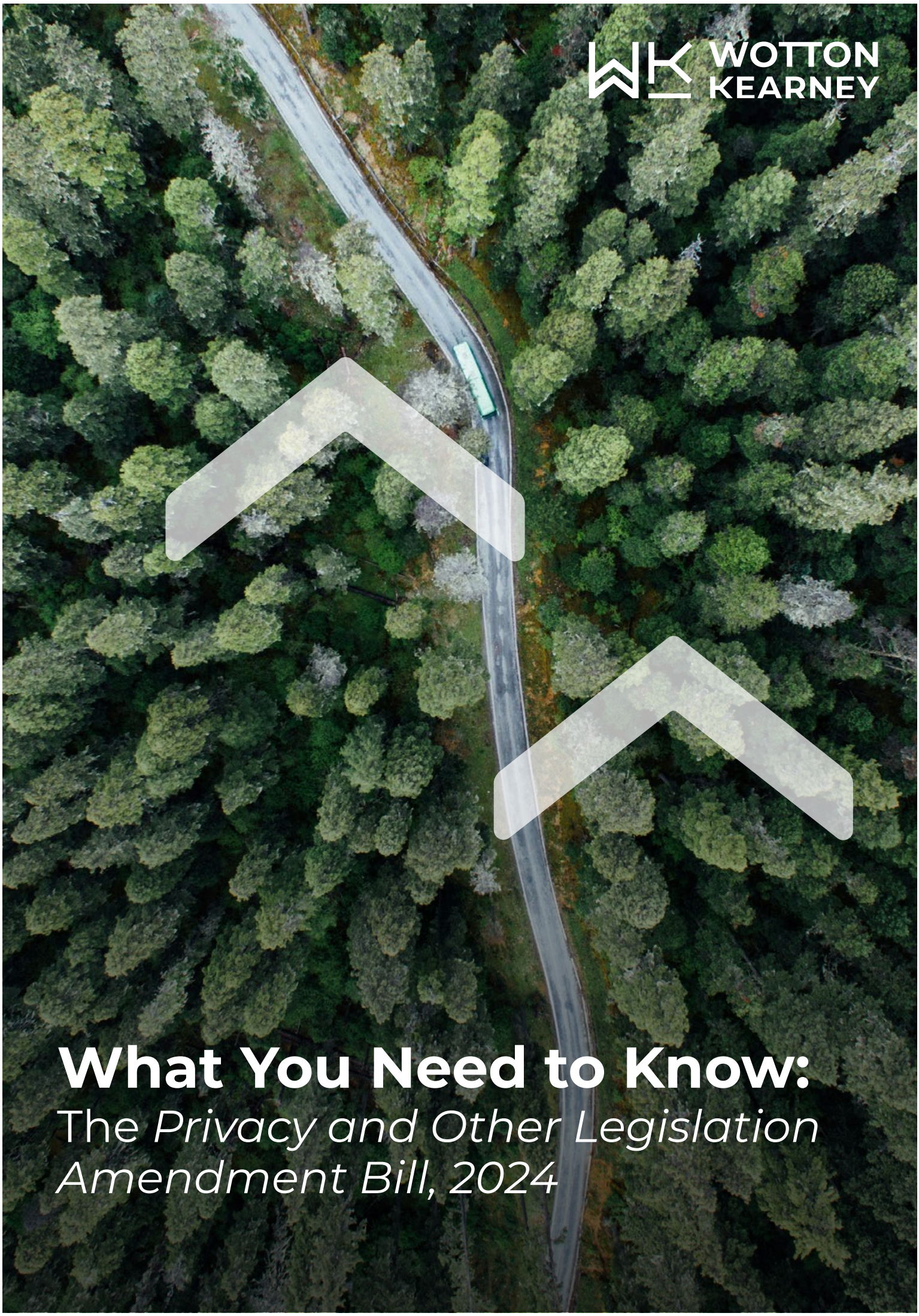

WOTTON KEARNEY

# What You Need to Know:

## The *Privacy and Other Legislation Amendment Bill, 2024*

# Contents


| | |
|---|---|
| **Introduction** | **1** |
| **APP Codes** | **2** |
| **Emergency declarations** | **3** |
| **Children's privacy** | **3** |
| **Security, retention and destruction** | **4** |
| **Overseas data flows** | **5** |
| **Eligible data breaches** | **6** |
| **Penalties for interference with privacy** | **7** |
| **Federal court orders** | **8** |
| **Public inquiries** | **9** |
| **Determinations following investigations** | **10** |
| **Annual reports** | **10** |
| **External dispute resolution** | **10** |
| **Monitoring and investigation** | **10** |
| **Automated decisions and privacy policies** | **12** |
| **Serious invasions of privacy** | **13** |
| **Doxxing offences** | **14** |


