



# **Privacy and Other Legislation Amendment Act 2024**

**No. 128, 2024**

**An Act to amend the law in relation to privacy and  
the criminal law, and for related purposes**

Note: An electronic version of this Act is available on the Federal Register of Legislation  
(<https://www.legislation.gov.au/>)



---

## Contents

1	Short title.....	1
2	Commencement .....	2
3	Schedules .....	3
4	Review of operation of amendments made by Schedule 3 .....	3
<b>Schedule 1—Privacy reforms</b>		<b>4</b>
Part 1—Objects of the Act		4
<i>Privacy Act 1988</i>		4
Part 2—APP codes		5
<i>Privacy Act 1988</i>		5
Part 3—Emergency declarations		8
<i>Privacy Act 1988</i>		8
Part 4—Children’s privacy		14
<i>Privacy Act 1988</i>		14
Part 5—Security, retention and destruction		18
<i>Privacy Act 1988</i>		18
Part 6—Overseas data flows		19
<i>Privacy Act 1988</i>		19
Part 7—Eligible data breaches		21
<i>Privacy Act 1988</i>		21
Part 8—Penalties for interference with privacy		31
<i>Data Availability and Transparency Act 2022</i>		31
<i>Digital ID Act 2024</i>		31
<i>Identity Verification Services Act 2023</i>		31
<i>Privacy Act 1988</i>		31
Part 9—Federal court orders		40
<i>Privacy Act 1988</i>		40
Part 10—Commissioner to conduct public inquiries		42
<i>Privacy Act 1988</i>		42

---

Part 11—Determinations following investigations	46
<i>Privacy Act 1988</i>	46
Part 12—Annual reports	47
<i>Australian Information Commissioner Act 2010</i>	47
Part 13—External dispute resolution	48
<i>Privacy Act 1988</i>	48
Part 14—Monitoring and investigation	49
<i>Competition and Consumer Act 2010</i>	49
<i>Crimes Act 1914</i>	49
<i>Data-matching Program (Assistance and Tax) Act 1990</i>	49
<i>National Health Act 1953</i>	50
<i>Privacy Act 1988</i>	50
Part 15—Automated decisions and privacy policies	60
<i>Privacy Act 1988</i>	60
<b>Schedule 2—Serious invasions of privacy</b>	62
<i>Privacy Act 1988</i>	62
<b>Schedule 3—Doxxing offences</b>	81
<i>Criminal Code Act 1995</i>	81



# Privacy and Other Legislation Amendment Act 2024

No. 128, 2024

---

## An Act to amend the law in relation to privacy and the criminal law, and for related purposes

[Assented to 10 December 2024]

The Parliament of Australia enacts:

### 1 Short title

This Act is the *Privacy and Other Legislation Amendment Act 2024*.

---

## 2 Commencement

- (1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Sections 1 to 4 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	10 December 2024
2. Schedule 1, Parts 1 to 7	The day after this Act receives the Royal Assent.	11 December 2024
3. Schedule 1, items 45 and 46	Immediately after the commencement of the provisions covered by table item 5.	11 December 2024
4. Schedule 1, item 47	The later of: (a) immediately after the commencement of the provisions covered by table item 5; and (b) immediately after the commencement of the <i>Digital ID Act 2024</i> .	11 December 2024 (paragraph (a) applies)
5. Schedule 1, items 48 to 58	The day after this Act receives the Royal Assent.	11 December 2024
6. Schedule 1, Parts 9 to 14	The day after this Act receives the Royal Assent.	11 December 2024
7. Schedule 1, Part 15	The day after the end of the period of 24 months beginning on the day this Act receives the Royal Assent.	10 December 2026
8. Schedule 2	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	10 June 2025

---

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
9. Schedule 3	The day after this Act receives the Royal Assent.	11 December 2024

---

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

- (2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

### 3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

### 4 Review of operation of amendments made by Schedule 3

- (1) The Minister must cause an independent review to be undertaken of the operation of the amendments made by Schedule 3 to this Act.
- (2) The review must commence as soon as practicable after the end of the period of 24 months starting at the commencement of that Schedule.
- (3) The persons who undertake the review must give the Minister a written report of the review within 6 months of the commencement of the review.
- (4) The Minister must cause a copy of the report of the review to be tabled in each House of the Parliament within 15 sitting days of that House after the report is given to the Minister.

## Schedule 1—Privacy reforms

### Part 1—Objects of the Act

#### *Privacy Act 1988*

##### **1 Paragraph 2A(a)**

Repeal the paragraph, substitute:

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

##### **2 Paragraph 2A(h)**

Omit “obligation”, substitute “obligations”.



## **Part 2—APP codes**

### ***Privacy Act 1988***

#### **3 Subsection 6(1)**

Insert:

*temporary APP code*: see section 26GB.

#### **4 Section 26G (at the end of the heading)**

Add “—following a request”.

#### **5 After section 26G**

Insert:

#### **26GA Development of APP codes by the Commissioner—at the direction of the Minister**

*Minister may give direction*

- (1) The Minister may, in writing, direct the Commissioner to develop an APP code if the Minister is satisfied that it is in the public interest:
  - (a) to develop the code; and
  - (b) for the Commissioner to develop the code.
- (2) Without limiting subsection (1), a direction under that subsection may:
  - (a) specify one or more matters that the code must deal with; and
  - (b) specify the APP entities, or a class of APP entities, that are to be bound by the code.
- (3) A direction under subsection (1) is not a legislative instrument.

*Commissioner must develop and register code*

- (4) The Commissioner must develop and register an APP code if the Minister has given the Commissioner a direction under subsection (1) to develop the code.

*Matters covered by code*

- (5) Despite paragraph 26C(3)(b), the APP code must not cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3).

*Consultation etc.*

- (6) In developing the APP code, the Commissioner may consult any person the Commissioner considers appropriate.
- (7) Before registering the APP code under section 26H, the Commissioner must:
- (a) make a draft of the code publicly available; and
  - (b) invite the public to make submissions to the Commissioner about the draft within a specified period (which must run for at least 40 days); and
  - (c) give consideration to any submissions made within the specified period.

**26GB Development of APP codes by the Commissioner—temporary APP codes**

*Minister may give direction*

- (1) The Minister may, in writing, direct the Commissioner to develop an APP code (a **temporary APP code**) if the Minister is satisfied that:
- (a) it is in the public interest:
    - (i) to develop the code; and
    - (ii) for the Commissioner to develop the code; and
  - (b) the code should be developed urgently.
- (2) Without limiting subsection (1), a direction under that subsection may:
- (a) specify one or more matters that the code must deal with; and
  - (b) specify the APP entities, or a class of APP entities, that should be bound by the code.
- (3) A direction under subsection (1) is not a legislative instrument.

*Commissioner must develop and register code*

- (4) The Commissioner must develop and register a temporary APP code if the Minister has given the Commissioner a direction under subsection (1) to develop the code.

*Matters covered by code*

- (5) However, despite paragraph 26C(3)(b), the temporary APP code must not cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3).

*Consultation etc.*

- (6) In developing the temporary APP code, the Commissioner may consult any person the Commissioner considers appropriate.

*Period code is in force*

- (7) The period set out for the temporary APP code for the purposes of paragraph 26C(2)(c) must not be longer than 12 months.

Note: Paragraph 26C(2)(c) deals with the period during which the code is in force.

*Disallowance*

- (8) Section 42 (disallowance) of the *Legislation Act 2003* does not apply to a temporary APP code that is a registered APP code.

Note: A registered APP code is a legislative instrument: see subsection 26B(2).

## **6 Paragraph 26H(1)(b)**

Omit “section 26G”, substitute “section 26G, 26GA or 26GB”.

## Part 3—Emergency declarations

### *Privacy Act 1988*

#### 7 Subsection 80G(1)

Insert:

*entity* includes the following:

- (a) a person;
- (b) an agency;
- (c) an organisation.

#### 8 Section 80H

Repeal the section.

#### 9 Subsections 80J(1) and (2)

After “Minister may”, insert “, by writing,”.

#### 10 At the end of section 80J

Add:

- (3) A declaration under this section is a legislative instrument, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to the declaration.

#### 11 Subsection 80K(1)

After “Minister may”, insert “, in writing,”.

#### 12 At the end of section 80K

Add:

- (3) A declaration under this section is a legislative instrument, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to the declaration.

#### 13 After section 80K

Insert:

## **80KA Matters covered by declarations**

### *Matters that must be specified*

- (1) Without limiting section 80J or 80K, an emergency declaration must specify the following matters:
  - (a) the kind or kinds of personal information to which the declaration applies;
  - (b) the entity or class of entities that may collect, use or disclose the personal information;
  - (c) the entity or class of entities that the personal information may be disclosed to;
  - (d) one or more permitted purposes of the collection, use or disclosure.

Note: See section 80P (authorisation of collection, use and disclosure of personal information).

### *Specified entities*

- (2) An entity or class of entities specified for the purposes of paragraph (1)(c):
  - (a) may include a State or Territory authority; and
  - (b) must not be or include a media organisation, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.

### *Specified permitted purposes*

- (3) A permitted purpose specified for the purposes of paragraph (1)(d) must be a purpose that directly relates to the Commonwealth's response to an emergency or disaster in respect of which an emergency declaration is in force.
- (4) Without limiting subsection (3), any of the following may be specified as a permitted purpose in relation to an emergency or disaster:
  - (a) identifying individuals who:
    - (i) are or may be injured, missing or dead as a result of the emergency or disaster; or

- (ii) are or may be at risk of injury, going missing or death as a result of the emergency or disaster; or
    - (iii) are or may be otherwise involved in or affected by the emergency or disaster; or
    - (iv) are or may be at risk of otherwise being involved in or affected by the emergency or disaster;
  - (b) assisting individuals involved in or affected by the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance;
  - (c) assisting individuals who are or may be at risk of being involved in or affected by the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance;
  - (d) assisting with law enforcement in relation to the emergency or disaster;
  - (e) coordination or management of the response to the emergency or disaster;
  - (f) ensuring that responsible persons for individuals who are, or may be, involved in the emergency or disaster are appropriately informed of matters that are relevant to:
    - (i) the involvement of those individuals in the emergency or disaster; or
    - (ii) the response to the emergency or disaster in relation to those individuals;
  - (g) ensuring that responsible persons for individuals who are or may be at risk of being involved in or affected by the emergency or disaster are appropriately informed of matters that are relevant to:
    - (i) the involvement of or effect on those individuals in the emergency or disaster; or
    - (ii) the response to the emergency or disaster in relation to those individuals.
- (5) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, or any other provision of this Act, an emergency declaration may provide differently for:
- (a) different kinds of personal information; and

- (b) different entities or classes of entities; and
- (c) different permitted purposes.

