PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY

Bills Digest | 30 September 2024

Privacy and Other Legislation Amendment Bill 2024

Owen Griffiths and David McGovern
Bills Digest No. 16, 2024–25

Key points

- The Privacy and Other Legislation Amendment Bill 2024 (the Bill) amends the *Privacy Act 1988* to implement an initial tranche of reforms arising from the proposals of a review of the Privacy Act completed in 2022. The Government's response to the review accepted or accepted-in-principle most of the review's proposals.
- Key reforms in the Bill include:
  - establishing a Children's Online Privacy Code
  - creating a statutory tort for serious invasions of privacy
  - new powers for the Minister to direct the Commissioner to develop and register Australian Privacy Principles (APP) codes and conduct public inquiries
  - a new civil penalty for acts and practices which interfere with the privacy of individuals (but which fall below the threshold of 'serious') and a civil penalty infringement notice scheme for specific APP and other obligations.
- More controversial proposals from the Privacy Act review, such as removing an exemption for small businesses, have not been implemented in the Bill.
- The *Criminal Code Act 1995* will also be amended to introduce two offences for the menacing or harassing release of personal data using a carriage service (also known as doxxing).
- The Bill has been referred to the Senate Legal and Constitutional Affairs Legislation Committee for inquiry and report by 14 November 2024.

ISSN 1328-8091

Contents

Date of introduction: 12 September 2024

House introduced in: House of Representatives

Portfolio: Attorney-General

Commencement: Most parts of the Bill will commence the day after Royal Assent with some exceptions (discussed below).

This is a preliminary Bills Digest produced to assist early consideration of the Bill. It will be replaced with a more comprehensive Bills Digest in due course.

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill's home page, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as at September 2024.

Purpose of the Bill

The key purpose of the Privacy and Other Legislation Amendment Bill 2024 (the Bill) is to amend the *Privacy Act 1988* to implement an initial tranche of reforms the Government committed to in its response to the Privacy Act review report.

The Bill will also amend the *Criminal Code Act 1995* (Cth) to introduce two new offences for the menacing or harassing release of personal data using a carriage service (also known as doxxing).

Background

The Privacy Act protects the handling of 'personal information'. This includes the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector. Most of this regulation is outlined in the Australian Privacy Principles (APPs) (contained in Schedule 1 of the Privacy Act) and applies to 'APP entities'. Further information about the APPs, including key concepts such as 'personal information' and 'APP entity' is available on the Office of the Australian Information Commissioner (OAIC) website.

The Office of the Australian Information Commissioner (OAIC) is the agency responsible for monitoring compliance with, and enforcement of, the Privacy Act. A breach of the Privacy Act does not in itself give rise to a cause of action for any individuals affected by a breach, although they may lodge a complaint with the Commissioner which may be investigated. Currently, an APP entity which engages in a serious or repeated interference with privacy may be subject to a civil penalty.

The Privacy Act review report was publicly released by the Attorney-General on 16 February 2023. The review began in October 2020 following recommendations made in the *Digital platforms inquiry – final report* published by the Australian Competition and Consumer Commission (ACCC) in 2019, and incorporated work on amendments to the Privacy Act which had been previously announced in March 2019. The ACCC's report noted that in response to the increasing collection and use of personal information a number of other jurisdictions, including the European Union (EU), Japan and certain US states had recently reformed their privacy laws (p. 24), and proposed several reforms to the Privacy Act (recommendations 16-19). Previewing upcoming reforms in January 2023, the Attorney-General reportedly acknowledged that international reforms, especially the European Union's General Data Protection Regulation (GDPR) were significant considerations.

The Government response to the Privacy Act review report was released on 28 September 2023. Of the 116 proposals made the government 'agreed' to 38 proposals, 'agreed-in-principle' to 68 proposals and 'noted' 10 proposals. In his second reading speech for the Bill, the Attorney-General stated that the Bill 'implements a first tranche of agreed recommendations of the Privacy Act review, ahead of consultation on a second tranche of reforms'.

On 11 March 2024, the Attorney-General announced a national public consultation 'on measures to address the practice of doxxing' (aligning with proposal 4.7 of the Privacy Act

review). The consultation followed an incident where details of almost 600 Jewish writers, artists and academics in a Whatsapp group were published by pro-Palestinian activists.

