

ROBOTS AND DOXXING AND FINES, OH MY!

NAVIGATING THE PRIVACY REFORM ROAD,
AND THE STEPS TO TAKE RIGHT NOW

PRESENTED BY
NIKKI MACOR HEATH | SPECIAL COUNSEL

24 MARCH 2025



ACKNOWLEDGEMENT OF COUNTRY

HWLE would like to acknowledge that this presentation is being delivered on the traditional lands of the Kurna people. We pay our respects to Kurna Elders past and present, and recognise the ongoing connection the Kurna people have to waters, kin and Community

OVERVIEW

Current privacy landscape

Privacy reforms and what to do about them

What's next?



CURRENT PRIVACY LANDSCAPE



PRIVACY LAW

CURRENT PRIVACY LANDSCAPE

- The *Privacy Act 1988* (Cth) regulates how Commonwealth agencies and private organisations collect, hold, use and disclose **personal information** about individuals
- Key obligations of the *Privacy Act* are set out in the **Australian Privacy Principles (APPs)**
- **Confidentiality** ≠ privacy
 - A legal duty to protect information which is conveyed between parties in confidence
 - Governed by the common law, and confidentiality clauses in agreements or contracts between parties

PRIVACY

PERSONAL INFORMATION

- Personal information is defined in the *Privacy Act* as:

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a) whether the information or opinion is true or not; and*
- b) whether the information or opinion is recorded in a material form or not.*

PRIVACY

PERSONAL INFORMATION

- The definition is broad in scope, and may include:
 - contact information
 - sensitive information
 - racial or ethnic origin
 - political or religious beliefs
 - criminal record
 - health or genetic information
 - credit information
 - tax file information

PRIVACY

WHAT DOES THE ACT APPLY TO?

- **Employee record exemption:** Employer's handling of employee records regarding current and former employment relationships is exempt from the APPs in certain circumstances
 - Only applies to records already held by an entity, not to collection
- **Small business exemption:** Most small businesses with annual turnover under \$3 million are not subject to the *Privacy Act*
 - Health service providers, entities trading in personal information, credit reporting bodies and some others are caught regardless of turnover
- Information that is **aggregated** or **de-identified** is no longer personal information and outside the scope of the *Privacy Act*

PRIVACY

AUSTRALIAN PRIVACY PRINCIPLES (APPS)

1 Open and Transparent Management of Personal Information

2 Anonymity and Pseudonymity

3 Collection of Solicited Personal Information

4 Dealing with Unsolicited Personal Information

5 Notification of the Collection of Personal Information

6 Use or Disclosure of Personal Information

7 Direct Marketing

Cross-Border Disclosure of Personal Information

Adoption, Use or Disclosure of Government Related Identifiers

Quality of Personal Information

Security of Personal Information

Access to Personal Information

Correction of Personal Information

8

9

10

11

12

13

PRIVACY

AUSTRALIAN PRIVACY PRINCIPLES (APPS)

A failure to comply with
the **APPs** or an **APP Code** is

an **interference with the privacy of an individual**

and may be investigated by the
Office of the Australian Information Commissioner
(OAIC)

The image features a dark green background with several white geometric shapes. In the top left, there is a square with a black speckled pattern. To its right is a white circular ring, also speckled. In the bottom left, a white triangular shape is visible, and in the bottom right, a white circular shape is shown. All these shapes have a black speckled pattern, similar to a starry sky or a textured surface.

PRIVACY ACT REFORMS

HOW DID WE GET HERE?



PRIVACY ACT

PRIVACY AND OTHER LEGISLATION AMENDMENT ACT 2024

- Major changes to the Privacy Act include:
 - A statutory tort for serious invasion of privacy
 - A children's online privacy code
 - New automated decision making disclosure requirements
 - Updated data security requirements
 - Express mechanism for declaration of an overseas disclosure white list
 - New data breach declaration powers
 - New civil penalty options
 - New criminal offence for doxxing

AUTOMATED DECISION MAKING DISCLOSURE

What changed?

If an APP entity uses a computer program to make a decision using **personal information** which could be **reasonably expected** to **significantly affect** the rights or interests of an individual, it will need to include details of such practices in its privacy policy

What do you need to do?