#### **14 Sections 80L and 80M**

Repeal the sections.

#### **15 Section 80N (heading)**

Omit “cease to have effect”, substitute “cease to be in force”.

#### **16 Section 80N**

Omit “ceases to have effect at the earliest of”, substitute “ceases to be in force at the earliest of the following”.

#### **17 Paragraph 80N(a)**

Omit “cease to have effect”, substitute “cease to be in force”.

#### **18 Paragraph 80N(a)**

Omit “or”.

#### **19 Paragraph 80N(b)**

Omit “revoked; or”, substitute “repealed;”.

#### **20 Paragraph 80N(c)**

Repeal the paragraph, substitute:

- (c) the start of the day after the end of the period of 12 months beginning on the day the declaration commences.

#### **21 Paragraphs 80P(1)(b) to (e)**

Repeal the paragraphs, substitute:

- (b) the collection, use or disclosure is for a permitted purpose specified in the declaration; and
- (c) the information is information of a kind specified in the declaration; and
- (d) the information is disclosed by an entity specified in the declaration, or an entity included in a class of entities specified in the declaration; and

- (e) the information is disclosed to an entity specified in the declaration, or an entity included in a class of entities specified in the declaration; and
- (f) if a matter mentioned in paragraph (b), (c), (d), or (e) is specified in the declaration subject to conditions—those conditions are satisfied.

**22 Subsection 80P(7) (paragraph (a) of the definition of *designated secrecy provision*)**

After “18B,” insert “34GF, 35P,”.

**23 Subsection 80P(7) (paragraph (a) of the definition of *designated secrecy provision*)**

After “92A”, insert “, and subsection 34GE(4),”.

**24 Subsection 80P(7) (after paragraph (a) of the definition of *designated secrecy provision*)**

Insert:

- (aa) section 15LC of the *Crimes Act 1914*;

**25 Subsection 80P(7) (paragraph (c) of the definition of *designated secrecy provision*)**

Omit “and 41 of”, substitute “and 41 of, and clause 9 of Schedule 1 to,”.

**26 Subsection 80P(7) (after paragraph (ca) of the definition of *designated secrecy provision*)**

Insert:

- (cb) sections 22, 22A and 22B of the *Witness Protection Act 1994*;

**27 Subsection 80P(7) (definition of *entity*)**

Repeal the definition.

**28 After paragraph 80Q(2)(a)**

Insert:

- (b) a disclosure for the purposes of carrying out a State’s constitutional functions, powers or duties;



- (ba) a disclosure for the purposes of obtaining or providing legal advice in relation to the operation of this Part;

## **29 Application of amendments**

- (1) The amendments of sections 80J, 80K, 80N and 80P, the repeal of sections 80H, 80L and 80M, and the insertion of section 80KA, of the *Privacy Act 1988* made by this Part apply in relation to declarations made on or after the commencement of this item.
- (2) The amendments of section 80Q of the *Privacy Act 1988* made by this Part apply in relation to the disclosure of information by a person on or after the commencement of this item, whether the information was first disclosed to that person before or after that commencement.

## Part 4—Children's privacy

### *Privacy Act 1988*

#### 30 Subsection 6(1)

Insert:

*child* means an individual who has not reached 18 years.

*Children's Online Privacy Code*: see section 26GC.

#### 31 After subsection 26C(4)

Insert:

(4A) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, an APP code may provide differently for different:

- (a) classes of entities; and
- (b) classes of personal information; and
- (c) classes of activities of entities.

#### 32 Before section 26H

Insert:

### 26GC Development of APP codes by the Commissioner—Children's Online Privacy Code

*Children's Online Privacy Code*

- (1) The Commissioner must develop an APP code (the *Children's Online Privacy Code*) about online privacy for children.
- (2) The other provisions of this Division (including section 26C) apply in relation to the Children's Online Privacy Code subject to this section.

Note: Section 26C deals with requirements for APP codes generally.

*Matters covered by code*

- (3) For the purposes of paragraph 26C(2)(a), the Children's Online Privacy Code must set out how one or more of the Australian Privacy Principles are to be applied or complied with in relation to the privacy of children.
- (4) For the purposes of subsections 26C(3) and (4), the Children's Online Privacy Code may provide for one or more of the matters mentioned in those subsections in relation to the privacy of children. However, despite paragraph 26C(3)(b), the code must not cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3).

Note: Codes may provide differently for different things: see subsection 26C(4A).

*Entities bound by code*

- (5) Subject to subsection (7), an APP entity is bound by the Children's Online Privacy Code if:
  - (a) all of the following apply:
    - (i) the entity is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021*);
    - (ii) the service is likely to be accessed by children;
    - (iii) the entity is not providing a health service; or
  - (b) the entity is an APP entity, or an APP entity in a class of entities, specified in the code for the purposes of this paragraph.

Note: In relation to subparagraph (a)(ii), see subsection (11).

- (6) Paragraph 26C(2)(b) does not apply in relation to the Children's Online Privacy Code.

*Specified entities not bound by code*

- (7) Despite subsection (5), an APP entity is not bound by the Children's Online Privacy Code if the entity is an APP entity, or an APP entity in a class of entities, specified in the code for the purposes of this subsection.

*Requirements*

- (8) In developing the Children's Online Privacy Code, the Commissioner may:
- (a) consult with:
    - (i) children; and
    - (ii) relevant organisations or bodies concerned with children's welfare; and
    - (ia) industry organisations or bodies representing the interests of one or more entities that may potentially be bound by the Code;
    - (iii) the eSafety Commissioner; and
    - (iv) the National Children's Commissioner; and
  - (b) consult any other person the Commissioner considers appropriate.
- (9) Before registering the Children's Online Privacy Code under section 26H, the Commissioner must:
- (a) make a draft of the code publicly available; and
  - (b) invite the public to make submissions to the Commissioner about the draft within a specified period (which must run for at least 60 days); and
  - (c) give consideration to any submissions made within the specified period; and
  - (d) consult with:
    - (i) the eSafety Commissioner; and
    - (ii) the National Children's Commissioner.

*Time by which code must be made*

- (10) The Commissioner must develop and register the Children's Online Privacy Code within the period of 24 months beginning on the day the *Privacy and Other Legislation Amendment Act 2024* receives the Royal Assent.

*Services likely to be accessed by children*

- (11) The Commissioner may make written guidelines to assist entities to determine if a service is likely to be accessed by children for the purposes of subparagraph (5)(a)(ii).

(12) The Commissioner may publish any such guidelines on the Commissioner's website.

(13) Guidelines under subsection (11) are not a legislative instrument.

**33 After paragraph 26H(1)(b)**

Insert:

; or (c) the Commissioner develops a Children's Online Privacy Code under section 26GC;

## **Part 5—Security, retention and destruction**

### ***Privacy Act 1988***

#### **34 At the end of clause 11 of Schedule 1**

Add:

- 11.3 For the purposes of subclauses 11.1 and 11.2, without limiting those subclauses or any other provision of this Act, such steps include technical and organisational measures.

#### **35 Application of amendment**

The amendment of clause 11 of Schedule 1 to the *Privacy Act 1988* made by this Part applies in relation to information held after the commencement of this Part, regardless of whether the information was acquired or created before or after that commencement.

## **Part 6—Overseas data flows**

### ***Privacy Act 1988***

#### **36 After subsection 100(1)**

Insert:

- (1A) Before the Governor-General makes regulations for the purposes of Australian Privacy Principle 8.3 prescribing a country or binding scheme, the Minister must be satisfied that:
- (a) the laws of the country, or the binding scheme, has the effect of protecting personal information about an individual in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
  - (b) there are mechanisms that the individual can access to take action to enforce that protection.
- (1B) The regulations may prescribe a country or binding scheme for the purposes of Australian Privacy Principle 8.3 subject to:
- (a) conditions in relation to a specified entity or class of entities; and
  - (b) conditions in relation to a specified kind or kinds of personal information.

#### **37 After paragraph 8.2(a) of Schedule 1**

Insert:

- (aa) subclause 8.3 applies in relation to the disclosure of the information; or

#### **38 At the end of clause 8 of Schedule 1 (after the note)**

Add:

- 8.3 This subclause applies in relation to the disclosure of personal information (the ***relevant personal information***) about an individual by an APP entity to an overseas recipient if:
- (a) the recipient of the relevant personal information is:

- (i) subject to the laws of a country that is prescribed by the regulations; or
- (ii) a participant in a binding scheme that is prescribed by the regulations; and
- (b) if the country or binding scheme is prescribed subject to conditions—those conditions are satisfied.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed: see subsection 100(1A).

### **39 Application of amendments**

The amendments of clause 8 of Schedule 1 to the *Privacy Act 1988* made by this Part apply in relation to information disclosed after the commencement of this Part, regardless of whether the information was acquired or created before or after that commencement.



## **Part 7—Eligible data breaches**

### ***Privacy Act 1988***

#### **40 Subsection 6(1)**

Insert:

*eligible data breach declaration* means a declaration under subsection 26X(1).

#### **41 Section 26WA (heading)**

Repeal the heading, substitute:

#### **26WA Guide to this Part**

#### **42 At the end of section 26WA**

Add:

- This Part also deals with the collection, use and disclosure of personal information involved in eligible data breaches.

#### **43 At the end of Part IIIC**

Add:

### **Division 5—Dealing with personal information involved in eligible data breaches**

#### **Subdivision A—Eligible data breach declaration**

#### **26X Eligible data breach declaration**

*Minister may make eligible data breach declaration*

- (1) The Minister may, by writing, make a declaration under this subsection if:
- (a) there is an eligible data breach of an entity; and

- (b) the Minister is satisfied that making the declaration is:
  - (i) necessary or appropriate to prevent; or
  - (ii) necessary or appropriate to reduce;a risk of harm arising from a misuse of personal information about one or more individuals following unauthorised access to, or unauthorised disclosure of, that personal information from the eligible data breach of the entity.

Note: A declaration under this subsection is relevant for the operation of section 26XB (authorisation of collection, use and disclosure of personal information) and related provisions.

*Matters covered by declaration*

- (2) Without limiting subsection (1), the declaration must specify the following matters:
  - (a) the kind or kinds of personal information to which the declaration applies;
  - (b) the entity or class of entities that may collect, use or disclose the personal information;
  - (c) the entity or class of entities that the personal information may be disclosed to;
  - (d) one or more permitted purposes of the collection, use or disclosure.

*Specified entities*

- (3) An entity or class of entities specified for the purposes of paragraph (2)(c):
  - (a) may include a State or Territory authority; and
  - (b) must not be or include a media organisation, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.