Committees

On 18 September 2024, the Senate Standing Committee of Scrutiny of Bills deferred consideration of the Bill (p. 21). The next day the Bill was referred to the Senate Legal and Constitutional Affairs Committee for inquiry and report by 11 November 2024. Submissions have been requested by 11 October 2024. Further information is available at the inquiry webpage.

Non-government parties/independents

Non-government parliamentarians have previously emphasised the need for privacy reforms to be coordinated with other related legislation. For example, in their dissenting committee report on the Digital ID Bill 2023, Coalition senators recommended that Bill only be considered 'once the reforms of the Privacy Act are introduced … to ensure that privacy, data protections and compliance requirements are consistent and coordinated'.

Senator Michaelia Cash reportedly stated the Coalition would 'closely examine the Bill' and drew attention to potential new costs for businesses, the role of class action law firms and the interaction with other proposed legislation. She stated '[w]e recognise the need for appropriate reform, but privacy is both highly technical and far-reaching'.

The Greens spokesperson Senator David Shoebridge reportedly characterised the Bill's reforms as an 'extraordinarily unambitious proposal'. While the Greens welcomed the provision for a Children's Online Privacy Code and were broadly supportive of the new doxxing offences, they flagged potential amendments to include further privacy protections and raised the issue of OAIC funding.

Major interest groups

Privacy reforms

Major interest groups have mostly focused on what isn't included in the Bill. For example, business groups such as the Australian Chamber of Commerce and Industry (ACCI), Australian Industry Group (Ai Group) and the Council of Small Business Organisations Australia welcomed the fact that the Bill did not include additional regulatory burdens on businesses by keeping the current exemptions for small businesses and for employee records. ACCI welcomed 'the decision of the Attorney-General to continue consulting with stakeholders on more far-reaching aspects of the proposed reforms'.

In contrast, the Australian Information Industry Association (AIIA) was disappointed that the Bill did not remove the small business exemption. It 'firmly believed all businesses, regardless of size, should be held accountable for protecting the privacy of Australians and their personal and sensitive information'. The AIIA and the Tech Council also expressed the view the Bill should have included the concept of 'controllers and processors'. The AIIA stated the '… distinction between data controllers and processors, as enshrined in the European Union's [General Data Protection Regulation], is essential for clearly defining responsibilities in the management of personal data'.

The Privacy Commissioner, Carly Kind welcomed the reform noting that that 'enhanced civil penalty regime will add significantly to our enforcement toolkit' and that '[t]he statutory tort would also fill a gap in our privacy landscape'. However, she stated 'much more needed to be done' and described further reform of the Privacy Act as 'urgent'. Ms Kind also highlighted a need to bring small businesses within the Privacy Act's remit.

Digital Rights Watch considered the Bill was a 'good first step' but called on the government 'to lay out a clear time frame for the remaining 100+ reforms that it has committed to implementing'. Electronic Frontiers Australia highlighted the need to redefine and update key terms such as 'consent' and 'personal information' and urged the Government to commit to further reform 'before the next federal election'.

The proposed Children's Online Privacy Code was supported by a number of organisations which have been advocating for this initiative. These included Reset Australia, Human Rights Watch and Child Fund Australia.

Doxxing and a statutory tort for serious invasions of privacy

The public submissions made in March 2024 to the Attorney-General's Department's consultation on proposed legal reforms to address doxxing harms and behaviours, including a statutory tort for serious invasions of privacy are available here. A range of views were expressed. For example, Australia/Israel & Jewish Affairs Council (AIJAC) submission considered the existing laws were insufficient and highlighted the impact that doxxing has had on victims.

The Law Council of Australia cautioned that any changes must 'reflect a very careful balance between addressing the unacceptable harm to individuals caused by illegitimate doxxing behaviours, and ensuring that legitimate instances of information publication are not prevented'. Professor Anne Twomey urged 'careful consideration … to ensure that there is no breach of the implied freedom of political communication'.

Key issues and provisions

Codes, powers and enforcement

APP codes and temporary APP codes developed and registered at the direction of the Minister

APP codes are written codes of practice about information privacy which set out how the APPs are to be applied or complied with by specified APP entities and can impose additional requirements. Once registered, APP codes are binding on the specified APP entities.

