

1.60 From a small business perspective, COBOA submitted:

> The current small business exemption in the Privacy Act – for entities with less than $3 million annual turnover – ensures a degree of nuance between small and micro-businesses compared to expectations of large multinational companies. Small businesses of all sizes already actively process data with appropriate care and concern, many of which already have a turnover of over $3 million and are therefore already subject to the Act.
>
> However, the rapid introduction of complex and expanding obligations to comply with all 13 Australian Privacy Principles for those small businesses with an annual turnover under $3 million would have undermined the viability of those businesses already facing a laundry list of increased red tape and regulation.
>
> COSBOA is therefore encouraged to see that the small business exemption is being maintained. There is never a good time to hoist higher costs onto small businesses, but to do so in the current environment would be reckless.
>
> COSBOA notes that the ATO defines small business as those with an annual turnover of $10 million or less whilst micro-businesses are defined as those with a turnover of less than $2 million. **We note that the current "small business exemption" relating to an annual turnover threshold of $3 million was introduced two decades since but has never been indexed. Therefore, the effect over time has been that an increased number of small businesses have become subject to the Australian Privacy Principles but with few resources to assist them in meeting their compliance requirements…**

> COSBOA is concerned about the drafting of Schedule 2 – Serious Invasions of Privacy which introduces a statutory tort of privacy into the Act. The Explanatory Memorandum notes that the Schedule is intended to be treated as a set of stand-alone provisions which are independent from the rest of the Act. The inclusion of the Schedule itself in the Act is likely to cause confusion…
>
> **There is no reference or exemption for entities who are not required to comply with Schedule 1 (e.g. small businesses with a turnover of less than $3 million). Additionally, the Bill does not make it clear how the actions of employees who seriously invade an individual's privacy could render employers liable under this provision…**
>
> COSBOA reiterates its appreciation that the Government listened to and took on board our significant concerns and decided against pushing ahead with the proposed removal of the small business exemption for small businesses under $3 million. **However, further consideration of the new statutory cause of action for serious invasions of privacy is now required…**[19]

Freedom of the press

1.61 From a freedom of press perspective, strong submissions were made by Australia's Right to Know Coalition (ARTK) (comprising many of the leading news media organisations).

1.62 ARTK submitted:

> The Bill, in proposing a statutory tort of privacy:
>
> (i) actions for injunctions will flourish should the tort be introduced despite the addition of section 9(2) mainly because some persons involved in journalism fall outside the exemption (such as publishers, licensees and sources) and injunctions targeted at them will impact journalism. Any application will invariably be an application for an interlocutory injunction to ensure the plaintiff is immediately protected from any imminent publication (which will indirectly supress media publication); or
>
> (ii) proceedings for pre-discovery against persons involved in journalism who fall outside the exemption such as publishers, licensees and the source of journalist's information.[20]

1.63 In answers to questions on notice, ARTK provided extremely strong rebuttal against those who argued that media and journalism exemption was inappropriate, including through comparison with overseas jurisdictions.

---

[19] COSBOA, *Submission 46*, pp. 1–3.

[20] Australia's Right to Know (ARTK), *Submission 59*, p. 2.

1.64 ARTK submitted:

ARTK submits that some of the questions posed and ARTK's responses should be considered in light of the following contextual material:

That protection does not exist in Australia. Thus, the ALRC accepted that in the absence of those overarching laws it was "essential" that ALRC include the public interest in free speech as an element of the tort it proposed and not a mere defence. In evidence to the Committee Professor McDonald conceded that the drafting of clause 7(3) of the Bill departed from that principle and that she had "no idea" why that had occurred.

Various submissions made to the Committee make similar assertions that the media has engaged in unjustifiable intrusions of privacy, without providing evidence of such and are without factual basis.

The reason no evidence was put before the Committee is not because of deficiently drafted submissions. The reason is that such evidence does not exist.

(1) the OIAC has greater powers in relation to declarations and recompensing victims;

(2) in defamation law the requirement of "serious harm" has been adopted by Australian legislatures as an appropriate counterbalance to excessive litigation and to protect the public interest;

- there continues to be no evidence of any systemic or serious intrusions or misuse of information by media organisations nor is there any evidence of the breach of criminal laws by the media resulting in breaches of privacy;

- the Australian media landscape has changed significantly including that the current economic landscape, competition from social media and the costs of litigation pose an existential threat to journalism. The current debate regarding privacy law and its impact on journalism appears to be being conducted without reference to this critical context;

(3) serious intrusions and/or misuse of information are more likely to be engaged in by individuals on social media on other platforms; and

(4) misuse of information from data breaches are more likely to be by foreign criminal actors who are unlikely to be deterred by or sued under the tort.[21]

1.65 One area of concern is in relation to the impact of the statutory tort upon sources for press/media stories, including where important information/intelligence is provided to journalists.