# Introduction

A first tranche of reforms to the *Privacy Act 1988* (Cth) was passed on 28 November 2024 as the *Privacy and Other Legislation Amendment Bill, 2024* (Cth) (**Privacy Amendment Bill**). The Privacy Amendment Bill seeks to implement 23 reforms that were "agreed-to" in the Government's response to the Privacy Act Review Report. The Review Report included 116 reforms of which only 89 are legislative changes, and the Government only "agreed-to" 25 proposals which are legislative changes (with the remaining 13 proposals agreed to being non-legislative changes).

Once Royal Assent is received, most of the provisions of the Privacy Amendment Bill will commence and we will see a strengthening in privacy obligations on APP entities and broader powers granted to the Office of the Information Commissioner (**OAIC**) which will help bring Australia's privacy laws into the new digital age and align with international best standards.

Many of the more substantial reforms expected have not been included, such as:

- An expansion of the definition of personal information
- Further protections to de-identified information
- Updates to the definition of sensitive information
- Removal of the small business exemption
- Enhanced protections to employees' information
- Updates to the requirements around privacy policies, collection notices, and consents
- Requirement for the fair and reasonable handling of personal information
- Requirement to conducting Privacy Impact Assessment for activities with high privacy risks
- Clarification and broadening of the rights of individuals
- Updating the rights of individuals in the context of direct marketing, targeting and trading
- Introduction of the distinction between controllers and processors.

We expect the second tranche of privacy reforms (likely to be published in 2025) will address the more fundamental reforms stated above. These reforms are likely to align to international privacy laws, most notably the General Data Protection Regulation (GDPR). For Australian organisations (who have not had to apply a strict level of privacy compliance in their businesses) this will require a deep dive into their data lake to understand what data they hold, for what purposes and how it has been used. While privacy compliance can seem daunting and tedious, there are many benefits for organisations to undergo this exercise.

# APP Codes

A number of amendments have been introduced including a new clause 26GA and 26GB which increases the APP code-making process and enables the Information Commissioner to develop an APP code on the written direction of the Minister (i.e. the Attorney-General) if the Minister is satisfied that it is in the public interest. A mandatory consultation process must be followed for each new APP code ensuring that that APP codes are fit for purpose and capable of being implemented. Where an APP code is urgently required, the Minister is also empowered to request the Information Commissioner to develop a temporary APP code which does not include a mandatory consultation process and cannot be in force for longer than 12 months.

APP codes allow identified privacy issues within a sector or industry to be dealt with effectively and enables the clarification of any uncertainty. APP codes are not legislative instruments and are merely a declaration which has an administrative quality.

If an APP code is developed for your sector or industry and your APP entity is bound by such APP code or you have chosen to "opt-in" then a failure to comply with such APP code may amount to an interference with the privacy of an individual.

# Emergency declarations

The Privacy Amendment Bill introduces the ability of the Minister to make emergency declarations to authorise the more targeted handling of personal information to assist individuals in an emergency or disaster situation. The amendments include provisions detailing circumstances under which an emergency declaration can be made, including that a permitted purpose must directly relate to the Commonwealth's response to an emergency or disaster.

# Children's privacy

In an effort to strengthen and protect the privacy of children online, the Information Commissioner must develop and register a Children's Online Privacy Code within 24 months of the Privacy Amendment Bill receiving Royal Assent. The Children's Online Privacy Code will set out how the Australian Privacy Principles (**APPs**) should be applied to the privacy of children. This may mean that stricter requirements may be imposed on APP entities regarding targeting, direct marketing and trading of children. We may also see stricter requirements in the collection, use or disclosure of children's information which will likely be linked to the best interests of a child test.

APP entities who will be required to comply with this code if they:

1. provide a social media service, relevant electronic service (RES) or designated internet service (DIS) (as these terms are defined in the Online Safety Act)
2. the service is likely to be accessed by children (individuals under the age of 18)
3. the service is not a health service.