Currently APP codes may be developed by 'code developers' (such as a body representing a group of APP entities) on their own initiative or by request of the Commissioner (if satisfied it is in the public interest). If the Commissioner's request has not been complied with, or the Commissioner has decided not to register the APP code, the Commissioner can also develop an APP code if 'satisfied that it is in public interest' (sections 26E, 26F and 26G).

Schedule 1, Part 2 of the Bill contains amendments to the Privacy Act to enable the Minister to direct the Commissioner to develop and register APP codes and temporary APP codes. These codes must not cover certain acts and practices which are exempt under the Privacy Act (such as individuals acting in a non-business capacity, organisations acting under Commonwealth contract and employee records).

The Minister may direct the Commissioner to develop an APP code 'if the Minister is satisfied that it is in the public interest'. The Minister may direct the Commissioner to develop a temporary APP code if the Minister is satisfied that 'it is in the public interest' and 'the code should be developed urgently'. The period a temporary APP code may be in force 'must not be longer than 12 months'.

While a registered APP code is a legislative instrument (section 26B) and subject to the usual parliamentary disallowance processes, the Minister's written directions to the Commissioner would not be legislative instruments (**proposed subsections 26GA(3) and 26GB(3)**). Further, a temporary APP code would not be subject to the usual parliamentary disallowance processes (**proposed subsection 26GB(8)**). The Explanatory Memorandum states this is necessary to 'establish an immediate, clear and certain legal basis' for temporary APP codes and noted certain safeguards in the code development process (pp 34–35). Nonetheless, this may represent a significant new ministerial power to direct the Commissioner to impose privacy requirements on specified APP entities without parliamentary oversight.

Penalties and remedies

Currently section 13G of the Privacy Act outlines civil penalties which may be imposed for 'serious' or 'repeated' interferences with privacy. The amendments in **Schedule 1, Part 8** will refocus section 13G on 'serious' interferences with privacy. Whether an act or practice was done or engaged in 'repeatedly or continuously' will be one of the factors which a court may take into account in determining if an interference with privacy was 'serious'. The maximum amounts of the penalties in section 13G (substantially increased in 2022) would remain the same.

Other provisions will expand the Commissioner's options to seek penalties and other remedies for interferences with privacy which may not reach the threshold of being 'serious'. **Proposed section 13H** creates a civil penalty if an entity does an act, or engages in a practice, which interferes with the privacy of an individual. The maximum penalty would be 2,000 penalty units for an individual (currently $626,000) or 10,000 penalty units for a body corporate ($3,130,000).

Proposed section 13K and amendments to section 80UB will introduce a scheme for civil penalty infringement notices to be issued for breaches of a number of specific obligations under the APPs and non-compliant eligible data breach statements. Examples of specific obligations include APP 1.4 (failure to include required information in an APP privacy policy) or non-compliance with subsection 26WK(3) which sets out what must be contained in an eligible data breach statement. **Proposed paragraph 13K(1)(x)** would allow other APP obligations to be prescribed by regulation as part of the infringement notice scheme.

The maximum civil penalty for a breach of proposed subsections 13K(1) and (2) would be 200 penalty units (currently $62,600). However, under subsection 104(2) of the *Regulatory Powers (Standard Provisions) Act 2014* the amount payable under an infringement notice for one alleged contravention would be 12 penalty units for an individual (currently $3,756) and 60 penalty units for a body corporate (currently $18,780). Further proposed amendments to section 80UB of the Privacy Act would modify the applicable number of penalty units for infringement notices given to publicly listed corporations which would be worked out by 'multiplying the number of alleged contraventions by 200'.

Schedule 1, Part 9 will insert **proposed section 80UA** which will provide that Federal Courts will also have the power to make a range of orders in civil penalty proceedings where a contravention of a civil penalty provision under the Privacy Act has been established.

Public inquiries

Part IV of the Privacy Act deals with the functions of the Commissioner. **Schedule 1, Part 10** would insert provisions into Part IV to allow the Minister to direct the Commissioner to conduct, or to approve the Commissioner conducting, public inquiries into specified matters relating to privacy. The Minister's direction or approval would not be a legislative instrument. For the purposes of a public inquiry, the Commissioner would be able invite public submissions and use existing investigation powers to obtain documents and examine witnesses (sections 44 and 45).