*Specified permitted purposes*

- (4) A permitted purpose specified for the purposes of paragraph (2)(d) in relation to an eligible data breach must be a purpose that is directly related to preventing or reducing a risk of harm mentioned in paragraph (1)(b) to one or more individuals at risk from the eligible data breach.

- (5) Without limiting subsection (4), any of the following things may be specified as a permitted purpose in relation to an eligible data breach, to the extent that it is directly related to preventing or reducing a risk of harm mentioned in paragraph (1)(b):
- (a) preventing a cyber security incident (within the meaning of the *Security of Critical Infrastructure Act 2018*), fraud, scam activity or identity theft;
  - (b) responding to a cyber security incident, fraud, scam activity or identity theft;
  - (c) responding to the consequences of a cyber security incident, fraud, scam activity, identity crime and misuse, financial loss, emotional and psychological harm, family violence and physical harm or intimidation;
  - (d) addressing malicious cyber activity.
- (6) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, or any other provision of this Act, an eligible data breach declaration may provide differently for:
- (a) different kinds of personal information; and
  - (b) different entities or classes of entities; and
  - (c) different permitted purposes.

#### *Conditions*

- (7) The declaration may specify a matter mentioned in subsection (2) subject to conditions.

#### *Consultation*

- (8) Before the Minister makes a declaration under subsection (1), the Minister may consult with any person or body, including the Commissioner and the Director-General of the Australian Signals Directorate.
- (9) Despite subsection 29(1) of the *Australian Information Commissioner Act 2010* and any provision of this Act, the Commissioner may disclose information to the Minister for the purposes of consultation under subsection (8).

*Declaration is a legislative instrument*

- (10) A declaration under subsection (1) is a legislative instrument, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to the declaration.

**26XA When declarations cease to be in force**

An eligible data breach declaration ceases to be in force at the earliest of the following:

- (a) if a time at which the declaration will cease to be in force is specified in the declaration—at that time;
- (b) the time at which the declaration is repealed;
- (c) the start of the day after the end of the period of 12 months beginning on the day the declaration commences.

**Subdivision B—Provisions dealing with the collection, use and disclosure of personal information**

**26XB Authorisation of collection, use and disclosure of personal information**

- (1) At any time when an eligible data breach declaration is in force in relation to an eligible data breach, an entity may collect, use or disclose personal information about an individual if:
- (a) the entity reasonably believes that the individual may be at risk from the eligible data breach; and
  - (b) the collection, use or disclosure is for a permitted purpose specified in the declaration; and
  - (c) the information is information of a kind or kinds specified in the declaration; and
  - (d) the information is disclosed by an entity specified in the declaration, or an entity included in a class of entities specified in the declaration; and
  - (e) the information is disclosed to an entity specified in the declaration, or an entity included in a class of entities specified in the declaration; and

- (f) if a matter mentioned in paragraph (b), (c), (d) or (e) is specified in the declaration subject to conditions—those conditions are satisfied.
- (2) An entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by subsection (1) unless the secrecy provision is a designated secrecy provision (see subsection (6)).
- (3) An entity is not liable to any proceedings for contravening a duty of confidence in respect of a disclosure of personal information authorised by subsection (1).
- (4) An entity does not breach an Australian Privacy Principle, a registered APP code that binds the entity or a rule issued under section 17 (rules relating to tax file number information) in respect of a collection, use or disclosure of personal information authorised by subsection (1).
- (5) A collection, use or disclose of personal information by an officer or employee of an agency in the course of duty as an officer or employee is authorised by subsection (1) only if the officer or employee is authorised by the agency to collect, use or disclose the personal information.
- (6) In this section:

***designated secrecy provision*** means any of the following:

- (a) sections 18, 18A, 18B, 34GF, 35P, 92 and 92A, and subsection 34GE(4), of the *Australian Security Intelligence Organisation Act 1979*;
- (b) section 15LC of the *Crimes Act 1914*;
- (c) section 34 of the *Inspector-General of Intelligence and Security Act 1986*;
- (d) sections 39, 40C, 40D and 41 of, and clause 9 of Schedule 1 to, the *Intelligence Services Act 2001*;
- (e) sections 42 and 44 of the *Office of National Intelligence Act 2018*;
- (f) sections 22, 22A and 22B of the *Witness Protection Act 1994*;

- (g) a provision of a Commonwealth law prescribed by the regulations for the purposes of this paragraph;
- (h) a provision of a Commonwealth law of a kind prescribed by the regulations for the purposes of this paragraph.

**secrecy provision** means a provision of a Commonwealth law (including a provision of this Act) that prohibits or regulates the use or disclosure of personal information, whether the provision relates to the use or disclosure of personal information generally or in specified circumstances.

## Subdivision C—Other matters

### 26XC Disclosure of information—offence

- (1) A person (the **first person**) commits an offence if:
  - (a) personal information that relates to an individual is disclosed to the first person because of the operation of this Division; and
  - (b) the first person subsequently discloses the personal information.

Penalty: 60 penalty units or imprisonment for 1 year, or both.

- (2) Subsection (1) does not apply to the following disclosures:
  - (a) if the first person is an APP entity—a disclosure permitted under an Australian Privacy Principle, a registered APP code that binds the person or a rule issued under section 17 (rules relating to tax file number information);
  - (b) a disclosure for the purposes of carrying out a State's constitutional functions, powers or duties;
  - (c) a disclosure for the purposes of obtaining or providing legal advice in relation to the operation of this Division;
  - (d) a disclosure permitted under section 26XB;
  - (e) a disclosure made with the consent of the individual to whom the personal information relates;
  - (f) a disclosure to the individual to whom the personal information relates;
  - (g) a disclosure to a court;
  - (h) a disclosure prescribed by the regulations.

Note: A defendant bears an evidential burden in relation to a matter in this subsection (see subsection 13.3(3) of the *Criminal Code*).

- (3) If a disclosure of personal information is covered by subsection (2), the disclosure is authorised by this section.
- (4) For the purposes of paragraph (2)(g), court includes any tribunal, authority or person having power to require the production of documents or the answering of questions.

## **26XD Division not limited by secrecy provisions**

- (1) The operation of this Division is not limited by a secrecy provision of any other Commonwealth law (whether made before or after the commencement of this Act) except to the extent that the secrecy provision expressly excludes the operation of this section.

Note: Section 3 provides for the concurrent operation of State and Territory laws.

- (2) Nothing in this Division is to be taken to require an entity to collect, use or disclose personal information.
- (3) In this section:

***secrecy provision*** means a provision of a Commonwealth law (including a provision of this Act) that prohibits or regulates the use or disclosure of personal information, whether the provision relates to the use or disclosure of personal information generally or in specified circumstances.

## **26XE Constitutional basis of this Division**

This Division relies on the Commonwealth's legislative powers under paragraph 51(xxix) (external affairs) of the Constitution as it relates to giving effect to Australia's obligations under relevant international agreements, in particular Article 17 of the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23).

Note: The Covenant is in Australian Treaty Series 1980 No. 23 ([1980] ATS 23) and could in 2024 be viewed in the Australian Treaties Library on the AustLII website (<http://www.austlii.edu.au>).

**26XF Additional operation of this Division**

- (1) In addition to section 26XE, this Division also has effect as provided by this section.

*Corporations*

- (2) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure by a corporation to which paragraph 51(xx) of the Constitution applies.

*Banking*

- (3) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure that occurs in the course of, or in relation to, the carrying on of the business of banking (within the meaning of paragraph 51(xiii) of the Constitution), other than State banking not extending beyond the limits of the State concerned.

*Insurance*

- (4) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure that occurs in the course of, or in relation to, the carrying on of the business of insurance (within the meaning of paragraph 51(xiv) of the Constitution), other than State insurance not extending beyond the limits of the State concerned.

*Trade and commerce*

- (5) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure that occurs in the course of, or in relation to, trade or commerce:
- (a) between Australia and places outside Australia; or
  - (b) among the States; or
  - (c) within a Territory, between a State and a Territory or between 2 Territories.



*Communications*

- (6) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure using a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution).

*Territories*

- (7) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place in a Territory.

*Aliens*

- (8) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to:
- (a) a collection, use or disclosure by an alien (within the meaning of paragraph 51(xix) of the Constitution); or
  - (b) a collection, use or disclosure of personal information about an alien (within the meaning of paragraph 51(xix) of the Constitution).

*External affairs*

- (9) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place outside Australia.

*Executive power*

- (10) This Division also has the effect it would have if a reference to a collection, use or disclosure were expressly confined to a collection, use or disclosure by a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*) for the purposes of the Commonwealth entity performing its functions or duties or exercising its powers.

## **26XG Interaction with section 12B**

To avoid doubt, section 12B does not apply in relation to this Division.

## **26XH Compensation for acquisition of property**

- (1) If the operation of this Division would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the person.
- (2) If the Commonwealth and the person do not agree on the amount of the compensation, the person may institute proceedings in the Federal Court of Australia or the Supreme Court of a State or Territory for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

## **44 Application provision**

Division 5 of Part IIIC of the *Privacy Act 1988*, as inserted by this Part, applies in relation to:

- (a) eligible data breaches that happen on or after the commencement of this Part; and
- (b) information collected, used or disclosed after the commencement of this Part, regardless of whether the information was acquired or created before or after that commencement.

## **Part 8—Penalties for interference with privacy**

### ***Data Availability and Transparency Act 2022***

#### **45 Paragraph 16F(1)(b)**

Omit “sections 13 and 13G”, substitute “sections 13, 13G and 13H”.

#### **46 Subsection 16F(3)**

Omit “section 13G”, substitute “sections 13G and 13H”.

### ***Digital ID Act 2024***

#### **47 Paragraphs 37(2)(b) and 38(1)(b)**

Omit “sections 13 and 13G”, substitute “sections 13, 13G and 13H”.

### ***Identity Verification Services Act 2023***

#### **48 Paragraph 10A(2)(b)**

Omit “sections 13 and 13G”, substitute “sections 13, 13G and 13H”.

### ***Privacy Act 1988***

#### **49 Section 13G (heading)**

Repeal the heading, substitute:

#### **13G Civil penalty provision for serious interference with privacy of an individual**

#### **50 Subsection 13G(1)**

Repeal the subsection, substitute:

##### *Civil penalty provision*

- (1) An entity contravenes this subsection if:
- (a) the entity does an act, or engages in a practice, that is an interference with the privacy of an individual; and

(b) the interference with privacy is serious.

Note: The court may determine that an entity has contravened section 13H if the court is satisfied of paragraph (a) but not paragraph (b) (see section 13J).

## 51 After subsection 13G(1A)

Insert:

*Factors that may be taken into account in determining if interference with privacy is serious*

- (1B) In determining whether an interference with privacy is serious, a court may have regard to any of the following matters:
- (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;
  - (h) any other relevant matter.

