Reforms to Privacy Laws

THOMPSON COOPER LAWYERS

7 September 2023

Welcome and Introduction

Patrick's entire career has involved acting in litigated and non-litigated liability claims, almost exclusively on behalf of insurers and defendants. He advises public and private sector clients in a range of fields including privacy, compliance and contractual matters. His experience includes:

- Acting for major insurers in general liability litigation including contractual and consumer law matters.
- Advising the Commonwealth Government in relation to privacy compliance and complaints, including conduct of OAIC investigations.
- Acting for higher education sector clients in discrimination, victimisation, data breach and privacy disputes.
- Investigations regarding allegations of workplace misconduct or harassment.
- Property damage claims involving utilities and the roll-out of public infrastructure projects.
- Defending professional negligence claims against engineers, building designers, certifiers and allied medical practitioners.
- Acting for institutions and/or their insurers in a large number of historical abuse claims

Patrick is an experienced practitioner in ADR. In litigated claims, Patrick has acted in many State courts and all Federal courts, as well as in many tribunals.

Patrick has lectured at a post-graduate level on professional negligence/conduct claims and records management for allied medical practitioners. He participates in numerous law and insurance industry bodies and associations.

Patrick Riordan
Principal
thompson cooper lawyers

thompson cooper lawyers

Reforms to Privacy Laws

Presentation to Unimutual members
7 September 2023

Patrick Riordan
Principal, Thompson Cooper Lawyers

A quick “about us”

1. Thompson Cooper Lawyers has acted in Unimutual matters for many years, including acting in privacy disputes for Unimutual members (State/Territory jurisdiction)

2. Advising on privacy practices and compliance (Commonwealth Government departments, ASX200 companies, private companies, schools, universities, community organisations)

3. Acting for respondents to privacy complaints in Commonwealth jurisdiction (including OAIC investigations)

Agenda

1. Overview
2. Drivers of reform
3. Commonwealth reforms
4. State/Territory reforms
5. What to do?

thompson cooper lawyers

Section 1 – **Overview of privacy laws**

Privacy Act 1988 (and similar State/Territory laws)

- Main objective is to regulate how organisations handle “personal information”
  - Personal information is usually defined as information about an individual who identity is apparent from, or can be reasonably ascertained from, the information.
  - Names/addresses … car registration, IP addresses, student numbers?

- 13x Australian Privacy Principles (APPs). These are rules dealing with topics like collection, security, storage, access to and disclosure of personal information E.g. APP 1 relates to open and transparent management of personal information.

- Some crossover between APPs and State/Territory laws – e.g. the “Information Protection Principles” in Privacy and Protection of Personal Information Act 1998 (NSW).

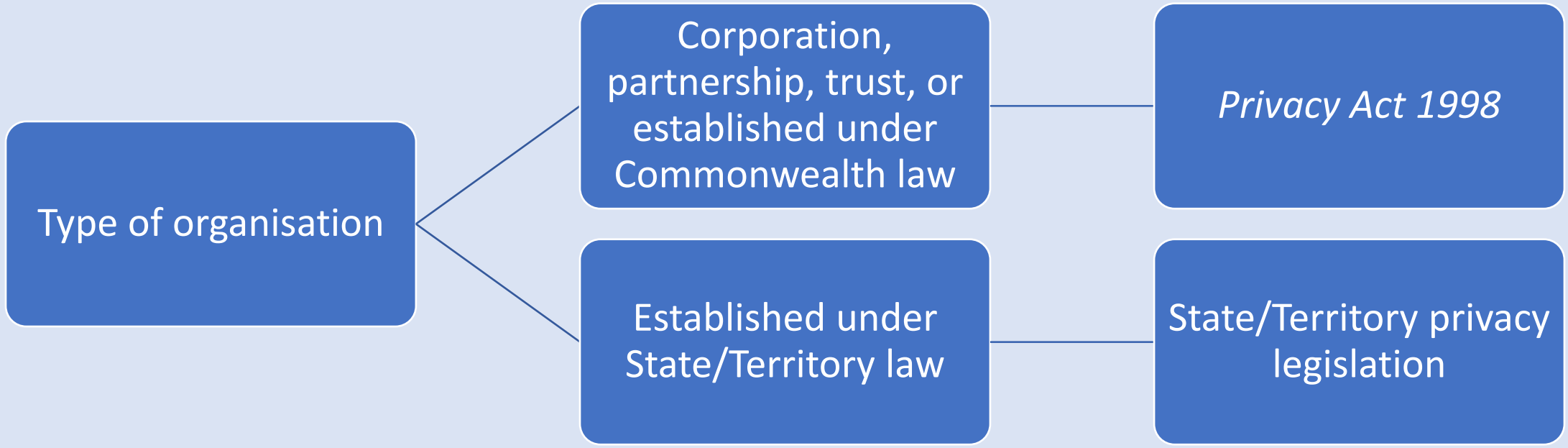
Applicability of different laws

- Under the Privacy Act, all "APP entities" are required to follow the APPs; s 15. Those "APP entities" include "agencies" (generally Commonwealth bodies) or "organisations"; s 6.