1.66 In this regard, ARTK submitted:

> Likewise, it is unclear how the provision will interact with s.126K of the Evidence Act (Cth) save to say that the legislation is very likely to be used by plaintiffs' lawyers to attempt to unmask confidential sources.
>
> It seems likely that the journalist shield in the Evidence Act will not always apply to assist journalists and their sources, given ambiguities and differences in the drafting, and the limitations built into those separate provisions – so the existence of this separate protection for journalists under the Evidence Act cannot be relied on as solving the vulnerabilities of journalists and their sources under the tort.
>
> **It seems the drafting hasn't given consideration to the interplay between the proposed privacy tort and journalists' sources...**
>
> **Importantly it underlines that consideration has not been given to the interplay between the proposed tort and source protection.** In the first ARTK submission we highlighted that and the conflict it will cause which can be summarised as follows:
>
> **(5) there is a real risk that the tort will have a chilling effect on freedom of the media and reporting of matters of public concern as it will be used to prevent dissemination of information including to the media;**
>
> *(6)* in light of the breadth of the proposed cause of action, there is a real risk that it will be applied by a court so broadly as to: restrict the reporting of investigations or matters of concern relating to public officials (where the constitutional protection does not apply); and have the effect of prohibiting police investigations in an equivalent manner to the development of the tort in the UK; *and*
>
> (7) the tort does not prevent individuals seeking interlocutory injunctions against other parties which would in effect apply against journalists and their employers to prevent publication of information to them, or otherwise passing on of the information to others.[22]

[21] ARTK, Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024).

[22] ARTK, Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024).

1.67 In relation to freedom of the press, Commercial Radio Australia (CRA) submitted:

> Key points:
>
> - CRA and commercial radio broadcasters support the aim of modernising Australia's privacy legislation so that it is fit for purpose in a digital world.
> - The proposals in the Bill to introduce a new statutory tort for serious invasions of privacy are not required to achieve this aim. Experience in other jurisdictions, particularly in the United Kingdom, has demonstrated that similar torts have had a significant chilling impact on freedom of speech and journalism.
> - The exclusion for journalism in the proposed statutory tort will not assist in avoiding these negative consequences, with significant adverse consequences for Australia's democracy.
> - CRA recommends that either the proposed tort is removed from the Bill or a more effective exclusion mechanism for journalism is incorporated, as set out in this submission.[23]

Concerns of the business sector

1.68 Whilst generally supportive of the introduction of a statutory tort, the Australian Institute of Company Directors raised the following concern:

> 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.**[24]

1.69 DIGI submitted:

> Noting that the proposed tort aims to build on a model developed by the ALRC, **DIGI believes that further work needs to be done to ensure that the scope of the Privacy Tort's application is clear and that it is harmonised with existing Australian laws to minimise the risk of unintended and unreasonable consequences.** In particular, the Privacy Tort should be framed to align with the various existing causes of action which have been historically used to protect privacy and reputation,

---

23 Commercial Radio Australia, *Submission 43*, p. 1.

24 Australian Institute of Company Directors, *Submission 39*, p. 2.

> including equitable actions for breach of confidence, tort actions for trespass to land, nuisance and defamation.[25]

1.70 The Ai Group raised numerous issues, including with respect to worker information, submitting:

> We set out below our key concerns as to the application of this cause of action as follows:
>
> (a) Employers legitimately use worker information, including as set out in paragraph 7 above. Although an individual themselves may consider the retention or use of their personal information in the workplace as being an infringement of a right to privacy it should not always be considered. The prospect of compensation being ordered by way of damages is inappropriate considering the public interest in employers exercising a reasonable use of workers' information to effectively manage their workforce.
>
> (b) **The introduction of a statutory tort for a serious invasion of privacy amounts to a significant change to the enforcement regime pertaining to privacy breaches that is not justified by any apparent shortcomings in the existing avenues available for enforcing individual rights to protection from an invasion of privacy or in the context of the flagged tranche 2 of amendments to the Privacy Act.**
>
> (c) Opening an avenue for prosecution on the basis of recklessness as envisaged is oppressive and will likely result in our members being compelled to take an excessively risk-averse stance with respect to the treatment of workers' information.
>
> (d) The nature of a tort, by focusing on redress by way of an award of damages, is unsuitable in relation to breaches of privacy in a workplace context. Also, the emphasis on damages and compensation in tort law may encourage speculative litigation by individuals claiming mental distress. Vicarious liability for the wrongs of an employee presents a significant risk for employers in the context of tort law. The various risk mitigation strategies and the litigation insurance costs which would be necessitated by the establishment of a privacy tort would not be in the public interest.
>
> (e) An actionable tort per se as is proposed (i.e. where there is no need for the claimant to establish any form of damage) exposes employers to an even greater risk which is not counterbalanced by any public benefit from introducing a tort of privacy.
>
> (f) **We consider that the forum with the appropriate expertise lies with the OAIC. The OAIC should be solely responsible for assessing breaches relating to privacy and acting on an affected individual's behalf. If there are concerns that the OAIC has insufficient resources to undertake its responsibilities or expeditiously resolve matters, a more appropriate response would be to increase the OAIC's resources. Creating another avenue and action for redress through the courts may generate other problems, including shifting the administrative burden from the OAIC to the courts, duplicating the OAIC's function, and potentially opening up**

[25] DIGI, *Submission 41*, p. 6.