## 52 Before subsection 13G(2)

Insert:

*Maximum pecuniary penalty*

## 53 Subsection 13G(3)

Omit “greater”, substitute “greatest”.

**54 Before subsection 13G(5)**

Insert:

*Meaning of adjusted turnover*

**55 Before subsection 13G(7)**

Insert:

*Meaning of breach turnover period*

**56 At the end of Division 1 of Part III**

Add:

**13H Civil penalty provision for interference with privacy of individuals**

*Civil penalty provision*

- (1) An entity contravenes this subsection if the entity does an act, or engages in a practice, that is an interference with the privacy of an individual.
- (2) Subsection (1) is a civil penalty provision.

Note: Section 80U deals with civil penalty provisions in this Act.

*Maximum pecuniary penalty*

- (3) The amount of the penalty payable by a person in respect of a contravention of subsection (1) must not exceed 2,000 penalty units.

**13J Alternative orders**

If, in proceedings for an order in relation to a contravention of section 13G, the court:

- (a) is satisfied that the entity has done an act, or engaged in a practice, that is an interference with the privacy of an individual; but
- (b) is not satisfied that the interference with privacy is serious;

the court may make a pecuniary penalty order against the entity for contravening section 13H, instead of section 13G.

**13K Civil penalty provision for which infringement notices or compliance notices can be issued**

*Civil penalty provision for breaching Australian Privacy Principles*

- (1) An entity contravenes this subsection if:
- (a) the entity does an act, or engages in a practice; and
  - (b) the act or practice breaches any of the following Australian Privacy Principles:
    - (i) Australian Privacy Principle 1.3 (requirement to have APP privacy policy);
    - (ii) Australian Privacy Principle 1.4 (contents of APP privacy policy);
    - (iii) Australian Privacy Principle 2.1 (individuals may choose not to identify themselves in dealing with entities);
    - (iv) Australian Privacy Principle 6.5 (written notice of certain uses or disclosures);
    - (v) Australian Privacy Principle 7.2(c) or 7.3(c) (simple means for individuals to opt out of direct marketing communications);
    - (vi) Australian Privacy Principle 7.3(d) (requirement to draw attention to ability to opt out of direct marketing communications);
    - (vii) Australian Privacy Principle 7.7(a) (giving effect to request in reasonable period);
    - (viii) Australian Privacy Principle 7.7(b) (notification of source of information);
    - (ix) Australian Privacy Principle 13.5 (dealing with requests);
    - (x) any other Australian Privacy Principle prescribed by the regulations.

Note: Conduct that contravenes this section may also contravene section 13G or 13H.

*Civil penalty provision for non-compliant eligible data breach statement*

- (2) An entity contravenes this subsection if:
- (a) the entity prepares a statement under section 26WK (eligible data breaches); and
  - (b) the statement does not comply with subsection 26WK(3).

*Civil penalty provisions*

- (3) Subsections (1) and (2) are civil penalty provisions.

Note: Section 80U deals with civil penalty provisions in this Act.

*Maximum pecuniary penalty*

- (4) The amount of the penalty payable by a person in respect of a contravention of subsection (1) or (2) must not exceed 200 penalty units.

## **57 Subsection 80UB(1)**

Repeal the subsection, substitute:

*Provisions subject to an infringement notice*

- (1) The following provisions are subject to an infringement notice under Part 5 of the Regulatory Powers Act:
- (a) subsections 13K(1) and (2) (civil penalty provision for which infringement notices or compliance notices can be issued);
  - (b) subsection 66(1) (failure to give information);
  - (c) subsection 80UC(4) (failure to comply with a compliance notice).

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

*Amount to be stated in an infringement notice for listed companies—section 13K*

- (1A) Despite subsection 104(2) of the Regulatory Powers Act, if an infringement notice relates to only one alleged contravention of subsection 13K(1) or (2), or 80UC(4), by a listed corporation (within the meaning of the *Corporations Act 2001*), the amount to

be stated in the notice for the purposes of paragraph 104(1)(f) of the Regulatory Powers Act is 200 penalty units.

- (1B) Despite subsection 104(3) of the Regulatory Powers Act, if an infringement notice relates to more than one alleged contravention of subsection 13K(1) or (2), or 80UC(4), by a listed corporation (within the meaning of the *Corporations Act 2001*), the amount to be stated in the notice for the purposes of paragraph 104(1)(f) of the Regulatory Powers Act is the number of penalty units worked out by multiplying the number of alleged contraventions by 200.

## 57A After Division 1A of Part VIB

Insert:

## Division 1B—Compliance notices

### 80UC Compliance notices

#### *Giving a compliance notice*

- (1) Any of the following persons may give an entity a notice if the person reasonably believes that the entity has contravened subsection 13K(1) or (2) (civil penalty provision for which infringement notices or compliance notices can be issued):
- (a) the Commissioner;
  - (b) a member of the staff of the Commissioner who holds, or is acting in, an office or position that is equivalent to an SES employee.

Note: The notice may be varied or revoked under subsection 33(3) of the *Acts Interpretation Act 1901*.

- (2) The notice must:
- (a) set out the name of the entity to whom the notice is given; and
  - (b) set out details of the contravention; and
  - (c) specify either or both of the following:
    - (i) action the entity must take, or refrain from taking, within a reasonable period specified in the notice, to address the contravention;



- (ii) steps the entity must take, within a reasonable period specified in the notice, to ensure that the conduct constituting the contravention is not repeated or continued; and
- (d) explain that a failure to comply with the notice may contravene a civil penalty provision; and
- (e) explain that the entity may apply to the Federal Court or the Federal Circuit and Family Court of Australia (Division 2) for a review of the notice on either or both of the following grounds:
  - (i) the entity has not committed the contravention set out in the notice;
  - (ii) the notice does not comply with this subsection.
- (3) The notice may also require the entity to produce, within a reasonable period specified in the notice, reasonable evidence of compliance with the notice.

*Entity must comply with compliance notice*

- (4) An entity contravenes this subsection if:
  - (a) the entity is given a notice under subsection (1); and
  - (b) the entity fails to comply with the notice.
- (5) Subsection (4) is a civil penalty provision.

Note: Section 80U deals with civil penalty provisions in this Act.

- (6) The amount of the penalty payable by a person in respect of a contravention of subsection (4) must not exceed 200 penalty units.

*Effect of complying with a compliance notice*

- (7) An entity that complies with a notice given under subsection (1) in relation to a contravention of subsection 13K(1) or (2) is not taken by that compliance:
  - (a) to have admitted to contravening that subsection; or
  - (b) to have been found to have contravened that subsection.

*Relationship with civil penalty provisions*

- (8) The Commissioner must not apply for an order under Part 4 of the Regulatory Powers Act in relation to a contravention of subsection 13G(1), 13H(1) or 13K(1) or (2) of this Act constituted by particular conduct engaged in by an entity, if:
- (a) the entity has been given a notice under subsection (1) of this section in relation to a contravention constituted by the same conduct; and
  - (b) either of the following subparagraphs applies:
    - (i) the notice has not been withdrawn, and the entity has complied with the notice;
    - (ii) the entity has made an application under section 80UD of this Act in relation to the notice and the application has not been completely dealt with.

*Relationship with infringement notices*

- (9) A notice must not be given under subsection (1) to an entity in relation to a contravention if:
- (a) the entity has been given an infringement notice under Part 5 of the Regulatory Powers Act in relation to the contravention; and
  - (b) the infringement notice has not been withdrawn.
- (10) An infringement notice must not be given to an entity under Part 5 of the Regulatory Powers Act in relation to a contravention of subsection 13K(1) or (2) of this Act if the entity has been given a notice under subsection (1) of this section, in relation to the contravention, that has not been withdrawn or cancelled.

*Relationship with enforceable undertakings*

- (11) A notice must not be given under subsection (1) to an entity in relation to a contravention if:
- (a) the Commissioner has accepted an undertaking from the entity under Part 6 of the Regulatory Powers Act in relation to the contravention; and
  - (b) the undertaking has not been withdrawn or cancelled.

### **80UD Review of compliance notices**

- (1) An entity that has been given a notice under subsection 80UC(1) may apply to the Federal Court or the Federal Circuit and Family Court of Australia (Division 2) for a review of the notice on either or both of the following grounds:
  - (a) the entity has not committed the contravention set out in the notice;
  - (b) the notice does not comply with subsection 80UC(2).
- (2) At any time after the application has been made, the court may stay the operation of the notice on the terms and conditions that the court considers appropriate.
- (3) The court may confirm, cancel or vary the notice after reviewing it.

### **58 Application of amendments**

- (1) The amendments of section 13G of the *Privacy Act 1988* made by this Part apply in relation to acts done, or practices engaged in, after the commencement of this item.
- (2) Sections 13H, 13J, 13K, 80UC and 80UD of the *Privacy Act 1988*, as inserted by this Part, and the amendments of section 80UB of the *Privacy Act 1988* made by this Part, apply in relation to acts done, or practices engaged in, after the commencement of this item.

## Part 9—Federal court orders

### *Privacy Act 1988*

#### **59 At the end of Division 1 of Part VIB**

Add:

#### **80UA Powers of court to make other orders**

- (1) The Federal Court, or the Federal Circuit and Family Court of Australia (Division 2), may make an order under this section in proceedings if, in the proceedings, the Court has determined, or will determine, under the Regulatory Powers Act that an entity has contravened a civil penalty provision of this Act (other than Part IIIA).
- (2) Without limiting subsection (1), examples of orders the Court may make under this section include the following:
  - (a) an order directing the entity to perform any reasonable act, or carry out any reasonable course of conduct, to redress the loss or damage suffered, or likely to be suffered, by any individual as a result of the contravention;
  - (b) an order directing the entity to pay damages to any individual by way of compensation for any loss or damage suffered, or likely to be suffered, by any individual as a result of the contravention;
  - (c) an order directing the entity to engage, or not to engage, in any act or practice to avoid repeating or continuing the contravention;
  - (d) an order directing the entity to publish, or otherwise communicate, a statement about the contravention.
- (3) The Court may make an order under subsection (1) whether or not the Court is to make, or has made, a civil penalty order under subsection 82(3) of the Regulatory Powers Act against the entity in relation to the contravention.
- (4) The Court may exercise the power under subsection (1):
  - (a) on its own initiative, during proceedings before the Court; or

- (b) on application, made within the period of 6 years of the contravention, by either of the following persons:
  - (i) an individual who has suffered, or is likely to suffer, loss or damage as a result of the contravention;
  - (ii) the Commissioner.

*Recovery of compensation as a debt*

- (5) If the Court makes an order that the entity pay an amount to an individual, the individual may recover the amount as a debt due to the individual.