- **Reflect** on if you use any computer programs to make decisions
- **Determine** what information is used by these programs
- **Update** your privacy policy to outline the decisions made with computer programs and the types of personal information used by the computer programs

Commencement: 11 December 2026

AUTOMATED DECISION MAKING DISCLOSURE

- Examples of kinds of decisions that may affect an individual's rights or interests:
 - Deciding whether to grant a benefit to an individual under legislation
 - Decisions that affect an individual's rights under a contract
 - eg life insurance policy
 - Decisions that affect an individual's access to a service
 - eg differential pricing for healthcare services

AUTOMATED DECISION MAKING DISCLOSURE

- If using automated decision making, privacy policy must include:
 - What kinds of **personal information** are used in the operation of the computer programs
 - What kinds of **decisions** are made **solely** by the operation of the computer programs (ie decision-making processes that are fully automated)
 - What kinds of **decisions** are made by human decision-makers but with **substantial and direct assistance** from the computer program

SERIOUS INVASION OF PRIVACY

STATUTORY TORT

What changed?

An **individual** can now take action for a serious breach of their privacy through a statutory tort for the **serious** invasion of privacy

What do you need to do?

- **Be aware** of the tort and its consequences
- **Audit** use of private information

Commencement: 11 June 2025

SERIOUS INVASION OF PRIVACY

- An invasion of privacy includes two types:
 - **Intrusion upon seclusion** i.e. physically intruding into someone's private space or watching/listening/recording private activities/affairs
 - **Misuse of information** including the unauthorised collection, use or disclosure of information that relates to the individual

SERIOUS INVASION OF PRIVACY

STATUTORY TORT

- For the invasion of privacy to be actionable there must be:
 - A reasonable expectation of privacy
 - Intentional or reckless invasion
 - Serious invasion
 - The public interest in the plaintiff's privacy outweighs any countervailing public interest
- No need to prove damage

SERIOUS INVASION OF PRIVACY

STATUTORY TORT

- Statutory defences to the tort include:
 - Lawful authority
 - Consent
 - Necessary to prevent threat to life/health/safety
 - Certain defamation law defences
- Exemptions for media, law enforcement, intelligence and minors
- Time limits on bringing an action
- Exemplary or punitive (but not aggravated) damages available

CHILDREN'S ONLINE PRIVACY CODE

What changed?

■ The Act:

- Sets up the framework for development of a Children's Online Privacy Code
- Leaves the specifics to the Australian Information Commissioner
- Introduces a definition of a child in the Privacy Act as 'an individual who has not yet reached 18 years'

What do you need to do?

- **Interrogate** whether any online service you provide is likely to be accessed by children
- **Familiarise** yourself with the UK Age Appropriate Design Code

Commencement:

11 December 2024 (Requirement to develop Children's Code) HWL

11 December 2026 (Registration of Children's Code)

CHILDREN'S ONLINE PRIVACY CODE

- APP entities will be bound by the Children's Code, unless otherwise specified, if:
 - The entity is a provider of a social media service, relevant electronic service or designated internet service;
 - The service is likely to be accessed by children; and
 - The entity is not providing a health service
- OR
- The entity is specified in the Code as bound by it

Commencement:

11 December 2024 (Requirement to develop Children's Code)
11 December 2026 (Children's Code)

ONLINE SERVICES AND CHILDREN

CHILDREN'S CODE

Code will cover:

- a) Social media services;
- b) Relevant electronic services; and
- c) Designated internet services likely to be accessed by individuals under 18 years old

E.g.

- Websites (including educational/news sites)
- Apps
- Instant messaging services
- Online gaming services
- Search engines
- Content streaming services

SOCIAL MEDIA BAN

Providers of age-restricted social media platforms must take reasonable steps to prevent individuals under 16 years old from holding accounts

Children 0-16 years old using certain 'social media platforms' with an account

UPDATED DATA SECURITY REQUIREMENTS

What changed?

An APP entity must now include ‘technical and organisational measures’ as part of the steps it takes to protect information from misuse, interference and unauthorised access or disclosure

What do you need to do?