APP entities who are specified in the code as it being applying to them will also be required to comply with the code. The Children's Online Privacy Code will be available for public comment and will include consultations with children, organisations concerned with children's welfare, the eSafety Commissioner and the National Children's Commissioner. The Information Commissioner may also publish guidelines to assist entities to determine if a service is likely to be accessed by children.

If you provide a service which is likely used by children, you will need to be mindful of the Children's Online Privacy Code, as well as other legislation that will impact digital businesses, such as the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* (Cth) which aims to combat the most seriously harmful content on digital platforms and contains strengthened protections for freedom of speech.

# Security, retention and destruction

APP11 (Security of Personal Information) is updated to include APP11.3 to clarify that an APP entity must ensure that in taking reasonable steps to secure information it must also take **technical and organisational measures** to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure.

### Examples of technical measures

includes taking physical measures, such as ensuring that any physical records containing personal information or hardware are kept in a locked, secure space or access to such spaces/ premises is limited, and in respect of software it means encrypting data, anti-virus software and strong passwords.

### Examples of organisational measures

includes training employees on protecting information, developing standard operating procedures and policies for securing personal information.

In the OAIC's Notifiable Data Breaches Report for January to June 2024 the OAIC has included some additional guidance to APP entities. Some of the guidance mentioned lends itself to understanding the technical and organisation measures the OAIC may expect APP entities to implement, namely:

1. Improving third-party vendor procurement processes
2. Prioritising training employees on secure information handling practices and keeping employees updated on the latest cyber threats
3. Minimising access to personal information to only those employees who have a need to such information
4. Employing multi-factor authentication, IP access control and encryption in cloud environments.
5. Having proper policies, processes and procedures which govern the configuration and management of cloud data storage.



# Overseas data flows

The Governor-General may make regulations regarding the acceptability of disclosing personal information to recipients who are based in other countries or bound by a binding scheme. In accordance with a new section 100(1A) in the Privacy Amendment Bill the Governor-General in making regulations must consider the laws of a country or binding scheme to ensure that it has the effect of protecting personal information of an individual in the same or substantially similar manner as the APPs and must also consider if there are mechanisms that individuals can access to take action to enforce the protection of their personal information.

APP8 (Cross-border Disclosure of Personal Information) is also amended by the Privacy Amendment Bill to introduce that the disclosure of personal information to an overseas recipient will be considered permissible where such recipient is subject to the laws of a country or binding scheme which is prescribed by the regulations, and if any conditions are prescribed in the regulations, then such conditions are satisfied.

A "whitelist" of countries whose laws provide adequate levels of protection to individuals' personal information will be helpful in enabling the transfer and disclosure of personal information overseas. Any conditions noted in the regulations will need to be complied with, which could include incorporating contractual clauses (such as the GDPR standard contractual clauses) or conducting risk assessments.

# Eligible data breaches

The Privacy Amendment Bill has been amended to include a new Division 5 under section 26WA which provides for the ability of the Minister to make eligible data breach declarations enabling the handling of personal information in a manner which would not otherwise be permissible under the APPs or secrecy provisions, i.e. essentially enabling the sharing of personal information to government agencies and authorities.

A declaration may only be made if there is an eligible data breach of an entity and the Minister is satisfied that the declaration is necessary or appropriate to prevent or reduce a risk of harm arising from a misuse of personal information about one or more individuals following the unauthorised access or disclosure of personal information.

A declaration must specify:

1. the kinds of personal information to which it applies
2. the entities that may collect, use or disclose personal information
3. the entities that the personal information may be disclosed to – this may include a State or Territory authority, and must not be a media organisation
4. the permitted purposes of the collection, use or disclosure – this purpose must be related to preventing or reducing risk of harm to affected individuals of an eligible data breach.

A declaration may only operate for a maximum of 12 months. This amendment is stated as being reasonable, proportionate and necessary to achieve the legitimate objective of preventing and reducing risk of harm to individuals in the aftermath of a data breach.

The amendments contained in this section also addresses the authorisation of collecting, using and disclosing personal information, offences under this section, secondary disclosures of personal information and other administrative issues.

Specified permitted purposes of a declaration includes:

- Preventing a cyber security incident (as defined in the *Security of Critical Infrastructure Act 2018* (Cth), fraud, scam activity or identity theft
- Responding to a cyber security incident, fraud, scam activity or identity theft
- 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
- Addressing malicious cyber activity.