After completing the public inquiry, Commissioner must prepare a written report for the Minister. If any entities have been specified in the Minister's direction or approval of the public inquiry, they will also receive a copy. The Minister must table a copy before each House of the Parliament within 15 sitting days and the Commissioner must make the report publicly available (unless the Minister otherwise directs).

Monitoring and investigation powers

Schedule 1, Part 14 includes provisions which will insert new divisions into Part VIB to add monitoring and investigation powers set out in the *Regulatory Powers (Standard Provisions) Act 2014*. These powers include entry, search and seizure powers. The Explanatory Memorandum (p. 65) states:

> Bringing the Information Commissioner's regulatory powers in line with the standard provisions would provide additional powers and greater safeguards to ensure they are robust and align with best practice. Additionally, ensuring uniformity with the standard provisions would bring the Information Commissioner's powers in line with comparable domestic regulators, and increase legal certainty for entities and individuals who are subject to those powers.

Children's Online Privacy Code

The introduction of a Children's Online Privacy Code (COPC) was a proposal of the Privacy Act review (proposal 16.5, p 157). The Government has indicated it will provide $3 million funding to the OAIC to develop a Children's Online Privacy Code (COPC) over 3 years.

Schedule 1, Part 4 contains the provisions to establish a COPC. **Proposed section 26GC** provides that the Commissioner must develop and register an APP code about online privacy for children within 24 months. **Item 30** will insert a definition of the term ***child*** into the Privacy Act meaning 'an individual who has not reached 18 years' which is consistent with the *Online Safety Act 2021* and UK's age appropriate design code.

The Commissioner will have a broad discretion regarding who 'may' be consulted in developing the COPC (**proposed subsection 26GC(8)**). This differs slightly from the Privacy Act review which proposed the developer 'should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry' (p. 157).

Before registering the COPC, the Commissioner must make a draft of the COPC available, invite and give consideration to public submissions and consult with the eSafety Commissioner and the National Children's Commissioner (**proposed subsection 26GC(9)**).

The COPC must set out how the APPs are to be applied or complied with in relation to the privacy of children. However, the COPC will not cover some acts and practices which are exempt under the Privacy Act such as individuals acting in non-business capacity, organisations acting under Commonwealth contract or employee records.

Under **proposed subsection 26GC(5)** the entities who will be bound by the COPC would be providers of social media services, relevant electronic services or designated internet services (within the meaning of the *Online Safety Act 2021*) who are 'likely to be accessed by children' and are not providing a health service. There would also be a capacity to specify other APP entities for the purposes of the COPC.

Emergency and eligible data breach declarations

Emergency declarations

Part VIA of the Privacy Act contains provisions dealing with personal information in emergencies or disasters. This includes provision for the Prime Minister or the Minister to make a declaration of emergency in certain circumstances to allow for the wider sharing of information (sections 80J and 80K).

Schedule 1, Part 3 will make amendments to Part VIA to require a more targeted approach to emergency declarations. In particular, **proposed section 80KA** will set out the matters which must be specified in an emergency declaration. These matters include:

- the kind or kinds of personal information to which the declaration applies
- the entity or class of entities that may collect, use or disclose the personal information and the entity or class of entities that the personal information may be disclosed to
- one or more permitted purposes of the collection, use or disclosure (these must be purposes which directly relate to the Commonwealth's emergency or disaster response).

Eligible data breach declarations

Part IIIC of the Privacy Act establishes a scheme which requires regulated entities to notify certain individuals and the Commissioner about 'eligible data breaches'. Data breaches are 'eligible' if they are likely to result in serious harm to any of the individuals to whom the information relates (section 26WE). More information is available on the OAIC website regarding the Notifiable Data Breaches scheme.

Schedule 1, Part 7 of the Bill will insert **proposed Division 5** into Part IIIC to allow the Minister to make eligible data breach declarations which, similarly to emergency declarations, would permit 'collections, uses and disclosures of personal information…to prevent or reduce the risk of harm to individuals' (Explanatory Memorandum, p. 46). These declarations can be made where the Minister is satisfied it is 'necessary or appropriate' to prevent or reduce a risk of harm arising from the misuse of personal information from an eligible data breach (**proposed subsection 26X(1)**).