> **the floodgates to a litigious culture. Such an outcome would be an administratively inefficient use of public resources and would most likely harm many businesses.**
>
> (g) The introduction of the statutory tort is unnecessary given that an employer's reasonable monitoring or use of employees' information in connection with work, including in areas of 'seclusion' is already comprehensively regulated by state and territory surveillance legislation. Monitoring and surveillance has long been acknowledged by legal decision-makers as being a legitimate practice, particularly in the context of managing conduct and performance, as a pro-active step to prevent unlawful workplace behaviours in the virtual workplace environment and to ensure the health and safety of workers and the community.[26]

Concerns of the health sector

1.71 As referred to in the majority report, the Australian Medical Association (AMA) raised a number of material issues with respect to the application of the statutory tort in the context of the provision of health services and research.

1.72 The AMA submitted:

> **While the Privacy and Other Legislation Amendment Bill 2024 aims to strengthen privacy protections, the introduction of the statutory tort under Schedule 2 creates substantial risks for the medical and public health sectors.**
>
> The lack of clear definitions, the removal of key exemptions, and the potential for dual liability will lead to greater legal uncertainty, increased litigation, and higher operational costs for healthcare providers.
>
> **These consequences will not only affect the delivery of medical care but could also stifle medical research and limit open debate in scientific and other publications that fall outside the journalist exception. We respectfully request Schedule 2 is withdrawn, pending further sector and legal consultation.[27]**

Concerns of other stakeholders

1.73 Electronic Frontiers Australia (EFA) (not-for-profit national organisation that works to ensure that technology makes our lives better, not worse and which promotes the idea that digital rights are human rights) submitted:

> **EFA holds concerns in respect of the proposed Statutory Tort for Serious Invasions of Privacy being introduced at Schedule 2 of the Privacy Amendment Bill. We note that there are financial barriers of access to this remedy which will be prohibitive to most ordinary Australians, let alone vulnerable classes of Australians. The courts are not a universal remedy, it offers bespoke protection to those that can afford it.[28]**

---

26 Ai Group, *Submission 42*, pp. 8–9.

27 Australian Medical Association, *Submission 26*, p. 4.

28 Electronic Frontiers Australia, *Submission 45*, p. 7.

1.74 To address these concerns, EFA proposed a number of amendments – amendments which would be strongly contested by other stakeholders.

Commentary

1.75 The above is a selection of the views provided to the committee with respect to the statutory tort. There are many others which have not been included. This provides an insight into the complicated nature of the issues arising from Schedule 2.

1.76 The assessment becomes even more vexed when one considers the multitude of amendments proposed by different stakeholders. In the time available, it is simply not practical to undertake a meaningful assessment of the different options for amendment and to determine whether or not they satisfactorily deal with the material concerns raised in relation to Schedule 2. Hence, I provide no opinion with respect to recommendations 6 to 9 in the majority report. At this stage, it is not possible to opine with respect to their adequacy or otherwise to address the many serious issues raised by stakeholders.

1.77 Having reviewed the submissions, I am firmly of the view that it would be imprudent for the Senate to attempt to resolve the complicated issues raised by Schedule 2 in a rushed manner. This would no doubt lead to unintended consequences. There is an overwhelming case for further detailed consultation of Schedule 2 prior to it being further considered by the Senate.

Recommendation 10

1.78 It is recommended that Schedule 2 be excised from the bill. Prior to any re-introduction into the Parliament there needs to be further extensive consultation, including with respect to the range of stakeholders who have made submissions in relation to potential unintended consequences. As part of the consultation, the government should consider developments since the Australian Law Reform Commission tabled its report recommending the introduction of the statutory tort, including experiences in the United Kingdom with respect to press freedom. Any reintroduction of a bill which proposes the introduction of the statutory tort needs to be preceded by circulation of an exposure draft and consultation. Further, any such bill will need to be the subject of detailed examination by the Legal and Constitutional Affairs Committee with sufficient time to consider and balance competing views and interests.

Introduction of doxxing offences into the Criminal Code (Schedule 3)

Overview

1.79 The case for the introduction of doxxing offences is well made in the majority report. The views of stakeholders is summarised in paragraphs 2.283 to 2.301 of the majority report. There is no need for me to repeat them.

