DAVIES COLLISON CAVE LAW

dcc.com

PRIVACY REFORMS

THE LAST 12 MONTHS AND THE NEXT

PREPARED BY
Gordon Hughes

DATE
12.03.26

AGENDA

- The purpose of the Privacy Act
- Background to the reform process
- This time last year
- The last 12 months
- The next 12 months

BACKGROUND – EVOLUTION OF THE PRIVACY ACT

- The *Privacy Act* has experienced problems from the very outset
  - Confined to the Commonwealth public sector
- Major amendment in 2001
  - Extended to private sector, but two sets of privacy principles
- Major amendment in 2014
  - Privacy Principles consolidated
- Lingering problems
  - Not up to international standard
  - Contentious exemptions
  - Lack of "adequacy" status
  - Imprecise cross-border transfer obligations
  - Excessive reliance on APP Guidelines

DAVIES COLLISON CAVE LAW
dcc.com
Privacy Reforms – The last 12 months and the next

BACKGROUND – THE CURRENT REFORM PROCESS

- **2017** – ACCC investigation into online search engines
  - Commenced 2017
  - Final report 2019 – *Digital Platforms Inquiry Final Report*
- **2019** – Commonwealth government response
  - Further ACCC investigation into ad-tech
- **2020** – Commonwealth government Issues paper
- **2021** – Commonwealth government Discussion Paper
- **2022 -** Interim Reform:
  - Penalties increased
- **2023** – Two developments
  - February: Attorney-General's *Privacy Act Review Report*
  - September: Attorney-General announces review of *Privacy Act* after assessing feedback

2024 REFORMS

- Four distinct initiatives:
  - Amendments to the data protection provisions of the *Privacy Act*
  - Amendment of the Criminal Code to create the offence of "doxxing "
  - Introduction of a statutory tort of privacy in the *Privacy Act*
  - Enhanced data security obligation pursuant to the *Cyber Security Act 2024* (Cth)

DAVIES COLLISON CAVE LAW
dcc.com
Privacy Reforms – The last 12 months and the next

DATA PROTECTION REFORMS – PROGRESS REPORT

- Four changes which potentially impacted the current data protection provisions of the Privacy Act:
  - APP 8 – whitelist – no countries have been formally whitelisted
  - APP 11 – reasonable security measures – no decisions by Privacy Commissioner involving the new APP 11.3
  - Part IIIC – notifiable data breaches – no declarations by the Minister involving the new Division 5 of Part IIIC
  - Automated decision making – changes not due to come into effect until 10 December 2026

2024 DOXXING REFORM – PROGRESS REPORT

- "Doxxing" takes many forms but essentially involves the intentional online exposure of an individual's identity, private information or personal details without their consent
- 2024 Amendment Bill amended the Criminal Code to create two new offences of doxing:
  - Releasing personal data to harass an individual
  - Releasing personal datal to discriminate against a group
- Penalty – up to 7 years' imprisonment
- Privacy Act exemptions do not apply
- There have been no publicly reported prosecutions under the new law (although federal criminal cases often take a significant time to investigate, charge and proceed to court, specially given that identifying an online perpetrator can be technically and legally complex).

DAVIES COLLISON CAVE LAW
dcc.com
Privacy Reforms – The last 12 months and the next

STATUTORY PRIVACY TORT – BACKGROUND

Common law position unclear:

- *ABC v Lenah Game Meats* (2001) 208 CLR 199
- *Doe v ABC* [2007] VCC 281
- *Sands v South Australia* [2013] SASC 44

Recommended legislation:

- ALRC, 2008
- VLRC, 201
- Federal Government Discussion Paper, 2011
- ALRC, 2014
- NSW Standing Committee of Justice, 2016
- ACCC, 2018

STATUTORY PRIVACY TORT – KEY ELEMENTS

- Not the same as data protection
- Key elements:
  - Intruding upon seclusion or misusing information
  - Person had a reasonable expectation of privacy
  - Intentional or reckless act
  - Serious
- Exemptions
- Damages