As with the amendments to facilitate emergency declarations, an eligible data breach declaration must specify particular matters:

- the kind or kinds of personal information to which the declaration applies
- the entity or class of entities that may collect, use or disclose the personal information
- the entity or class of entities that the personal information may be disclosed to
- one or more permitted purposes of the collection, use or disclosure.

A 'permitted purpose' must be a purpose directly related to preventing or reducing a risk of harm to one or more individuals at risk from the eligible data breach.

Restrictions on disclosures and disallowance

For both emergency and eligible data breach declarations the specified entities or classes of entities may include State and Territory authorities but must not be, or include, a media organisation (**proposed subsections 80KA(2) and 26X(3)**).

Both emergency and eligible data breach declarations would be legislative instruments which will not be subject to the usual parliamentary disallowance process (**proposed subsections 80J(3) and 26X(10)**). The Explanatory Memorandum states this is necessary 'to ensure that decisive action can be taken' and 'to establish an immediate, clear and certain legal basis for entities to handle personal information…'. (pp 35 and 48).

Overseas data flows

APP 8 addresses cross-border disclosures of personal information. In particular, APP 8.1 provides that before an APP entity discloses personal information about an individual to an

overseas recipient, the entity must take 'reasonable steps' to ensure that the recipient does not breach the APPs (except APP 1) in relation to that information. This operates in conjunction with section 16C of the Privacy Act which essentially makes APP entities accountable for breaches of the APPs where they have disclosed personal information about an individual to an overseas recipient under APP 8.

APP 8.2 provides exceptions from the obligations under APP 8.1. This includes APP 8.2(a) which provides an exception where the recipient is subject to a law or binding scheme with 'substantially similar' protections for personal information as the APPs. The amendments in **Schedule 1, Part 6** will allow the Minister to prescribe countries and binding schemes which would fall under the existing exception in APP 8.2(a).

Proposed paragraph 8.2(aa) amends APP 8.2 to include a new exception to APP 8.1 where countries or binding schemes are prescribed under **proposed APP 8.3.** Amendments will also be made to the regulation-making power in section 100 of the Privacy Act to provide that the Minister may only prescribe a country or binding scheme where:

- the laws of the country, or the binding scheme protect personal information in a way that, 'overall, is at least substantially similar to the way in which' the APPs protect information and
- there are mechanisms that the individual can access to take action to enforce that protection.

The Attorney-General's second reading speech indicated the amendments would give businesses and individuals 'greater confidence' in the safety of personal information and to 'reduce costs' for businesses when entering into arrangements with overseas entities.

Article 45(3) of the EU's GDPR contains comparable provision for the European Commission to decide that a non-EU country 'has an adequate level of data protection' to facilitate legal international data flows without further safeguards. Due to a lapse of the framework enabling commercial data transfers between the US and the EU between July 2020 and July 2023, common business practices including Facebook's operations were potentially in breach of the GDPR. Consequently, the Irish Data Protection Authority issued a 1.2 billion euro fine to Meta in May 2023. (This decision is being appealed by Facebook's parent company, Meta.) Countries which have a comparable provision in privacy laws include Japan and New Zealand.

Automated decision-making and privacy policies

Currently, the APPs regulate the content and availability of privacy policies of APP entities (APP 1.3–1.6). **Schedule 1, Part 15** would introduce new requirements for APP entities concerning the information that must be included in their privacy policies about the kinds of personal information used, and types of decisions made, in automated decision-making.

Proposed subclause APP 1.7 would require an APP entity to include certain information if:

- the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision
- the decision could reasonably be expected to significantly affect the rights or interests of an individual and

- 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.

The information which must be included in the privacy policy is set out in **proposed subclause APP 1.8.** These are:

- the kinds of personal information used in the operation of such computer programs
- the kinds of such decisions made solely by the operation of such computer programs
- 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.

The amendments in **Schedule 1, Part 15** would commence 24 months after Royal Assent.

Statutory tort for serious invasions of privacy

There have been a number of proposals for the creation of a statutory tort for serious invasions of privacy, including by the Australia Law Reform Commission (ALRC) in its report on *Serious Invasions of Privacy in the Digital Era* in 2014 (recommendation 4-1). The Privacy Act review proposed the tort should be introduced 'in the form recommended by the ALRC' (proposal 27.1, p 287). The Government response accepted this proposal in-principle but also noted that it would undertake further consultation with 'media organisations on additional safeguards for public interest journalism' (p 19).