Concerns raised by key stakeholders

1.80 Many of the concern raised by stakeholders are reflected in the submission of the Law Council who submitted:

> 128. The term 'doxxing' is very broad—the eSafety Commissioner defines it as 'the intentional online exposure of an individual's identity, private information or personal details without their consent'.
>
> 129. Whilst the term is not mentioned in the Privacy Act Review Report, we acknowledge that the issue of doxxing has received significant media attention in 2024. We also appreciate that, as identified by the eSafety Commissioner, doxxing can leave targets vulnerable to—and fearful of—public embarrassment, discrimination, stalking, identity theft, financial fraud, and damage to their personal and professional reputation. We outlined these considerations in more detail in our April 2024 submission to the Department.
>
> 130. We also acknowledge that there are instances in which doxxing behaviour is legitimate and should not be circumscribed. For example, doxxing can be part of public interest journalism where it involves the unveiling of private information that exposes contradictory, unethical, or illegal behaviour by public officials or business people.
>
> **131. In respect of Schedule 3 to the Bill, we are concerned that there is potential for the proposed offences to be misused. We have received feedback that proposed offences are so broad that they may unintentionally criminalise many forms of conduct that they were not intended to cover, or that they may be used strategically to stifle legitimate public debate. [my emphasis].**
>
> 132. For instance, a person who writes or publishes an online article that is critical of a group (as per proposed section 474.17D of the Criminal Code), that includes the names of people who are members of that group, may be committing an offence under that section. By way of illustration, in April 2023, there was an ABC Four Corners report about Paralympic athletes who were deliberately overstating their disabilities. The report included the names and images of certain athletes who were alleged to be engaging in this conduct. Under the Bill, that story may constitute a criminal offence (if the test is met that a reasonable person would regard the reporting as being menacing or harassing towards them). Additionally, we query whether the proposed offences would capture instances where an individual has posted allegations on their social media account that a person (or persons) sexually assaulted them.
>
> 133. The Bill also should provide further guidance on what constitutes 'menacing' or 'harassing' behaviour. As drafted, there is no clear definition

> of what behaviour constitutes 'harassing'—the term most likely applicable to doxxing.
>
> 134. Moreover, the concept of 'personal data' is defined very broadly in proposed subsections 474.14C(2) and 474.14D(2) to mean information about the individual or group members that allows them to be 'identified, contacted or located'. There also appears to be no clear differentiation between penalties for certain types of 'personal data' being released. For instance, leaking sensitive information (e.g., private medical, legal, or financial records) may warrant a harsher punishment under the Bill, compared to publishing an individual's name and social media handle.
>
> 135. Certainty about these matters is crucial, particularly noting the significant penalties of six and seven years' imprisonment for the offences in proposed sections 474.14C and 474.14D, respectively.
>
> 136. Finally, further education is needed to inform the community about the harms associated with doxxing. Emphasis should be placed on the importance of limiting public disclosure of personal information online, not only the information of individuals but also the information of groups of individuals.[29]

1.81 To address these concerns, the Law Council recommended:

> Schedule 3 to the Bill should be redrafted to address the concerns raised in this submission about: - the doxxing offences being drafted too broadly; - the need for guidance on what constitutes 'menacing' or 'harassing' behaviour; and - the lack of differentiation between penalties for the release of certain types of 'personal data'.[30]

1.82 I note that the Australian Federal Police (AFP) consider that there is sufficient law with respect to what constitutes 'menacing or harassing behaviour. In their submission:

> The Bill seeks to introduce new offences targeting the release of personal data using a carriage service in a manner that would be menacing or harassing (i.e. doxxing). In this digital age it is easier than ever to not only obtain someone's personal information, but share it with millions of people. The harms and risks associated with doxxing are varied and can be significant. Criminalising this conduct may deter offenders and will provide a clear message to the community that this conduct is not tolerated. The new offences complement existing offences in the Criminal Code Act 1995 for using a carriage service to menace, harass or cause offence (section 474.17).
>
> The AFP was consulted during the development of the new offences, to ensure they are operationally workable. Doxxing offences reported to the AFP for investigation will be reviewed and prioritised according to the AFP's Operation Prioritisation Model (OPM), which considers the severity of the threat of harm and the impact that the AFP could have in eliminating or reducing that threat. All reports of crimes to the AFP are prioritised through the OPM, which is designed to ensure AFP operational decisions

---

29 Law Council, *Submission 67*, pp. 38–39.

30 Law Council, *Submission 67*, p. 39.

> are appropriately focused on ensuring public safety, minimising community harm, and protecting national interests. The offences will also be available to state and territory police to investigate and prosecute.
>
> Based on past experience, the AFP would expect to investigate the new offences in the broader context of racially or politically motivated violence or harassment. In other cases, investigations may fall to state and territory police in their community policing roles.[31]

1.83 Noting the experience of the AFP in investigating offences dealing with menacing and harassing conduct through use of a carriage service, it should be possible to resolve the concerns of the Law Council with appropriate amendments.