# Penalties for interference with privacy

New penalties and offences have been included in the Privacy Amendment Bill. These seek to give the OAIC broader and stronger enforcement powers.

## Serious privacy interferences contravention redefined

The existing section 13G is deleted and replaced with a new section that provides that if an entity does an act or engages in a practice that is an interference with the privacy of an individual and is serious, then such entity will have contravened subsection 13G. An interference with privacy is not limited to a single act or practice, and it may be relevant to consider multiple acts. 13G(1A) then lists 8 factors which may be taken into account in determining if an interference is serious, which includes:

- the particular kinds of information involved
- the sensitivity of the personal information of the individual
- the consequences/potential consequences of the interference with privacy for the individual
- the number of individuals affected
- whether the individual affected is a child or person experiencing vulnerability
- whether the act was done, or the practice engaged in, repeatedly or continuously
- 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
- any other relevant matter.

The above list is not meant to be exhaustive when considering whether an interference with privacy is serious.

## Maximum pecuniary penalty

A new section 13H has been introduced providing for a maximum pecuniary penalty for interferences with the privacy of individuals of 2,000 penalty units, i.e. $660,000 at present. For bodies corporate the maximum penalty is five times the amount specified for a person.

In the Explanatory Memorandum to the Privacy Amendment Bill, it has been explained that this maximum penalty amount is to "*deter privacy breaches and meet increasing community expectations for meaningful privacy protection*". It goes on further to note that the penalty amount is meant to reflect the gains made by an organisation from engaging in practices which interfere with privacy.

A court is also able to make an alternative order for a pecuniary penalty order where there has been an interference of privacy of individuals, but a court is not satisfied that such interference is serious.

## Civil penalty for breaching APPs

New civil penalty provisions have been introduced through a new section 13K(1) where there is a breach of specific APPs. A person may be subject to a penalty not exceeding 200 penalty units, i.e. $66,000 (for bodies corporate this will be 1,000 penalty units, i.e. $330,000) at present, where they breach:

- the requirement to have a privacy policy (APP 1.3)
- the privacy policy is deficient (APP1.4)
- individuals are not provided with the option to not identify themselves (APP2.1)
- written notice of certain uses or disclosures are not made (APP6.5)
- a simple means for opting out of direct marketing communications is not provided (APP7.2(c) or 7.3(c));
- the requirement to draft attention to the ability to opt out of direct marketing communications is not met (APP 7.3(d))
- a request to opt out or not use or disclose personal information is not dealt with within a reasonable period (APP7.7(a))

- a request to provide the source of the original collector of personal information is not dealt with (APP7.7)(b))
- a request to correct personal information is not dealt with (APP13.5)
- any other APPs prescribed by regulations.

### Civil penalty for providing non-compliant eligible data breach statements

A further civil penalty provision has been included as section 13K(1) which provides that a person may be subject to a penalty not exceeding 200 penalty units, i.e. $66,000 (for bodies corporate this will be 1,000 penalty units, i.e. $330,000) at present, where an entity prepares a statement notifying of an eligible data breach but that statement does not comply with subsection 26WK(3).

### Infringement notices

In addition to an entity failing to provide information under section 66(1), an infringement notice may also be issued where civil penalty provisions under section 13K(1) and 13K(2) applies (i.e. the new sections above). For one allegation of contravention a penalty of 200 penalty units, i.e. $66,000 (at present) will apply and for multiple alleged contraventions the penalty will be the number of alleged contraventions multiplied by 200 penalty units.

Infringement notices will present a cost-effective and speedy way for the OAIC to address less severe contraventions or to enforce compliance with the Privacy Act.

## Federal court orders

The Federal Court and the Federal Circuit and Family Court of Australia (Division 2) is empowered to make additional orders where an entity has been found to have contravened a civil penalty provision under the Privacy Act (other than Part IIIA – Credit reporting).

The orders which may be made by these Courts include:

- directing an entity to perform or carry out any reasonable act or course of conduct to redress any loss or damage suffered/likely to be suffered
- directing the entity to pay damages to any individual by way of compensation for any loss or damage suffered/likely to be suffered
- directing the entity to engage/not engage in any act or practice to avoid repeating or continuing the contravention
- directing the entity to publish or otherwise communicate a statement about the contravention.

These orders are examples only, and these Courts have the discretion to make any orders it considers appropriate.