## **60 Application of amendments**

Section 80UA of the *Privacy Act 1988*, as inserted by this Part, applies in relation to proceedings instituted after the commencement of this Part, whether the contravention to which the proceedings relate is alleged to have occurred before, on or after that commencement.

## Part 10—Commissioner to conduct public inquiries

### *Privacy Act 1988*

#### **61 Subsection 33(1)**

Omit “or 32”, substitute “, 32 or 33J”.

#### **62 Subsection 33(3)**

Omit “or monitoring”, substitute “, monitoring or inquiry”.

#### **63 After Division 3A of Part IV**

Insert:

### **Division 3B—Public inquiries**

#### **33E Inquiries by Commissioner**

*Minister may give direction or approval for public inquiry*

- (1) The Minister may, in writing, direct the Commissioner to conduct, or approve the Commissioner conducting, a public inquiry into a specified matter or specified matters relating to privacy.
- (2) The direction or approval must specify:
  - (a) the acts or practices in relation to which the inquiry is to be held; and
  - (b) the types of personal information in relation to which the inquiry is to be held.
- (3) The direction or approval may also specify any one or more of the following:
  - (a) the date by which the inquiry is to be completed;
  - (b) any directions in relation to the manner in which the inquiry is to be conducted;
  - (c) one or more APP entities that are to be the subject of the inquiry;
  - (d) one or more classes of APP entities that are to be the subject of the inquiry;

- (e) any matters to be taken into consideration in the inquiry.
- (4) The Minister may vary a direction or approval.

*Conduct of inquiry*

- (5) The Commissioner must conduct a public inquiry in accordance with a direction or approval given under subsection (1).
- (6) Subject to any directions given by the Minister in accordance with paragraph (3)(b), the Commissioner may conduct the inquiry in such manner as the Commissioner thinks fit.

*Status of inquiries, directions and approvals*

- (7) To avoid doubt, an inquiry does not constitute an investigation under section 40 nor a preliminary inquiry under section 42.
- (8) A direction or approval given under subsection (1) is not a legislative instrument.

**33F Commissioner may invite submissions**

The Commissioner may invite submissions on matters that are the subject of a public inquiry.

Note: Under subsection 33E(6), the Commissioner may require submissions to be in writing.

**33G Commissioner not bound by the rules of evidence**

The Commissioner is not bound by the rules of evidence and may inform themselves on any matter in such manner as the Commissioner thinks fit.

**33H Commissioner's powers**

Sections 44 (power to obtain information or documents) and 45 (power to examine witnesses) apply for the purposes of a public inquiry in the same way as those provisions apply to an investigation under Part V.

Note 1: Other provisions may apply on their own terms, such as section 33B (Commissioner may disclose certain information if in the public interest etc.).

### **33J Reporting on public inquiries**

#### *Commissioner to report on public inquiries*

- (1) After completing a public inquiry, the Commissioner must prepare a written report on the inquiry and give the report to the Minister.

#### *Requirement to give report to APP entity*

- (2) If a direction or approval specifies one or more entities under paragraph 33E(3)(c), the Commissioner must give the entities a copy of the report on the day the Commissioner gives the report to the Minister under subsection (1) of this section.

#### *Contents of report*

- (3) The report may include findings and recommendations in relation to any matter included in the report.
- (4) The report must not:
- (a) make any finding or recommendation that a specific act or practice is an interference with the privacy of an individual; or
  - (b) include any matter which the Commissioner thinks it is desirable to exclude under section 33.

Note: For paragraph (a), the report may include previously made findings or recommendations that specific acts or practices interfere with the privacy of individuals.

#### *Making report public*

- (5) The Minister must table a copy of the report before each House of the Parliament within 15 sitting days of that House after the day on which the Minister receives the report.
- (6) Unless the Minister otherwise directs, the Commissioner must make the report publicly available.

Note: The Commissioner may, under section 33B, publish other information relating to the inquiry if it is in the public interest to do so.



## **64 Application of amendments**

Division 3B of Part IV of the *Privacy Act 1988*, as inserted by this Part, applies in relation to public inquiries commenced on or after the commencement of this Part, whether the matter to which the inquiry relates arose, before or after that commencement.

## Part 11—Determinations following investigations

### *Privacy Act 1988*

#### **65 Subparagraph 52(1)(b)(ii)**

After “damage suffered”, insert “, or to prevent or reduce any reasonably foreseeable loss or damage that is likely to be suffered,”.

#### **66 Paragraph 52(1A)(c)**

After “damage suffered”, insert “, or to prevent or reduce any reasonably foreseeable loss or damage that is likely to be suffered,”.

#### **67 Application of amendments**

The amendments of section 52 of the *Privacy Act 1988* made by this Part apply in relation to determinations made after the commencement of this Part.

## **Part 12—Annual reports**

### ***Australian Information Commissioner Act 2010***

#### **68 Paragraph 32(1)(a)**

After “performance”, insert “during the year”.

#### **69 Paragraph 32(1)(b)**

After “made”, insert “during the year”.

#### **70 At the end of subsection 32(1)**

Add:

- ; (c) a statement including details about the number of complaints made under section 36 of the *Privacy Act 1988* during the year;
- (d) a statement including details about the number of complaints made under section 36 of the *Privacy Act 1988* in relation to which the Commissioner has decided during the year under section 41 of that Act not to investigate, or not to investigate further, and the relevant grounds for the decision.

#### **71 Application of amendments**

The amendments of section 32 of the *Australian Information Commissioner Act 2010* made by this Part apply in relation to an annual report for a period beginning after the commencement of this Part.

## Part 13—External dispute resolution

### *Privacy Act 1988*

#### **72 Paragraph 41(1)(dc)**

After “is being dealt with”, insert “, or has been dealt with,”.

#### **73 Application of amendments**

The amendment of section 41 of the *Privacy Act 1988* made by this Part applies in relation to any complaint made:

- (a) before the commencement of this Part if the complaint has not been finalised by the Commissioner by that commencement; and
- (b) after the commencement of this Part.

## **Part 14—Monitoring and investigation**

### ***Competition and Consumer Act 2010***

#### **74 Subsection 56ET(3) (at the end of the note)**

Add “The Information Commissioner also has the power, under Division 1AC of Part VIB of the *Privacy Act 1988*, to investigate contraventions of civil penalty provisions in Division 5 of Part IVD of this Act.”.

#### **75 Subsection 56ET(4) (item 5 of the table)**

Repeal the item.

#### **76 Subsection 56ET(4) (note 1)**

Omit “Note 1”, substitute “Note”.

#### **77 Subsection 56ET(4) (note 2)**

Repeal the note.

### ***Crimes Act 1914***

#### **78 Subsection 85ZZG(1)**

Omit “68”, substitute “67”.

#### **79 At the end of subsection 85ZZG(1)**

Add:

Note: In addition, under subsection 80TB(1) of the *Privacy Act 1988*, the Commissioner has the power to monitor, under the Regulatory Powers Act, compliance with Divisions 2 and 3 of this Part.

### ***Data-matching Program (Assistance and Tax) Act 1990***

#### **80 Subsection 13(7)**

Add:

Note: In addition, under paragraphs 80TB(1)(b) and (3)(b) of the *Privacy Act 1988*, the Commissioner has the power to monitor, under the

Regulatory Powers Act, compliance with this Act or rules issued under section 12. See also paragraph 33C(1)(d) of that Act.

### ***National Health Act 1953***

#### **81 Subsection 135AB(3)**

After “Part V”, insert “, and Division 1AC of Part VIB,”.

### ***Privacy Act 1988***

#### **82 Subsection 6(1)**

Insert:

*member of the staff of the Commissioner* means a person referred to in section 23 of the *Australian Information Commissioner Act 2010*.

#### **83 Sections 68 and 68A**

Repeal the sections.

#### **84 Part VIB (heading)**

Repeal the heading, substitute:

### **Part VIB—Compliance and enforcement**

#### **85 Before Division 1 of Part VIB**

Insert:

#### **Division 1AA—Introduction**

##### **80TA Simplified outline of this Part**

Certain provisions, information and matters are subject to monitoring under Part 2 of the Regulatory Powers Act.

Certain provisions are subject to investigation under Part 3 of the Regulatory Powers Act.

Civil penalty orders may be sought under Part 4 of the Regulatory Powers Act from a relevant court in relation to contraventions of civil penalty provisions. If a relevant court has determined, or will determine, under the Regulatory Powers Act that an entity has contravened certain civil penalty provisions of this Act, the court may make other orders in the proceeding.

Infringement notices may be given under Part 5 of the Regulatory Powers Act for alleged contraventions of certain provisions.

Undertakings to comply with the provisions of this Act may be accepted and enforced under Part 6 of the Regulatory Powers Act.

Injunctions under Part 7 of the Regulatory Powers Act may be used to restrain a person from contravening a provision of this Act or to compel compliance with a provision of this Act.

## **Division 1AB—Monitoring powers**

### **80TB Monitoring powers**

#### *Provisions subject to monitoring*

- (1) The following provisions are subject to monitoring under Part 2 of the Regulatory Powers Act:
  - (a) Divisions 2 and 3 of Part VIIC of the *Crimes Act 1914* (pardons, and quashed and spent convictions);
  - (b) Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990*, or rules issued under section 12 of that Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the provisions mentioned in this subsection have been complied with. It includes powers of entry and inspection.

#### *Information subject to monitoring*

- (2) Information given in compliance, or purported compliance, with any of the following provisions is subject to monitoring under Part 2 of the Regulatory Powers Act:
  - (a) subsection 26WU(3) (power to obtain information and documents relating to eligible data breaches);

- (b) subsection 33C(3) (requirement to provide information relating to an assessment);
- (c) subsection 44(1) (requirement to provide information relating to investigations).

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of entry and inspection.

*Matters subject to monitoring*

- (3) The following matters are subject to monitoring under the Regulatory Powers Act:
  - (a) a matter referred to in subsection 28A(1) of this Act in relation to which the Commissioner has a monitoring related function (credit reporting and tax file number monitoring-related functions);
  - (b) a matter referred to in subsection 33C(1) of this Act if the Commissioner is undertaking an assessment of the matter (assessments related to Australian Privacy Principles).

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring the matters mentioned in this subsection. It includes powers of entry and inspection.

*Authorised applicant*

- (4) For the purposes of Part 2 of the Regulatory Powers Act, each of the following persons is an authorised applicant in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3):
  - (a) the Commissioner;
  - (b) a member of the staff of the Commissioner who is an SES employee, or an acting SES employee, or who holds, or is acting in, a position that is equivalent to, or higher than, a position occupied by an SES employee.