1.84 In this regard, I note the proposal from the Human Rights Commissioner Lorraine Finlay who submitted:

> The proposed criminal offence of doxxing will limit the human right to freedom of expression by restricting certain forms of sharing information. The key issue is ensuring any offence is carefully tailored to meet the strict tests of necessity and proportionality and to avoid capturing reasonable online discourse about a person.
>
> One example of a potential risk area is students sharing in online forums the names and subjects taught by teachers at educational institutions. Such a case arose in Germany: A profile of a teacher was created on a website where students can rate their teachers … The teacher 'filed a lawsuit seeking the erasure of the data and an injunction restraining the website provider from publishing this information again'.
>
> The relevant court, however, did not grant the request. Given that the students' right to freedom of expression, and that the information was already publicly available on the educational institution's website, the comments were not considered to be defamatory, and further that they did not relate to her private life, but only to her working life as a teacher.
>
> Challenges may also arise concerning online groups created to share information, and warnings about individuals who allegedly engaged in conduct that was abusive, harassing or otherwise inappropriate. For example, a 2022 survey by the Australian Institute of Criminology found that three in four dating app users have experienced harassment when using dating apps.
>
> Many have turned to social media to share their experiences and warn others about potentially dangerous individuals.
>
> While the sharing of information online in this way has the potential to enhance public safety, there is also a potential risk of digital vigilante activity, which may see individuals seek to enforce a 'parallel form of criminal justice', and can undermine rule of law protections.
>
> There are also concerns that doxxing laws may unreasonably capture public interest whistleblowing and journalism.

---

31 Australian Federal Police, *Submission 71*, pp. 1–2.

> The Bill as currently drafted seeks to guard against these risks by providing that the offences only apply where 'the person engages in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those individuals'.
>
> **However, including a provision in the Bill which expressly protects the release of information for legitimate public interest purposes would help to further strengthen the protection of freedom of expression while still effectively addressing the harms caused by doxxing.**
>
> Recommendation 6: The Federal Government include a provision in the Privacy and Other Legislation Amendment Bill 2024 (Cth) which provides protection for the release of information for legitimate public interest purposes.[32]

Commentary

1.85 In my view, consideration should be given to the recommendations made by the Law Council and the Australian Human Rights Commission. The conduct contemplated by the provisions is not conduct at the margins – it should be reasonably clear whether relevant behaviour falls outside the realm of legitimate public purpose.

Recommendation 11

1.86 It is recommended that the bill be amended to address the concern that the offence as drafted may be too wide. In this regard, consideration should be given to the recommendations made by the Law Council of Australia and the Australian Human Rights Commission.

Conclusion

1.87 In summary, I support the passage of Schedule 1 of the bill (subject to the issues raised in recommendations 1 to 5 of the majority report) and the recommendations in these additional comments being addressed.

1.88 Schedule 2 introducing a statutory tort needs to be withdrawn for further consultation. Given the strength of the submissions received and the myriad of complicated amendments proposed, it is my strong view that it would be imprudent for the Senate attempt to resolve the issues and pass the provisions into law in an abbreviated period of time.

1.89 Lastly, I support the introduction of the doxxing provisions, subject to consideration of opportunities to tighten the drafting to avoid unintended consequence.

---

[32] AHRC, *Submission 36*, pp. 8–9.

Recommendation 12

1.90 Subject to Schedule 2 (the introduction of the statutory tort) being withdrawn from the bill for further consultation and detailed consideration, it is recommended that bill be passed comprising Schedule 1 (Privacy Act reforms) and Schedule 3 (the creation of doxxing offences in the Criminal Code) subject to the amendments discussed in these additional comments (including recommendations 1 to 5 in the majority report).

Senator Paul Scarr
Deputy Chair

Additional comments from the Australian Greens

1.1 The Australian Greens believe that privacy should be recognised as a fundamental human right in the objects of the Privacy Act, and further codified in an eventual Human Rights Act. As technology becomes ever more important for everyday life it is essential that people's privacy is enhanced so that corporations cannot rapaciously consume individual and communities' private lives.

1.2 This report makes a number of recommendations that deal with issues raised about the drafting of the bill. These amendments are reasonable and supported by the evidence received. In particular, the recommendations extending the consultation period and requiring consultation with a wide range of stakeholders for the children's privacy code are strongly supported.

1.3 Serious concerns have been raised about the proposed doxxing offence, including the fact that the offence as drafted does not require intention, could cover the narrow sharing of publicly available information like the email address of a politician and the fact there is no exemption for industrial disputes or other political purposes. We agree with stakeholders including the Queensland Council of Civil Liberties and Digital Rights Watch who contend that this offence should be removed from the bill and pursued as standalone legislation.