- **Check** that you have governance and organisational data security controls in place
- **Implement** measures in areas which are lacking

Commencement: 11 December 2024

OVERSEAS DISCLOSURE WHITE LIST

What changed?

The Act introduces a separate mechanism for the Commonwealth government to recognise foreign laws and binding schemes that are considered adequate and therefore allow cross-border disclosure

What do you need to do?

- **Watch** for Government publication of recognised foreign laws

Commencement: 11 December 2024

DATA BREACH RESPONSE DECLARATIONS

What changed?

The Minister will be empowered to make eligible data breach declarations to allow entities to collect, use and disclose personal information in ways that are not otherwise permitted under the APPs

What do you need to do?

- **Update** your data breach response plans
- **Be aware** of the potential for a data breach declaration from the Minister

Commencement: 11 December 2024

NEW CIVIL PENALTY OPTIONS



Section 13G

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

Section 13H

Civil penalty provision for **interference** with privacy of an individual

Section 13K

Civil penalty provision for **infringement/compliance notices**

NEW CIVIL PENALTY OPTIONS

NEW PENALTY TIERS

What changed?

- Section 13G - Civil penalties for **serious or repeated** privacy interferences replaced with penalties for **serious** interferences with privacy
- Section 13H – New mid-tier penalty for an interference with privacy where the court is not satisfied the interference is serious

What do you need to do?

- **Be aware** of a broader range of penalties for breaches
- **Audit compliance** with APPs and other relevant laws

Commencement: 11 December 2024

NEW CIVIL PENALTY OPTIONS

NEW PENALTY TIERS

- Seriousness may be considered against the following criteria:
 - the kind of information involved in the interference with privacy
 - the sensitivity of the personal information of the individual
 - the consequences, or potential consequences, of the interference with privacy for the individual
 - the number of individuals affected by the interference with privacy
 - whether the individual affected by the interference is a child or person experiencing vulnerability
 - whether the act was done repeatedly or continuously
 - whether the contravening entity failed to implement procedures to comply with privacy obligations in a way that contributed to the privacy interference
 - any other relevant matter

NEW CIVIL PENALTY OPTIONS

'SPEEDING FINES'

What changed?

- Section 13K - Civil penalties imposed by way of infringement notices issued by the Commissioner for a variety of prescribed contraventions
- The penalty is **per contravention**, even if multiple contraventions are included in the same penalty notice

What do you need to do?

- **Be aware** of a broader range of penalties for breaches
- **Audit compliance** with APPs and other relevant laws

Commencement: 11 December 2024

NEW CIVIL PENALTY OPTIONS

'SPEEDING FINES'

Infringement notices can be issued for breaches of the following:

Requirement to have
APP privacy policy

APP 1.3

Contents of APP
privacy policy

APP 1.4

Individuals may
choose not to identify
themselves in dealing
with entities

APP 2.1

Written notice of
enforcement-related
uses or disclosures

APP 6.5

Simple means for
individuals to opt out
of direct marketing
communications

APP 7.2(c) or 7.3(c) and 7.3(d)

Giving effect to opt
out request in
reasonable period

APP 7.7(a)

Notification of source
of marketing
information

APP 7.7(b)

Dealing with
correction requests

APP 13.5

CRIMINAL DOXXING OFFENCE

What changed?

The Act has amended the Criminal Code to introduce two new criminal offences for 'doxxing', with jail terms of up to 7 years

What do you need to do?

- **Be aware** of the risk and consequences of doxxing
- **Be aware** of the possible recourse if you or a colleague experience doxxing

Commencement: 11 December 2024

CRIMINAL DOXXING OFFENCE

- Doxxing is generally considered to involve the intentional online exposure of an individual's identity, private information or personal details without consent
- Offence to:
 - use a 'carriage service' to
 - make available, publish or distribute
 - information that enables an individual to be identified, contacted or located
 - in a way that reasonable persons would consider to be menacing or harassing to the individual

OTHER PRIVACY-ADJACENT UPDATES

- *Digital ID Act 2024*

- Legislates a voluntary Accreditation Scheme for digital ID service
- Expands the Australian Government Digital ID System (AGDIS)

- *Cyber Security Act 2024*

- Minimum cyber security standards for internet/network devices
- Requires organisations to notify the Government within 72 hours of acquiescing to a cyber extortion demand
- Encourages organisations to voluntarily share information with government cyber security officials
- Establishes independent advisory board to conduct no-fault reviews of novel or nationally significant cyber incidents

UNFAIR CONTRACT TERMS & PRIVACY CLAUSES

- Unfair contract terms in standard form contracts (UCTs) are prohibited under the Australian Consumer Law and since 2023 carry heavy penalties
 - Expanded definition of what constitutes a “small business contract”
- Privacy clauses in template contracts should be analysed for fairness

What do you need to do?