The Court may exercise these powers on its own initiative during proceedings, or on application to the Court may be made within 6 years of the contravention arising by individuals who suffered/likely to suffer loss or damage or the Information Commissioner.

## Public inquiries

The Minister has the power to direct the Information Commissioner to conduct or approve the Information Commissioner to conduct a public inquiry into specified matters relating to privacy.

The direction or approval from the Minister **must** include:

1. the acts or practices in relation to which the inquiry is to be held
2. the types of personal information in relation to which the inquiry is to be held

the direction or approval from the Minister **may** include:

3. the date by which the inquiry is to be completed
4. any directions in relation to the manner in which the inquiry is to be conducted
5. the APP entities that are to be the subject of the inquiry
6. the classes of APP entities that are to be the subject of the inquiry
7. any matters to be taken into consideration in the inquiry.

This is a new power granted under the Privacy Amendment Bill. An inquiry is not an investigation under section 40 or a preliminary inquiry under section 42 of the Privacy Act.

The Information Commissioner in conducting a public inquiry **may** invite submissions, is not bound by the rules of evidence, may exercise its powers to obtain information or documents (under section 44 of the Privacy Act), and may exercise its powers to examine witnesses (under section 45 of the Privacy Act).

The Information Commissioner must prepare a written report after completing a public inquiry which must include findings and recommendations. This report must be provided to the Minister and any affected APP entities. Furthermore, unless the Minister directs otherwise, the report must also be made public.

We expect the OAIC to use these powers to investigate large scale data breaches or privacy infringements, which have a wide-reaching impact on the public.

# Determinations following investigations

Section 52 of the Privacy Act gives the Information Commissioner the power to make a determination after investigating a complaint or an Information Commissioner-initiated investigation, which may include a declaration requiring certain steps or actions to be taken. The Privacy Amendment Bill amends section 52(1)(b)(ii) and 52(1A)(c) to include that such declaration may now also require that any reasonable act or course of conduct is performed to prevent or reduce the occurrence of any reasonably foreseeable loss or damage.

# External dispute resolution

The Privacy Amendment Bill amends section 41(a)(dc) so that the Information Commissioner now is able to decide to not investigate a complaint made to it which has been dealt with by a recognised external dispute resolution scheme.

# Annual reports

The Information Commissioner is now required to include in its annual reports (see amendments to section 32(1)):

1. a statement including details of the number of complaints made under section 36 of the Privacy Act during a year
2. a statement regarding the number of complaints which the Information Commissioner has decided not to investigate, not to investigate *further*, and the relevant grounds for the decision.

# Monitoring and investigation

The Privacy Act currently include a broad range monitoring, assessment and investigation powers granted to the Information Commissioner. The Privacy Amendment Bill amends the Privacy Act to extend these powers to include entry, search and seizure powers of the Information Commissioner by inserting a new Division 1AB and 1AC under Part VIB (Compliance and enforcement) and repeals the existing entry and inspection powers under section 68 and 68A of the Privacy Act. These powers will now align with other domestic regulators and include the standard safeguards that complement these powers as codified in the Regulatory Powers Act.

# Automated decisions and privacy policies

APP1 (Open and Transparent Management of Personal Information) of the Privacy Act is amended to include new APP1.7, 1.8 and 1.9 regarding automated decisions.

Where an APP entity:

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

the APP entity is required to include information in its privacy policy about:

- the kinds of **personal information** used in the operation of such computer programs
- the kinds of **decisions** made solely by the operation of such computer programs
- the kinds of such decisions for which a thing that is *substantially* **and** *directly* related to making the decision is done by the operation of such computer programs.

Examples of decisions that may affect the rights or interests of an individual includes:

- a decision under an Act or legislative instrument to grant or refuse to grant a benefit to an individual
- a decision that affects the individual's rights under a contract, agreement or arrangement
- a decision that affects the individual's access to a significant service or support.

APP entities which fail to disclose in their privacy policy information about using personal information in automated decisions will be in breach of APP1.7 and subject to the new civil penalty provisions.

The intention is to capture a broad range of matters, including rule-based processes, AI and machine learning processes, which enable a decision to be made which affects the rights or interests of an individual. It is only intended to capture the use of computer programs to facilitate the decision-making.

# Serious invasions of privacy

Schedule 2 of the Privacy Amendment Bill introduces a cause of action, defences, remedies and exemptions for serious invasions for privacy. This Schedule is intended to be a stand-alone set of provisions which are independent from the Privacy Act – i.e. they are intended to be interpreted separately from the provisions in the Privacy Act.