Schedule 2 of the Bill will insert **proposed Schedule 2** into the Privacy Act to establish a cause of action for serious invasions of privacy. The intention is that the Schedule will be read and construed separately from the rest of the Privacy Act. The new provisions in **proposed Schedule 2** would commence on the earlier of Proclamation or 6 months after Royal Assent.

Cause of action

Under **proposed subclause 7(1)**, a plaintiff will have a cause of action in tort against a defendant where:

- the defendant invaded the plaintiff's privacy by doing one or both of the following:
  - intruding upon the plaintiff's seclusion
  - misusing information that relates to the plaintiff and
- a person in the position of the plaintiff would have had 'a reasonable expectation of privacy in all of the circumstances'
- the invasion of privacy was intentional or reckless and
- the invasion of privacy was serious.

The term ***intruding upon the seclusion*** of an individual is defined in **proposed subclause 6(1)** as including (but not being limited to) 'physically intruding into the person's private space' and 'watching, listening to or recording the person's private activities or private affairs'. Similarly, the term ***misusing information*** that relates to an individual would be defined as including (but not being limited to) 'collecting, using or disclosing information about the individual'.

Guidance on a threshold regarding how closely information must 'relate to the plaintiff' does not appear to be included. However, **proposed subclause 7(7)** clarifies that where a defendant invades the plaintiff's privacy by misusing information that relates to the plaintiff, 'it is immaterial whether the information was true'.

Under **proposed subclause 7(2)** the new tort would be 'actionable without proof of damage'. A range of factors are listed which a court may consider in determining whether 'a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances' and whether the invasion of privacy was serious (**proposed subclauses 7(5) and (6)**).

Proposed clause 14 will set limitation periods within which actions must be commenced. Plaintiffs must commence an action before the earlier of '1 year after the day on which the plaintiff became aware of the invasion of privacy' and 'the day that is 3 years after the invasion of privacy occurred'. If the plaintiff was under 18 at the time when the invasion of privacy occurred, they must commence an action before their 21st birthday.

Defences

Where a defendant adduces evidence that there was a public interest in the invasion of privacy, the plaintiff must satisfy the court that this public interest is outweighed by the public interest in protecting the plaintiff's privacy (**proposed subclause 7(3)**).

Proposed clause 8 lists a range of other defences to claims of invasion of privacy including:

- where it was required or authorised by or under an Australian law or court/tribunal order
- where the plaintiff, or another authorised person, expressly or impliedly consented
- where the defendant reasonably believed it was necessary 'to prevent or lessen a serious threat to the life, health or safety of a person'
- where it was both incidental to the exercise of a lawful right of defence of persons or property and 'proportionate, necessary and reasonable'.

It will also be a defence to a cause of action where the invasion of privacy has occurred 'by publishing' within the meaning of defamation law and there is a defamation law 'related defence' which the defendant is able to establish. These 'related defences' would be:

- a defence of absolute privilege (such as publication of parliamentary or court proceedings)
- a defence for publication of public documents
- a defence of fair report of proceedings of public concern.

These three defences are not the only defences available in defamation law, but the Explanatory Memorandum indicates the other defences were not included 'because they are not relevant in the context of the statutory tort' (p. 91).

Damages and remedies

Under the new tort, courts may award damages for 'emotional distress'. Courts may also award exemplary or punitive damages for invasions of privacy in exceptional circumstances (damages intended to deter or sanction conduct) but will not be able to award aggravated damages (intended to compensate the plaintiff for egregious harm).

Proposed subclause 11(5) sets out a maximum cap for damages for non-economic loss and exemplary or punitive damages, which must not exceed the greater of $478,550 or the maximum amount of damages for non-economic loss under defamation law. The model defamation provisions include a mechanism to adjust the maximum damages amount over time (section 35). An ongoing link to the level of defamation damages for non-economic loss means the maximum damages available for invasions of privacy is likely to rise with inflation. Courts will also be able to grant a range of other remedies in addition to, or instead of, damages 'as the court thinks appropriate in the circumstances'.