1.4 Likewise, valid concerns were raised about the drafting of the tort of privacy and how this would work in practice. A careful review of the submissions, especially from legal groups, is warranted by the Attorney-General to ensure the tort delivers on the Australian Law Reform Commission's longstanding recommendations.

1.5 Unfortunately, the recommendations of this inquiry fail to grapple with the substantive concerns raised by the submissions and evidence in the inquiry including:

1. The lack of a roadmap for comprehensive privacy reform
2. The need to urgently address the outdated definition of 'personal information'
3. The failure to implement a 'fair and reasonable' test relating to data, and
4. The continued fiction regarding 'consent' in a digital context.

1.6 The absence of any of these substantive fixes to our broken privacy laws was explained by a departmental official in the following exchange, after being asked why at least the extension of the definition of personal information was not put in the bill, she replied:

> Ms Fitch: As I said, the first tranche that's represented in the current bill is largely things that don't directly and significantly impact on regulated

> entities. I'd draw attention to increased powers for the Office of the Australian Information Commissioner, emergency declarations et cetera.
>
> Senator SHOEBRIDGE: That's a pretty extraordinary proposition to say—that the reason we've got what we've got in this bill is that you don't want anything to impact on regulated entities. That's a pretty extraordinary position for the government to adopt if this is the only meaningful privacy reform. You'll do everything except for anything that impacts on a regulated entity. That surely hasn't been your ambition, has it? 'Don't do anything that actually changes anything'?
>
> Ms Fitch: No, not at all. But what I would say is that the government has made clear that it does seek to do another tranche of reform and, in certain cases, that requires further consultation on the detail of draft proposals.
>
> Senator SHOEBRIDGE: But I didn't mishear you. You've said that you want to make sure that there's nothing in this package of reforms that's going to impact on a regulated entity.

1.7 The Australian Greens believe that, because of this decision by the government to not 'significantly impact on regulated entities', this bill is a serious missed opportunity. We believe that addressing these key issues is urgent and necessary and will consider them in turn.

1. The lack of a roadmap for comprehensive privacy reform

1.8 Almost every submission received by the inquiry noted the uncertainty regarding the overall plan for privacy reform and the need for a publicly stated roadmap from the government for what changes should be expected and when. The lack of this is causing significant uncertainty for businesses and for communities. There was a strong consensus that this roadmap should be provided with this bill and the comprehensive laws tabled as soon as possible, but not less than six months after the next election.

1.9 The Australian Human Rights Commission expressed this in its 'Recommendation 1: The Federal Government set out a clear timeline for when each 'agreed' and 'agreed in principle' amendment will be introduced in future tranches'.

1.10 Three of the most substantive reforms with the broadest agreement are considered in detail below but it is of note that a significant number of other critical reforms were proposed in the Privacy Act Review Report and were agreed or agreed-in-principle by the government before the last election. None of these should be lost and include:

- Concerns relating to the children's privacy code raised including the fact that it doesn't apply to data brokers and EdTech which we believe warrant action.
- Future reform needs to also urgently address platforms that are 'risky by design' as was raised by the Alannah and Madeleine Foundation with algorithmic manipulation a particular concern.

- Likewise, the Human Technology Institute and CHOICE recommended steps to ensure individuals had a right to request meaningful information about how substantially automated decisions with legal or other significant impacts on them are made.
- The Human Technology Institute also raised the need to introduce a power for the Australian Privacy Commissioner to investigate complaints about serious invasions of privacy, and make appropriate declarations.
- Electronic Frontiers Australia argued for the removal of exemptions for small business, political parties and employee records as per the recommendations of the Privacy Act Review. This was supported by CHOICE who also noted the failure of the laws to cover high risk small businesses like real estate agents as a particular concern.
- In addition, submissions argued that reforms urgently need to address high-risk technologies, such as facial recognition technology, noting that this technology remains largely unregulated and has extremely serious human rights impacts.

2. The definition of 'personal information'

1.11 It was a consistent and strong recommendation including from the Office of the Australian Information Commissioner and the Human Technology Institute that this bill, not some future reform, should expand the Privacy Act's definition of 'personal information', as recommended by the Privacy Act Review Report.

1.12 The main issue here is that the definition of 'personal information' doesn't include the kind of information online that we know is being commercialised and weaponized against people right now. This includes real time location data, browsing histories, and related technical and inferred information (such as IP addresses and device identifiers).

1.13 It is plainly obvious that the location of a person's phone or tablet is personal information and yet the laws have not been updated to reflect this. The result is a significant number of predatory marketing and other practices have proliferated to take advantage of this information.

1.14 Other countries have already protected this information in their privacy laws, this is not hard. Multiple international examples are available that could be applied as tried and tested off the shelf solutions.

1.15 In Europe for example, the General Data Protection Regulation (GDPR) defines personal information as any information which is related to an identified or identifiable natural person. This includes any data through which people can be directly or indirectly identified, such as location data. Many businesses operating in Australia, who also operate in Europe, are already compliant with and knowledgeable of the GDPR requirements.