*Authorised person*

- (5) For the purposes of Part 2 of the Regulatory Powers Act, each of the following persons is an authorised person in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3):



- (a) the Commissioner;
- (b) a member of the staff of the Commissioner who is authorised in writing by the Commissioner or a delegate of the Commissioner;
- (c) a consultant who is:
  - (i) engaged under section 24 of the *Australian Information Commissioner Act 2010* in relation to performance of the functions or the exercise of the powers of the Commissioner; and
  - (ii) authorised in writing by the Commissioner or a delegate of the Commissioner.

*Issuing officer*

- (6) For the purposes of Part 2 of the Regulatory Powers Act, any judicial officer within the meaning of the Regulatory Powers Act is an issuing officer in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3).

*Relevant chief executive*

- (7) For the purposes of Part 2 of the Regulatory Powers Act, the Commissioner is the relevant chief executive in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3).
- (8) The relevant chief executive may, in writing, delegate the relevant chief executive's powers and functions under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3), to a person who is:
  - (a) a member of the staff of the Commissioner; and
  - (b) an SES employee, or an acting SES employee, or who holds, or is acting in, a position that is equivalent to, or higher than, a position occupied by an SES employee.
- (9) A person exercising powers or performing functions under a delegation under subsection (8) must comply with any directions of the relevant chief executive.

*Relevant court*

- (10) For the purposes of Part 2 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3):
- (a) the Federal Court of Australia;
  - (b) the Federal Circuit and Family Court of Australia (Division 2).

*Person assisting*

- (11) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3).

*Extension to external Territories*

- (12) Part 2 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3), extends to every external Territory.

*Relationship with other provisions*

- (13) Part 2 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (1), the information mentioned in subsection (2), and the matters mentioned in subsection (3), is subject to section 70 of this Act.

Note: Section 70 deals with certain documents and information not required to be disclosed.

**80TC Modifications of Part 2 of the Regulatory Powers Act**

*Use of force in executing a monitoring warrant*

In executing a monitoring warrant under Part 2 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection 80TB(1), the information mentioned in

subsection 80TB(2), and the matters mentioned in subsection 80TB(3), of this Act:

- (a) an authorised person may use such force against things as is necessary and reasonable in the circumstances; and
- (b) a person assisting the authorised person may use such force against things as is necessary and reasonable in the circumstances.

## **Division 1AC—Investigation powers**

### **80TD Investigation powers**

#### *Provisions subject to investigation*

- (1) A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is:
  - (a) an offence provision, or a civil penalty provision, in this Act; or
  - (b) any of the following:
    - (i) a civil penalty provision that is enforceable by the Commissioner under the *Digital ID Act 2024*;
    - (ii) a civil penalty provision that is enforceable by the Commissioner under the *Healthcare Identifiers Act 2010* or an instrument made under that Act;
    - (iii) a civil penalty provision that is enforceable by the Commissioner under the *My Health Records Act 2012*;
    - (iv) a civil penalty provision that is enforceable by the Commissioner under Division 5 of Part IVD of the *Competition and Consumer Act 2010*; or
  - (c) an offence provision of the *Crimes Act 1914* or the *Criminal Code*, to the extent that it relates to an offence provision in this Act.

Note 1: Part 3 of the Regulatory Powers Act creates a framework for investigating whether a provision has been contravened. It includes powers of entry, search and seizure.

Note 2: Part 3 of the Regulatory Powers Act is modified by section 80TE.

Note 3: Subparagraph (1)(b)(iv) is subject to subsection 80TE(2).

*Authorised applicant*

- (2) For the purposes of Part 3 of the Regulatory Powers Act, each of the following persons is an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1):
- (a) the Commissioner;
  - (b) a member of the staff of the Commissioner who is an SES employee, or an acting SES employee, or who holds, or is acting in, a position that is equivalent to, or higher than, a position occupied by an SES employee.

*Authorised person*

- (3) For the purposes of Part 3 of the Regulatory Powers Act, each of the following persons is an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1):
- (a) the Commissioner;
  - (b) a member of the staff of the Commissioner who is authorised in writing by the Commissioner or a delegate of the Commissioner;
  - (c) a consultant who is:
    - (i) engaged under section 24 of the *Australian Information Commissioner Act 2010* in relation to performance of the functions or the exercise of the powers of the Commissioner; and
    - (ii) authorised in writing by the Commissioner or a delegate of the Commissioner.

*Issuing officer*

- (4) For the purposes of Part 3 of the Regulatory Powers Act, any judicial officer within the meaning of the Regulatory Powers Act is an issuing officer in relation to evidential material that relates to a provision mentioned in subsection (1).

*Relevant chief executive*

- (5) For the purposes of Part 3 of the Regulatory Powers Act, the Commissioner is the relevant chief executive in relation to

evidential material that relates to a provision mentioned in subsection (1).

- (6) The relevant chief executive may, in writing, delegate the relevant chief executive's powers and functions under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1) to a person who is:
  - (a) a member of the staff of the Commissioner; and
  - (b) an SES employee, or an acting SES employee, or who holds, or is acting in, a position that is equivalent to, or higher than, a position occupied by an SES employee.
- (7) A person exercising powers or performing functions under a delegation under subsection (6) must comply with any directions of the relevant chief executive.

*Relevant court*

- (8) For the purposes of Part 3 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1):
  - (a) the Federal Court of Australia;
  - (b) the Federal Circuit and Family Court of Australia (Division 2).

*Person assisting*

- (9) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1).

*Extension to external Territories*

- (10) Part 3 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (1), extends to every external Territory.

*Relationship with other provisions*

- (11) Part 3 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (1), is subject to section 70 of this Act.

Note: Section 70 deals with certain documents and information not required to be disclosed.

**80TE Modifications of Part 3 of the Regulatory Powers Act**

*Use of force in executing an investigation warrant*

- (1) In executing an investigation warrant under Part 3 of the Regulatory Powers Act, as that Part applies in relation to evidential material that relates to a provision mentioned in subsection 80TD(1) of this Act:
- (a) an authorised person may use such force against things as is necessary and reasonable in the circumstances; and
  - (b) a person assisting the authorised person may use such force against things as is necessary and reasonable in the circumstances.

*Limitation on use of investigation powers in relation to matters under the Competition and Consumer Act*

- (2) If a civil penalty provision that is enforceable by the Commissioner under Division 5 of Part IVD of the *Competition and Consumer Act 2010* is subject to investigation under Part 3 of the Regulatory Powers Act, the powers under that Part may be exercised in relation to premises only if the premises are occupied by or on behalf of:
- (a) a CDR participant for CDR data; or
  - (b) an accredited person who may become an accredited data recipient of CDR data; or
  - (c) a designated gateway for CDR data; or
  - (d) an action service provider for a type of CDR action who has been, or may be, disclosed CDR data under the consumer data rules;
- (all within the meaning of the *Competition and Consumer Act 2010*).

## **86 Application of amendments**

- (1) Divisions 1AB and 1AC of Part VIB of the *Privacy Act 1988*, as inserted by this Part, apply in relation to monitoring and investigating matters after the commencement of this Part, whether in relation to acts or practices before or after the commencement of this Part.
- (2) The amendment of subsection 135AB(3) of the *National Health Act 1953* made by this Part applies in relation to monitoring and investigating matters after the commencement of this Part, whether in relation to acts or practices before or after the commencement of this Part.

## Part 15—Automated decisions and privacy policies

### *Privacy Act 1988*

#### **87 After subparagraph 13K(1)(b)(ii)**

Insert:

- (ia) Australian Privacy Principle 1.7 (contents of APP privacy policy—automated decisions);

#### **88 At the end of clause 1 of Schedule 1**

Add:

##### *Automated decisions*

- 1.7 Without limiting subclause 1.3, the APP privacy policy of an APP entity must contain the information covered by subclause 1.8 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; and
  - (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.
- 1.8 The information covered by this subclause is:
- (a) the kinds of personal information used in the operation of such computer programs; and
  - (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.
- 1.9 For the purposes of subclauses 1.7 and 1.8:
- (a) making a decision includes refusing or failing to make a decision; and



- (b) doing a thing includes refusing or failing to do a thing; and
- (c) a decision may affect the rights or interests of an individual, whether the rights or interests of the individual are adversely or beneficially affected; and
- (d) the following are examples of the kinds of decisions that may affect the rights or interests of an individual:
  - (i) a decision made under a provision of an Act or a legislative instrument to grant, or to refuse to grant, a benefit to the individual;
  - (ii) a decision that affects the individual's rights under a contract, agreement or arrangement;
  - (iii) a decision that affects the individual's access to a significant service or support.

## **89 Application of amendment**

The amendment of clause 1 of Schedule 1 to the *Privacy Act 1988* made by this Part applies in relation to decisions made after the commencement of this item, whether:

- (a) the arrangement for a computer program to make the decision, or do a thing that is substantially and directly related to making the decision, was made before or after that commencement; and
- (b) the use of personal information in the operation of the computer program occurred before or after that commencement; and
- (c) the personal information used in the operation of the computer program was acquired or created before or after that commencement.

## Schedule 2—Serious invasions of privacy

### *Privacy Act 1988*

#### **1 Section 2A**

Before “The objects”, insert “(1)”.

#### **2 At the end of section 2A**

Add:

(2) This section does not apply to Schedule 2.

Note: See also clause 1 of Schedule 2 (objects).

#### **3 Section 3**

Before “It is”, insert “(1)”.

#### **4 At the end of section 3**

Add:

(2) This section does not apply to Schedule 2.

Note: See also clause 21 of Schedule 2 (saving of other laws).

#### **5 Section 5A**

Before “This Act”, insert “(1)”.

#### **6 At the end of section 5A**

Add:

(2) This section does not apply to Schedule 2.

#### **7 At the end of section 5B**

Add:

*Application*

(5) This section does not apply to Schedule 2.

## **8 At the end of section 12B**

Add:

- (9) This section does not apply to Schedule 2.

Note: See also clauses 4 and 5 of Schedule 2 (constitutional basis and additional operation).

## **9 Before section 95 of Part IX**

Insert:

### **94A Schedule 2**

- (1) Schedule 2 has effect.
- (2) In determining the meaning of an expression used in a provision of this Act (other than Schedule 2), an expression used in Schedule 2 is to be disregarded.
- (3) In determining the meaning of a provision of this Act (other than Schedule 2), Schedule 2 is to be disregarded.

## **10 At the end of the Act**

Add:

# **Schedule 2—Statutory Tort for Serious Invasions of Privacy**

Note: See section 94A.