The elements to be proven to establish a tort for serious invasions of privacy set out in clause 7 are:

1. an invasion of privacy (by intrusion upon seclusion or misuse of information, or both)
2. a reasonable expectation of privacy in all the circumstances
3. fault (either intention or recklessness)
4. seriousness of the invasion
5. that the public interest in protecting the plaintiff's privacy outweighs countervailing public interests that are raised by the defendant.

Proof of damage is not necessary in order to action the invasion of privacy tort, however any harm or damage caused would be relevant in considering the seriousness of the invasion.

A defence to the cause of action can be raised by the defendant, if the defendant can prove that:

1. the invasion of privacy was required or authorised by or under an Australian law or court/tribunal order
2. there was the express or implied consent to the invasion of privacy
3. the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person
4. the invasion of privacy was incidental to the exercise of a lawful right of defence of persons or property and proportionate, necessary and reasonable
5. invasion of privacy was through publishing (within the meaning of an Australian law that deals with defamation), the Australian law provides for a related defence, and the defendant would be able to establish the related defence (i.e. absolute privilege, publication of public documents or fair report of proceedings of public concern).

Courts are granted the power to grant interim injunctions, summary judgment and damages (which is capped at a maximum of $478,550 – this reflects the current cap for damages under defamation law). In addition to, or instead of damages, a court may also grant the following remedies: an account of profits, an injunction, an apology order, a correction order, a destruction or delivery of materials order, or a declaration that defendant has seriously invaded the plaintiff's privacy.

Interestingly, no admission of fault or liability will be attached to an apology made by a defendant which may be made in the early resolution of a dispute, but that a court may take such an apology into account in determining the quantum of damages awarded.

Exemptions are granted to journalists, enforcement bodies, intelligence agencies and persons under 18 years of age.

This tort provides a recourse for persons who are affected by an invasion of privacy which might fall outside the scope of the Privacy Act.

# Doxxing offences

Schedule 3 of the Privacy Amendment Bill amends the *Criminal Code Act 1995* (Cth) to introduce a new offence for doxxing.

A person will be guilty of committing an offence if (section 474.17C):

1. the person uses a carriage service to make available, publish or otherwise distribute information
2. the information is personal data of one or more individuals
3. 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.

An offence will also be committed if (section 474.17D):

1. the person uses a carriage service to make available, publish or otherwise distribute information
2. the information is personal data of one or more individuals
3. 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
4. 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.

This Schedule refers to "personal data" which is defined to include information that helps identify, contact or locate individuals, and includes but is not limited to:

- names
- photographs or other images
- telephone numbers
- email addresses
- online accounts
- residential addresses
- work or business addresses
- places of education
- places of worship.

Doxxing is the intentional and malicious exposure of personal data that is menacing or harassing. An offence under section 474.17C attracts a maximum penalty of 6 years imprisonment, whilst an offence under section 474.17D attracts a maximum penalty of 7 years imprisonment.

Doxxing exposes victims to additional harms, such as exposing victims to physical threats, stalking, harassment, identity theft and fraud, humiliation and shaming, and discrimination, as well as psychological harms.

## Australian offices

**Adelaide**
Lvl 1, 25 Grenfell St
Adelaide, SA 5000
+61 8 8473 8000

**Brisbane**
Lvl 23, 111 Eagle St
Brisbane, QLD 4000
+61 7 3236 8700

**Canberra**
Ste 4.01, 17 Moore St
Canberra, ACT 2601
+61 2 5114 2300

**Melbourne**
Lvl 30, 500 Bourke St
Melbourne, VIC 3000
+61 3 9604 7900

**Perth**
Lvl 49, 108 St Georges Tce
Perth, WA 6000
+61 8 9222 6900

**Sydney**
Lvl 9, Grosvenor Plc
225 George St
Sydney, NSW 2000
+61 2 8273 9900

## New Zealand offices

**Auckland**
Lvl 8, 21 Queen St
Auckland 1010
+64 9 377 1854

**Christchurch**
202/235 High St
Christchurch 8011
+64 3 667 4003

**Wellington**
Lvl 12, 342 Lambton Qy
Wellington 6011
+64 4 499 5589

## Asia office

**Singapore**
138 Market St
05-01, CapitaGreen
Singapore, 048956
+65 6967 6460