3. Fair and reasonable test

1.16 Many organisations recommended urgent implementation of a fairness obligation or a fair and reasonable test on the use of personal information. Such an obligation would mean organisations would have to handle personal information from collection through to use and disclosure in a manner that is transparent, reasonable, and in line with community expectations.

1.17 Such a change could be implemented as a straightforward amendment to the Privacy Act and given this test is in use in other jurisdictions, including shortly in Western Australia, it is considered by multiple stakeholders as very achievable. This test would also be a way of addressing the Privacy Act's over-reliance on consent as the fair and reasonable test would apply to the use of data, sometimes in novel ways, well after consent was given.

4. Consent

1.18 Finally, it was broadly agreed that the issue of consent must be a priority area for privacy law reform. The current definition of consent in privacy laws is so simplistic as to be meaningless. As a demonstration of this it is worth noting consent is not dependent on understanding.

1.19 Evidence received from Consumer Policy Research Centre showed:

> Australia's current privacy framework disproportionately places the burden on individuals to protect their safety online: Australians would need to spend an average of 30 minutes daily to fully adjust privacy settings on websites and apps rather than accept the company default. Australians need to spend an average of two minutes per website/app managing their privacy, versus our participant in Europe who just spent an average of 3.1 seconds per website/app. Reading privacy policies for daily used sites/apps would take an average of 14 hours. 45% of participants struggled to locate and adjust privacy settings.

1.20 The GDPR provides an existing and functional model for how to remedy this and an equivalent must be implemented here urgently. It can't be that simply clicking 'I agree' to 10 pages of an indigestible corporate word salad is how we sign away our rights to privacy.

Senator David Shoebridge
Member

Appendix 1
Submissions and additional information

Submissions

1 Privacy 108
2 Mr Greg Peak
3 Reset.Tech Australia
4 Free Speech Union of Australia Pty Ltd
5 Uniting Church in Australia, Synod of Victoria and Tasmania
6 BSA | The Software Alliance
7 Mx Rebecca Trapani
8 Alcohol and Drug Foundation (ADF)
9 Global Data Alliance
10 Children and Media Australia
11 auDA - .au Domain Administration Ltd
12 Professor Normann Witzleb, Professor Megan Richardson & Dr Damian Clifford
- Attachment 1
- Attachment 2

13 Human Technology Institute, University of Technology Sydney
14 Australian Lawyers Alliance
15 Office of the Information Commissioner (Qld)
16 Human Rights Act Campaign
17 Queensland Council for Civil Liberties
18 Interactive Games and Entertainment Association (IGEA)
19 Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University
20 Consumer Policy Research Centre
21 CHOICE
22 Australian Information Industry Association (AIIA)
23 Office of the Australian Information Commissioner (OAIC)
24 Justice and Equity Centre
25 Financial Advice Association of Australia
26 Australian Medical Association
27 Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney
28 Insurance Council of Australia
29 Internet Association of Australia
30 Australian Banking Association
31 Attorney-General's Department
32 Arca

33 Food for Health Alliance
34 Dr Lisa Archbold, Professor Mark Burdon, Dr Tegan Cohen & Dr Henry Fraser, Queensland University of Technology
35 Per Capita, Centre of the Public Square
36 Australian Human Rights Commission
37 Clubs Australia
38 ABC
39 Australian Institute of Company Directors (AICD)
40 Special Broadcasting Service (SBS)
41 Digital Industry Group Inc. (DIGI)
42 Australian Industry Group
43 Commercial Radio & Audio
44 Electronic Frontiers Australia Inc
45 Association of Superannuation Funds of Australia (AFSA)
- Attachment 1

46 Council of Small Business Organisations Australia
47 Google Australia
48 Shopping Centre Council of Australia
49 Tech Council of Australia
50 Digital Rights Watch
51 Peter Clarke
52 Mr Michael Rivette
53 IDCARE
54 Dr Michael Douglas
55 Access Now
56 Business Council of Australia (BCA)
57 Meta
58 Australian Christian Lobby
59 Australia's Right to Know (ARTK)
60 Human Rights Law Centre
- Attachment 1
- Attachment 2

61 Alannah and Madeline Foundation
62 ChildFund Australia
63 UNICEF Australia
64 Australian Communications Consumer Action Network (ACCAN)
65 Australian Chamber of Commerce and Industry (ACCI)
66 eSafety Commissioner
67 Law Council of Australia
68 Association for Data-driven Marketing & Advertising (ADMA)
69 Mr Edward Caine
70 Mr Angus Murray & Dr Monique Mann
71 Australian Federal Police