## **Part 1—Preliminary**

### **1 Objects of this Schedule**

The objects of this Schedule are to:

- (a) establish a cause of action for serious invasions of privacy; and
- (b) provide for defences, remedies and exemptions in respect of the cause of action; and

- (c) recognise that there is a public interest in protecting privacy;  
and
- (d) recognise that the public interest in protecting privacy is  
balanced with other public interests; and
- (e) implement Australia's international obligations in relation to  
privacy.

## **2 Simplified outline of this Schedule**

This Schedule establishes a cause of action in tort for serious invasions of privacy.

An individual has a cause of action against another person if, among other things, the other person invaded the individual's privacy by intruding upon their seclusion or misusing information relating to them.

It is a defence to the cause of action if the other person acted with lawful authority or in certain circumstances involving consent, necessity or the defence of persons or property. If the invasion of privacy involved the publication of information, the other person may also have access to certain defences that would ordinarily arise in the context of defamation proceedings.

Exemptions apply in relation to intelligence agencies and law enforcement bodies, persons disclosing information to such agencies or bodies, persons using information disclosed by such agencies or bodies, and persons under 18 years of age. Journalists and certain other persons are also exempt in certain circumstances.

The court may, during the proceedings, grant an injunction restraining the other person from invading the individual's privacy. The court may also summarily dismiss the proceedings in certain circumstances.

The court may grant remedies including damages.

There are time limits on when proceedings under this Schedule may be commenced.

---

<p>This Schedule is intended to be read and construed separately from the rest of this Act.</p>
---

### **3 Crown to be bound**

This Schedule binds the Crown in each of its capacities.

### **4 Constitutional basis of this Schedule**

This Schedule relies on the Commonwealth's legislative powers under paragraph 51(xxix) of the Constitution to give effect to Australia's obligations under the International Covenant on Civil and Political Rights.

### **5 Additional operation of this Schedule**

- (1) In addition to clause 4, this Schedule also has effect as provided by this clause.

#### *Communications*

- (2) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy using a service to which paragraph 51(v) of the Constitution applies.

#### *Corporations*

- (3) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy by or on behalf of a corporation to which paragraph 51(xx) of the Constitution applies.

#### *Territories*

- (4) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy in a Territory.

*Trade and commerce*

- (5) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy in the course of trade or commerce:
- (a) between Australia and places outside Australia; or
  - (b) among the States; or
  - (c) between a State and a Territory; or
  - (d) between 2 Territories.

*Banking and insurance*

- (6) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy in the course of the carrying on of:
- (a) the business of banking, other than State banking (within the meaning of paragraph 51(xiii) of the Constitution) not extending beyond the limits of the State concerned; or
  - (b) the business of insurance, other than State insurance (within the meaning of paragraph 51(xiv) of the Constitution) not extending beyond the limits of the State concerned.

*Incidental*

- (7) This Schedule also has the effect it would have if a reference in this Schedule to an invasion of privacy were expressly confined to an invasion of privacy incidental to the execution of any of the legislative powers of the Parliament or the executive power of the Commonwealth.

## 6 Interpretation

- (1) In this Schedule:

***agency*** has the meaning given by subsection 6(1) of this Act.

***ASIO affiliate*** has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

***Australian Geospatial-Intelligence Organisation*** means that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation.

**Australian law** has the meaning given by subsection 6(1) of this Act.

**court/tribunal order** has the meaning given by subsection 6(1) of this Act.

**Defence Department** means the Department administered by the Minister administering Part III of the *Defence Act 1903*.

**Defence Intelligence Organisation** means that part of the Defence Department known as the Defence Intelligence Organisation.

**intelligence agency** means:

- (a) the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*; or
- (b) the Australian Geospatial-Intelligence Organisation; or
- (c) the Australian Secret Intelligence Service; or
- (d) the Australian Security Intelligence Organisation; or
- (e) the Australian Signals Directorate; or
- (f) the Defence Intelligence Organisation; or
- (g) the Office of National Intelligence.

**International Covenant on Civil and Political Rights** means the International Covenant on Civil and Political Rights done at New York on 16 December 1966, as in force for Australia from time to time.

Note: The Covenant is in Australian Treaty Series 1980 No. 23 ([1980] ATS 23) and could in 2024 be viewed in the Australian Treaties Library on the AustLII website (<http://www.austlii.edu.au>).

**intruding upon the seclusion** of an individual includes, but is not limited to, the following:

- (a) physically intruding into the person's private space;
- (b) watching, listening to or recording the person's private activities or private affairs.

**journalist** has the meaning given by subclause 15(2).

**journalistic material** has the meaning given by subclause 15(3).

**law enforcement body** means:

- (a) the Australian Federal Police; or
- (b) the National Anti-Corruption Commissioner; or
- (c) the Australian Crime Commission; or
- (d) a police force or service of a State or a Territory; or
- (e) the New South Wales Crime Commission; or
- (f) the Independent Commission Against Corruption of New South Wales; or
- (g) the Law Enforcement Conduct Commission of New South Wales; or
- (h) the Independent Broad-based Anti-corruption Commission of Victoria; or
- (i) the Crime and Corruption Commission of Queensland; or
- (j) the Corruption and Crime Commission of Western Australia; or
- (k) the Independent Commissioner Against Corruption of South Australia.

***misusing information*** that relates to an individual includes, but is not limited to, collecting, using or disclosing information about the individual.

***reckless*** has the same meaning as in the *Criminal Code*.

***staff member*** of an agency or State or Territory authority (including an intelligence agency or a law enforcement body) includes:

- (a) the head (however described) of the agency or authority, or another person who holds an office or appointment in relation to the agency or authority; and
- (b) a person who is otherwise a member of the staff of the agency or authority (whether an employee of the agency or authority, a consultant or contractor to the agency or authority, or a person who is made available to perform services for the agency or authority by another agency or authority, or another person); and
- (c) in the case of the Australian Federal Police—a member or special member of the Australian Federal Police; and
- (d) in the case of a police force of a State or Territory—a member (however described) of that police force.



---

***State or Territory authority*** has the meaning given by section 6C of this Act.

- (2) In determining the meaning of an expression used in a provision of this Schedule, an expression used in the rest of this Act is to be disregarded (unless a provision of this Schedule expressly provides otherwise).
- (3) In determining the meaning of a provision of this Schedule, the rest of this Act is to be disregarded.

## **Part 2—Serious invasions of privacy**

### **7 Cause of action**

- (1) An individual (the ***plaintiff***) has a cause of action in tort against another person (the ***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; and
  - (c) the invasion of privacy was intentional or reckless; and
  - (d) the invasion of privacy was serious; and
  - (e) the public interest in the plaintiff's privacy outweighed any countervailing public interest.
- (2) The invasion of privacy is actionable without proof of damage.

#### ***Countervailing public interest***

- (3) Without limiting what constitutes a countervailing public interest, any of the following matters of public interest may constitute a countervailing public interest:
  - (a) freedom of expression, including political communication and artistic expression;
  - (b) freedom of the media;

- (c) the proper administration of government;
- (d) open justice;
- (e) public health and safety;
- (f) national security;
- (g) the prevention and detection of crime and fraud.

*Reasonable expectation of privacy*

- (5) Without limiting the matters that the 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, the court may consider the following:
  - (a) the means, including the use of any device or technology, used to invade the plaintiff's privacy;
  - (b) the purpose of the invasion of privacy;
  - (c) attributes of the plaintiff including the plaintiff's age, occupation or cultural background;
  - (d) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy;
  - (e) if the defendant invaded the plaintiff's privacy by intruding upon the plaintiff's seclusion—the place where the intrusion occurred;
  - (f) if the defendant invaded the plaintiff's privacy by misusing information that relates to the plaintiff—the following:
    - (i) the nature of the information, including whether the information related to intimate or family matters, health or medical matters or financial matters;
    - (ii) how the information was held or communicated by the plaintiff;
    - (iii) whether and to what extent the information was already in the public domain.

*Seriousness*

- (6) Without limiting the matters that the court may consider in determining whether the invasion of privacy was serious, the court may consider the following:

- (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.

*Untrue information*

- (7) If the defendant invaded the plaintiff's privacy by misusing information that relates to the plaintiff, it is immaterial whether the information was true.

## **8 Defences**

- (1) It is a defence to the cause of action if:
  - (a) the invasion of privacy was required or authorised by or under an Australian law or court/tribunal order; or
  - (b) the plaintiff, or a person having lawful authority to do so for the plaintiff, expressly or impliedly consented to the invasion of privacy; or
  - (c) the defendant reasonably believed that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person; or
  - (d) the invasion of privacy was:
    - (i) incidental to the exercise of a lawful right of defence of persons or property; and
    - (ii) proportionate, necessary and reasonable.
- (2) It is also a defence to the cause of action if:
  - (a) the defendant invaded the plaintiff's privacy by publishing, within the meaning of an Australian law that deals with defamation, information that relates to the plaintiff; and
  - (b) the Australian law provides for a related defence; and
  - (c) the defendant would be able to establish the related defence if a reference in the Australian law to the publication of defamatory matter were to include a reference to the invasion of privacy.

- (3) Each of the following is a *related defence* for the purposes of this clause:
- (a) a defence of absolute privilege;
  - (b) a defence for publication of public documents;
  - (c) a defence of fair report of proceedings of public concern.

#### **8A Determination whether exemption applies**

- (1) The court may, at any stage of the proceedings, determine whether an exemption in Part 3 applies in relation to the invasion of privacy.
- (2) The court may make the determination on application of a party to the proceedings or on its own motion.
- (3) If a party to the proceedings applies for a determination under this clause before the trial for the proceedings commences, the court is to make the determination as soon as practicable, and before the trial commences, unless satisfied that there are special circumstances justifying the postponement of the determination to a later stage of the proceedings (including during the trial).
- (4) This clause does not limit any powers that the court has apart from this clause.

#### **9 Injunctions**

- (1) The court may, at any stage of the proceedings, grant an injunction restraining the defendant from invading the plaintiff's privacy.
- (2) If the invasion of privacy involves publishing information that relates to the plaintiff, the court must have particular regard to the public interest in the publication of the information when considering whether to grant the injunction.

#### **10 Summary judgment**

- (1) The court may give judgment for the defendant if the court is satisfied that the plaintiff has no reasonable prospect of successfully prosecuting the proceedings.

- 
- (2) This clause does not limit any powers that the court has apart from this clause.

## **11 Damages**

- (1) Subject to this clause, the court may award damages to the plaintiff.
- (2) The court must not award aggravated damages.
- (3) The court may award damages for emotional distress.
- (4) The court may award exemplary or punitive damages in exceptional circumstances.
- (5) The sum of:
- (a) any damages awarded for non-economic loss; and
  - (b) any exemplary or punitive damages;
- must not exceed the greater of:
- (c) \$478,550; and
  - (d) the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law.
- (6) Without limiting the matters that the court may consider in determining the amount of damages, the court may consider the following:
- (a) whether the defendant apologised to the plaintiff;
  - (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.