STATUTORY PRIVACY TORT – PROGRESS REPORT

- Commenced 10 June 2025
- **First decision** – *Kurraba Group Pty Ltd & Anor v Williams* [2025] NSWDC 396 (7 October 2025)
- Court granted interlocutory relief based on allegations of a "campaign of extortion" involving misuse of private information and publication of wedding photos online
- Has been heralded as "early guidance on how courts will interpret the elements of the tort, especially 'serious invasion' and 'misuse' of information". But this may be an over-hyped assessment of the decision (interlocutory ruling in an essentially defamation case)
- **Second case** – *Groth & Groth v Herald and Weekly Times* (Federal Court) – defamation and privacy – settled November 2025

CYBER SECURITY ACT – PROGRESS REPORT

- *Cyber Security Act 2024* (Cth) addresses:
  - (Part 2) – mandatory security standards for smart devices
  - (Part 3) – mandatory reporting obligations regarding ransomware
  - (Part 4) – information sharing for entities impacted by a cyber security incident
  - (Part 5) – Cyber Incident Review Board
- Parts 4 and 5 commenced 30 November 2024; Parts 2 and 3 did mot commence in 2024
- Part 2 – will become operational when subordinate instrument, the *Cyber Security (Security Safeguards for Smart Devices) Rules 2025* become operational – commenced 4 March 2026
- Part 3 – commenced 30 May 2025

No reported prosecutions or civil penalties as yet

OTHER NEW PRIVACY DEVELOPMENTS IN 2025

Legislation – social media restrictions

- *Online Safety Amendment (Social Media Minimum Age) Act 2025*, Part 4A
- Came into effect 10 December 2024, commenced 10 December 2025 with 12-month lead-in
- Key features: specified platforms (inc. Tik Tok, YouTube, X and Facebook) must take reasonable steps, using age verification technology, to prevent users under the age of 16 from holding accounts
- Penalties (up to $50m) apply to platforms, but not children or parents
- OAIC has published a Guide for platform providers in view of the personal information which may be handled when undertaking age verification

OTHER NEW PRIVACY DEVELOPMENTS IN 2025 (CONT.)

Facial recognition technology

Privacy Commissioner determination – September 2025 – *Kmart* - Kmart did not notify shoppers or seek their consent to use FRT to collect their biometric information – excessive to the exemption applicable to combatting unlawful activity or serious misconduct

Administrative Review Tribunal determination - February 2026 – *Bunnings* - Bunnings contravened Australian Privacy Principles (APP) 1 (open and transparent management of personal information) and 5 (notification of the collection of personal information) when rolling out facial recognition technology in its stores

OAIC Guidance: "Facial recognition technology and privacy" - general considerations for private sector organisations that are considering using facial recognition technology (FRT) to undertake facial identification in a commercial or retail setting

DAVIES COLLISON CAVE LAW
dcc.com
Privacy reforms - the last 12 months and the next

OTHER NEW PRIVACY DEVELOPMENTS IN 2025 (CONT.)

Civil penalties

Civil penalty decision - ACL

AIC v Australian Clinical Labs [2025] FCA 1224 – 8 October 2025 – first civil penalty case resulted in $5.8m civil penalties – failure to take reasonable security steps (breach of APP 11.1) and failing to conduct expeditious assessment regarding a possible "eligible data breach" under Part IIIC of the *Privacy Act*

Matter in progress - Optus

AIC v Optus – August 2025 – AIC commenced civil penalty proceedings over the 2022 cyber attack which affected 9.5 million individuals (the OAIC itself cannot impose penalties, but may apply to the Federal Court for a civil penalty order). Theoretical exposure is a maximum of $2.2m in respect of each of the 9.5 million data subjects

2026 AND BEYOND

Reforms previously foreshadowed and possibly on the horizon:

- Fair and reasonable test
- Harmonisation
- Review of exemptions
- Notice and consent
- Privacy Policies
- Controllers and processors
- Personal rights and freedoms
- Security and destruction
- Direct marketing and targeting

This is the same as last year's list.

DAVIES COLLISON CAVE LAW
dcc.com

Presenter

Gordon Hughes
Principal Lawyer
Davies Collison Cave Law
ghughes@dcc.com