72 Confidential
73 Confidential
74 Confidential
75 National Farmers' Federation

Additional Information

1 Form letter examples 1-5 (899 received in total).

Answers to Questions on Notice

1 Alannah and Madeline Foundation - Answers to spoken questions on notice, 22 October 2024 (received 22 October 2024)
2 Uniting Church in Australia, Synod of Victoria and Tasmania - Answers to spoken questions on notice, 22 October 2024 (received 27 October 2024)
3 Human Technology Institute, University of Technology Sydney - Answers to spoken questions on notice, 22 October 2024 (received 29 October 2024)
4 Australian Human Rights Commission – Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)
5 Emeritus Professor Barbara McDonald and Professor David Rolph, University of Sydney – Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)
6 Office of the Australian Information Commissioner – Answer to spoken question on notice, 22 October 2024 (received 4 November 2024)
7 Justice and Equity Centre - Answer to spoken question on notice, 22 October 2024 (received 4 November 2024)
8 Australia's Right to Know – Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)
9 Attorney-General's Department - Answers to spoken questions on notice, 22 October 2024 (received 5 November 2024)
10 Ai Group - Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)
11 auDA - Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)
12 Council of Small Business Organisations Australia - Answers to spoken questions on notice, 22 October 2024 (received 4 November 2024)

Tabled Documents

1 Any Buyer Accepted, tabled by Reset.Tech Australia at the public hearing on 22 October 2024

Appendix 2
Public hearings

Tuesday 22 October 2024
Committee Room 2S1, Parliament House
Canberra

Uniting Church in Australia, Synod of Victoria and Tasmania (via videoconference)

- Dr Mark Zirnsak, Senior Social Justice Advocate

Children and Media Australia (via videoconference)

- Professor Elizabeth Handsley, President

Alannah and Madeline Foundation (via videoconference)

- Ms Ariana Kurzeme, Director, Policy and Prevention
- Ms Jessie Mitchell, Advocacy Manager

auDA - .au Domain Administration Ltd

- Mr Jordan Carter, Internet Governance and Policy Director
- Ms Annaliese Williams, Specialist Adviser

Tech Council of Australia

- Mr Harry Godber, Head of Policy and Strategy
- Ms Erika Ly, Policy Manager

Reset.Tech Australia (via videoconference)

- Miss Alice Dawkins, Executive Director

Human Technology Institute, University of Technology Sydney (via videoconference)

- Professor Edward Santow, Co-Director
- Ms Sarah Sacher, Policy Specialist

Justice and Equity Centre (via videoconference)

- Ms Ellen Tilbury, Principal Solicitor

Electronic Frontiers Australia Inc (via videoconference)

- Mr John Pane, Chair

Digital Rights Watch (via videoconference)

- Ms Elizabeth O'Shea, Chair

ABC (via videoconference)

- Mr Brett Farrell, Senior Privacy Officer and Privacy Champion
- Ms Kathryn Wilson, Head of Prepublication and Training, ABC Legal

Special Broadcasting Service (SBS) (via videoconference)

- Ms Clare O'Neil, Director, Corporate Affairs
- Ms Lyn Kemmis, Senior Legal Counsel

Australia's Right to Know (ARTK) (via videoconference)

- Ms Georgia-Kate Schubert, Member and Policy and Government Affairs, News Corp
- Ms Bridget Fair, Member and Chief Executive Officer, Free TV Australia
- Ms Kiah Officer, Member and Executive Counsel, Nine
- Mr Hamish Thomson, Member and Head of Legal, Guardian Australia
- Ms Sarah Kruger, Member and Chief Legal and Government Affairs Officer, Commercial Radio and Audio

Australian Industry Group

- Ms Louise McGrath, Head of Industry Development and Policy
- Ms Yoness Blackmore, Principal Advisor - Workplace Relations Policy

Council of Small Business Organisations Australia (via videoconference)

- Mrs Adele Sutton, Head of Policy and Advocacy

Consumer Policy Research Centre (via videoconference)

- Ms Chandni Gupta, Deputy CEO and Digital Policy Director

CHOICE (via videoconference)

- Ms Rosie Thomas, Director of Campaigns
- Mr Rafi Alam, Senior Campaigns and Policy Advisor

Emeritus Professor Barbara McDonald & Professor David Rolph, University of Sydney

- Emeritus Professor Barbara McDonald

Office of the Australian Information Commissioner (OAIC) (via videoconference)

- Ms Carly Kind, Privacy Commissioner

Attorney-General's Department

- Ms Celeste Moran, First Assistant Secretary, Integrity Frameworks Division
- Ms Catherine Fitch, Assistant Secretary, Privacy Reform Taskforce, Integrity Frameworks Division
- Mr Parker Reeve, Assistant Secretary, High Tech Crimes Branch
- Ms Virginia Jay, Director, Privacy Reform Taskforce
- Mr Nathan Whiteman, Director, Cybercrime, Child Abuse Policy and Engagement Section

Australian Human Rights Commission (via videoconference)

- Mrs Lorraine Finlay, Human Rights Commissioner