## 12 Other remedies

- (1) The court may grant such remedies, in addition to or instead of damages awarded in accordance with clause 11, as the court thinks most appropriate in the circumstances.
- (2) Without limiting subclause (1), those remedies may include one or more of the following:
  - (a) an account of profits;
  - (b) an injunction;
  - (c) an order requiring the defendant to apologise to the plaintiff;
  - (d) a correction order;
  - (e) an order that any material (including copies):
    - (i) that is in the defendant's possession, or that the defendant is able to retrieve; and
    - (ii) that was obtained or made as a result of the invasion of privacy or was misused during the course of the invasion of privacy;be destroyed, be delivered up to the plaintiff or be dealt with as the court directs;
  - (f) a declaration that the defendant has seriously invaded the plaintiff's privacy.

## 13 The effect of an apology on liability

For the purposes of this Schedule, an apology made by or on behalf of the defendant in connection with the invasion of privacy:

- (a) does not constitute an express or implied admission of fault or liability by the defendant in connection with the invasion of privacy; and
- (b) is not relevant to the determination of fault or liability in connection with the invasion of privacy.

Note: The court may consider whether the defendant apologised to the plaintiff in determining the amount of damages (if any) to award to the plaintiff (see paragraph 11(6)(a)).

## 14 When proceedings must be commenced

- (1) The plaintiff must commence proceedings under this Schedule:
-

- (a) if the plaintiff was under 18 years of age when the invasion of privacy occurred—before the plaintiff’s 21st birthday; or
- (b) otherwise—before the earlier of:
  - (i) the day that is 1 year after the day on which the plaintiff became aware of the invasion of privacy; and
  - (ii) the day that is 3 years after the invasion of privacy occurred.

Note: See also clause 19 (single publication rule).

- (2) However, the plaintiff may apply to the court for an order that, despite subclause (1), the plaintiff may commence proceedings under this Schedule before a day specified in the order.
- (3) The court may make the order if the court is satisfied that it was not reasonable in the circumstances for the plaintiff to have commenced proceedings in accordance with subclause (1) in relation to the invasion of privacy.
- (4) The day specified in the order must not be later than 6 years after the day on which the invasion of privacy occurred.

## Part 3—Exemptions

### 15 Journalists etc.

- (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 collection, preparation for publication or publication of journalistic material:
  - (a) a journalist;
  - (b) an employer of, or a person engaging, a journalist;
  - (c) a person assisting a journalist who is employed or engaged by:
    - (i) the journalist’s employer; or
    - (ii) a person engaging the journalist;
  - (d) a person assisting a journalist in the person’s professional capacity.

- (1A) This Schedule does not apply to an invasion of privacy to the extent that the invasion of privacy involves the publication or distribution of journalistic material that was prepared for publication by a journalist.
- (2) A **journalist** is a person who:
- (a) works in a professional capacity as a journalist; and
  - (b) is subject to:
    - (i) standards of professional conduct that apply to journalists; or
    - (ii) a code of practice that applies to journalists.
- (3) Material is **journalistic material** if it:
- (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; or
  - (c) consists of editorial content relating to news, current affairs or a documentary.
- (4) For the purposes of this clause, if a journalist invades an individual's privacy, it is immaterial whether the invasion of privacy breaches the standards or the code of practice to which the journalist is subject.

## **16 Agencies and State and Territory authorities (other than intelligence agencies and law enforcement bodies)**

This Schedule does not apply to an invasion of an individual's privacy by an agency or a State or Territory authority (other than an intelligence agency or a law enforcement body) to the extent that the agency or authority invades the individual's privacy, in good faith:

- (a) in the performance or purported performance of a function of the agency or authority; or
- (b) in the exercise or purported exercise of a power of the agency or authority.



---

**16A Staff members of agencies or State and Territory authorities  
(other than intelligence agencies and law enforcement  
bodies)**

This Schedule does not apply to an invasion of an individual's privacy by a staff member of an agency or a State or Territory authority (other than a staff member of an intelligence agency or a law enforcement body) to the extent that the staff member invades the individual's privacy, in good faith:

- (a) in the performance or purported performance of a function of the agency or authority; or
- (b) in the exercise or purported exercise of a power of the agency or authority.

**16B Law enforcement bodies**

This Schedule does not apply to:

- (a) an invasion of privacy by a law enforcement body; or
- (b) an invasion of privacy by a person who is a staff member of a law enforcement body in the performance of the person's duties, powers or functions as such a staff member; or
- (c) an invasion of privacy to the extent that it involves a disclosure of information to a law enforcement body; or
- (d) an invasion of privacy to the extent that it involves information that was disclosed by a law enforcement body.

**17 Intelligence agencies**

This Schedule does not apply to:

- (a) an invasion of privacy by an intelligence agency; or
- (aa) an invasion of privacy by a person who is an ASIO affiliate, or an agent or staff member of an intelligence agency, in the performance of:
  - (i) if the person is an ASIO affiliate—functions or services for the Australian Security Intelligence Organisation; or
  - (ii) otherwise—the person's duties, powers or functions as such an agent or staff member; or
- (b) an invasion of privacy to the extent that it involves a disclosure of information to an intelligence agency; or

- (c) an invasion of privacy to the extent that it involves information that was disclosed by an intelligence agency.

## 18 Persons under 18

This Schedule does not apply to an invasion of privacy by a person who is under 18 years of age.

## Part 4—Miscellaneous

### 19 Single publication rule

- (1) This clause applies if:
  - (a) a publisher publishes information that relates to an individual to the public (the *first publication*); and
  - (b) the publisher or an associate of the publisher subsequently publishes (whether or not to the public) information that is substantially the same (the *subsequent publication*); and
  - (c) the manner of the subsequent publication is not materially different from the manner of the first publication.
- (2) If an invasion of the individual's privacy consists of the first publication or the subsequent publication, the invasion of privacy is taken to occur on the day of the first publication for the purposes of this Schedule.
- (3) In determining whether the manner of the subsequent publication is materially different from the manner of the first publication, the court may have regard to:
  - (a) the level of prominence that the information is given; and
  - (b) the extent of the subsequent publication.
- (4) In this clause:  
*associate*, of a publisher, means:
  - (a) an employee of the publisher; or
  - (b) a person who publishes information as a contractor of the publisher; or
  - (c) an associated entity of the publisher; or

- (d) an employee of an associated entity of the publisher; or
- (e) a person who publishes information as a contractor of an associated entity of the publisher.

*associated entity* has the same meaning as in the *Corporations Act 2001*.

## **20 Deceased persons**

- (1) A person (including a personal representative of a deceased person) cannot assert, continue or enforce an action under this Schedule in relation to:
  - (a) an invasion of the privacy of a deceased person (whether occurring before or after the deceased person's death); or
  - (b) an invasion of privacy by a person who has died.
- (2) Nothing in this clause prevents the court, if it considers it in the interests of justice to do so, from determining the question of costs for proceedings discontinued because of this clause.

## **21 Saving of other laws and remedies**

This Schedule is not intended to exclude or limit the concurrent operation of any law, whether written or unwritten, of a State or a Territory.

## **22 Intervention of Information Commissioner**

The Information Commissioner may, with the leave of the court:

- (a) intervene in proceedings under this Schedule; or
- (b) assist the court as *amicus curiae*.

## **23 Jurisdiction**

*Federal and State courts*

- (1) Jurisdiction is conferred on the Federal Circuit and Family Court of Australia (Division 2) in relation to matters arising under this Schedule.

Note: State courts and the Federal Court of Australia also have jurisdiction in relation to matters arising under this Schedule (see subsection 39(2) and paragraph 39B(1A)(c) of the *Judiciary Act 1903*).

*Territory courts*

- (2) Jurisdiction is conferred on the courts of the Territories in relation to matters arising under this Schedule.
- (3) Jurisdiction is conferred under subclause (2):
  - (a) only so far as the Constitution permits; and
  - (b) within the limits (other than limits of locality) of the jurisdiction of the court (whether those limits are limits as to subject matter or otherwise).

---

## Schedule 3—Doxxing offences

### *Criminal Code Act 1995*

#### **1 After section 474.17B of the *Criminal Code***

Insert:

#### **474.17C Using a carriage service to make available etc. personal data of one or more individuals**

- (1) A person commits an offence if:
- (a) the person uses a carriage service to make available, publish or otherwise distribute information; and
  - (b) the information is personal data of one or more individuals; and
  - (c) 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.

**Note:** Publishing the name, image and telephone number of an individual on a website and encouraging others to repeatedly contact the individual with violent or threatening messages is an example of conduct (commonly referred to as doxxing) that is covered by this subsection.

**Penalty:** Imprisonment for 6 years.

- (2) For the purposes of paragraph (1)(b), *personal data* of an individual means information about the individual that enables the individual to be identified, contacted or located, and includes the following:
- (a) the name of the individual;
  - (b) a photograph or other image of the individual;
  - (c) a telephone number of the individual;
  - (d) an email address of the individual;
  - (e) an online account of the individual;
  - (f) a residential address of the individual;
  - (g) a work or business address of the individual;
  - (h) a place of education of the individual;
  - (i) a place of worship of the individual.

**474.17D Using a carriage service to make available etc. personal data of one or more members of certain groups**

- (1) A person commits an offence if:
- (a) the person uses a carriage service to make available, publish or otherwise distribute information; and
  - (b) the information is personal data of one or more members of a group; and
  - (c) the person engages in the conduct in whole or in part because of the person's belief that the group is distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin; and
  - (d) 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 members.

Note: Publishing the names, images and residential addresses of members of a private online religious discussion group across multiple websites and encouraging others to attend those addresses and block entryways, or otherwise harass the members of that group, is an example of conduct (commonly referred to as doxxing) that is covered by this subsection.

Penalty: Imprisonment for 7 years.

- (2) For the purposes of paragraph (1)(b), **personal data** of one or more members of a group means information about the members that enables the members to be identified, contacted or located, and includes the following:
- (a) the names of the members;
  - (b) photographs or other images of the members;
  - (c) telephone numbers of the members;
  - (d) email addresses of the members;
  - (e) online accounts of the members;
  - (f) residential addresses of the members;
  - (g) work or business addresses of the members;
  - (h) places of education of the members;
  - (i) places of worship of the members.
- (3) For the purposes of paragraph (1)(c), it is immaterial whether the group is actually distinguished by race, religion, sex, sexual

---

orientation, gender identity, intersex status, disability, nationality  
or national or ethnic origin.

---

*[Minister's second reading speech made in—  
House of Representatives on 12 September 2024  
Senate on 18 November 2024]*

(115/24)