Journalists and other exclusions

Proposed clause 15 provides **proposed Schedule 2** would not apply to an invasion of privacy to the extent it involves the collection, preparation for publication or publication of journalistic material by a journalist, their employer, a person assisting employed or engaged by the journalist's employer or a person assisting a journalist in a professional capacity.

The scope of this exclusion is limited by the definition of certain terms. The term ***journalist*** is defined as a person who 'works in a professional capacity as a journalist' and is subject to 'standards of professional conduct' or 'a code of practice' that applies to journalists (**subclause 15(2)**). Material will be ***journalistic material*** where it:

- has the character of news, current affairs or a documentary; or
- consists of commentary or opinion on, or analysis of, news, current affairs or a documentary (**subclause 15(3)**).

Proposed Schedule 2 would also not apply to invasions of privacy by:

- an ***enforcement body*** to the extent the enforcement body believes it is reasonably necessary for ***enforcement related activities*** (using the definitions in subsection 6(1) of the Privacy Act)
- an ***intelligence agency*** (using the definition in subsection 6(1) of the Privacy Act), or to the extent it involves a disclosure to, or by, an ***intelligence agency***
- a person who is under 18 years of age (**proposed clauses 16, 17 and 18**).

Doxxing offences

Schedule 3 contains amendments to the *Criminal Code* to insert two new doxxing offences.

Proposed section 474.17C would make it an offence to use a carriage service to make available, publish or otherwise distribute 'personal data' in a way that 'reasonable persons would regard as being, in all the circumstances, menacing or harassing' towards the individuals concerned. The maximum penalty for this offence would be 6 years imprisonment.

Unlike the Privacy Act, which uses a concept of 'personal information', the definition of ***personal data*** in the new offence would be limited to 'information about the individual that enables the individual to be identified, contacted or located'. This definition would expressly include a number of types of ***personal data*** such as an individual's name, image, telephone number, email address, online account, residential or work address, place of education or place of worship.

Proposed section 474.17D would also make it an offence to use a carriage service to make available, publish or otherwise distribute the 'personal data' of 'one or more members of a group'. Similar to the above offence, the person must engage in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards the members. For this offence to apply, the person must engage in the conduct 'in whole or in part' because of their belief that 'the group is distinguished by one or more protected attributes, such as race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin' (Explanatory Memorandum, p 101). However, it will be immaterial whether the group is actually distinguished by the relevant attributes (**proposed subsection 474.17D(3)**).

The maximum penalty for this offence would be 7 years imprisonment.

Other provisions

Schedule 1, Part 1 will amend the objects of the Privacy Act to clarify that the promotion of the protection of privacy is 'with respect to' personal information as well as to 'recognise the public interest in protecting privacy' (**proposed paragraphs 2A(a) and (aa)**).

Schedule 1, Part 5 will amend APP 11 which obliges APP entities to take reasonable steps to protect the security of personal information which they hold and destroy or de-identify information they no longer need. **Proposed APP 11.3** would clarify that these steps include 'technical and organisational measures'. In September 2022, following a high profile hack of Optus which exposed private data, the Attorney-General and Commissioner highlighted that organisations retaining data they no longer needed exacerbated the impact of data breaches.

Schedule 1, Part 11 will expand the declarations which the Commissioner can make where an investigation has found a complaint has been substantiated (section 52). Declarations could include requiring persons or entities to take any reasonable act or course of conduct to 'prevent or reduce any reasonably foreseeable loss or damage that is likely to be suffered'.

Schedule 1, Part 12 will amend the annual reporting requirements for the Commissioner to include further details regarding number of complaints, complaints not investigated and the grounds for decisions.

Schedule 1, Part 13 will expand the Commissioner's grounds to not to investigate a complaint to include where it 'has been' dealt with by a recognised external dispute resolution scheme.

Acknowledgement of Country

We acknowledge the traditional owners and custodians of country throughout Australia and acknowledge their continuing connection to land, waters and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

The Parliamentary Library of Australia was established in 1901 and serves as a trusted source of information, analysis and advice for the Australian Parliament. The Library is part of the Department of Parliamentary Services.

Our services are confidential, impartial, and offered on an equal basis to all parliamentarians, parliamentary committees, and to staff acting on their behalf.

Our published material is available to everyone at:

aph.gov.au/library

Australian Parliamentary Library

@ParlLibrary

Confidential, Impartial, Timely

ISSN 1328-8091