- **Check** your entity's service agreements and standard form contracts for the presence of potentially unfair privacy provisions

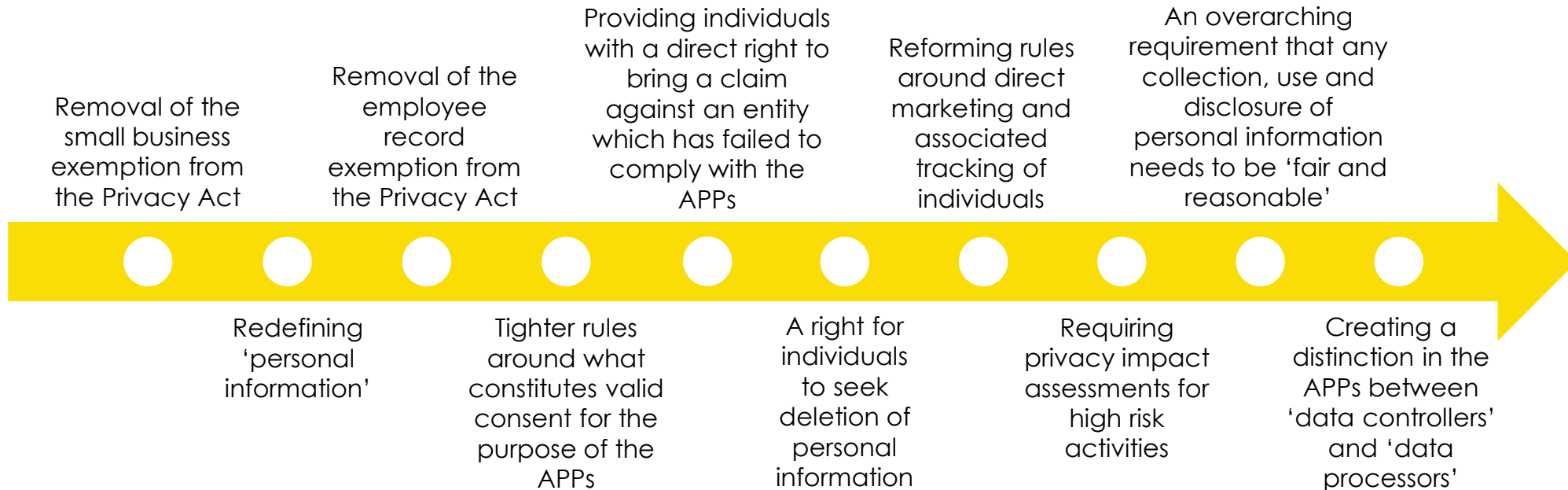
Commencement: 9 November 2023



WHAT'S NEXT?



POTENTIAL FUTURE PRIVACY LAW UPDATES



QUESTIONS?




CONTACT DETAILS



NIKKI MACOR HEATH
SPECIAL COUNSEL, SA

T +61 8 8205 0515
E nmacorheath@hwle.com.au





**This seminar and accompanying
documentation is not intended to
be legal advice and should not
be relied upon as such.**

The copyright of this material is
and will remain the property of
HWL Ebsworth Lawyers.

The background features a dark green field with several light-colored, textured geometric shapes. In the top left is a square, in the top right is a circular ring, and in the bottom right is a sphere. All these shapes have a pitted, crater-like texture. A large, semi-transparent white circle is centered behind the text.

HWLEBSWORTH

LAWYERS

ADELAIDE | BRISBANE | CANBERRA | DARWIN | HOBART | MELBOURNE | NORWEST | PERTH | SYDNEY