- An "organisation" includes (s 6C) body corporates, partnerships, trusts but not State or Territory authorities or small businesses ($3M turnover).

- A "State or Territory authority" includes bodies (incorporated or not) established under a State/Territory law. E.g. many universities which have a State enabling Act (e.g. *Monash University Act 2009* (Vic)).

Applicability of laws – a (very*) simplified overview



*there are lots of exceptions / qualifications!
*can be subject to both – e.g. incorporated business unit, or contracted service provider to agency

State/Territory Regimes

New South Wales

- *Privacy and Personal Information Protection ACT 1998* (NSW).

Queensland

- *Information Privacy Act 2009* (Qld).
- *Right to Information Act 2009* (Qld).

Victoria

- *Privacy and Data Protection Act 2014* (Vic).

Australian Capital Territory

- *Information Privacy Act 2014* (ACT).

State/Territory Regimes

Northern Territory

- *Information Act 2002* (NT).

South Australia

- No legislation, but agencies subject to PC circular 102 – *Information Privacy Principles (IPPS) Instructions*.

Tasmania

- *Personal Information Protection Act 2004* (Tas).

Western Australia

- *Freedom of Information Act 1992* (WA).

Information Protection Principles (State/Territory laws)

- Most State/Territory regimes invoke “Information Protection Principles” (or similar name)
- Generally these deal with topics similar to APPs, e.g.:
  - Only collecting personal information where necessary, and where steps taken to make person aware that their information is being collected, and why it is being collected
  - Safe and secure storage of personal information
  - Allowing people access to their personal information
  - Permitting amendment of personal information that is held
  - Limits on use of personal information (considering purpose of collection)
  - Limits on disclosure of personal information (person aware, agrees, or exemption applies)

Regulators

- OAIC (Commonwealth)
- State/Territory regulators including
  - Information and Privacy Commission (NSW)
  - Office of the Information Commissioner QLD
  - Office of Victorian Information Commissioner

  …and others
- Regulators generally:
  - Oversee compliance with applicable privacy principles
  - Investigate complaints, and/or commence investigations of own accord
  - Conciliate complaints/disputes, sometimes with power to direct remedial action or payment of compensation (modest)
  - Make determinations and can enforce via Court action

thompson cooper lawyers

Section 2 – **Drivers of reform**

Privacy Act Review Report

- February 2023 - Attorney-General's Department released review of the *Privacy Act 1988* (Cth)
- Follows two year process of consultation
- Doubts about whether Act (first enacted 1988) fit for purpose 30+ years later
- Community support for stronger privacy protections, minimising personal data retained by organisations. E.g. report follows the 2022 Optus and Medibank data breaches.
- The report included 116 recommendations based on 30 key themes.

Attorney-General's Department

*"The proposed reforms are aimed at **strengthening the protection of personal information** and the control individuals have over their information. Stronger privacy protections would **support digital innovation and enhance Australia's reputation** as a trusted trading partner."*

thompson cooper lawyers

Section 3 – **key proposed Commonwealth reforms**

‘Fair and reasonable’ test

- The collection, use and disclosure of personal information to be ‘fair and reasonable’ in the circumstances.
- Factors to consider include:
  - the reasonable expectations of the individual;
  - the kind, sensitivity and amount of personal information being collected, used or disclosed; and
  - whether the impact on privacy is proportionate to the benefit of the activity.
- The ‘fair and reasonable’ test applies regardless of whether an individual has provided their consent (notice and consent forms place *“an unrealistic burden on individuals”* in understanding the use and risks around their personal information).

Amended definitions: personal information

Personal information

- Definition is intended to be an “expansive”, contrary to Telstra case below
- Amendments were recommended following *Privacy Commissioner v Telstra* (2015):

> *“The starting point must be whether the information or opinion is about an individual. If it is not, that is an end of the matter and it does not matter whether that information or opinion could be married with other information to identify a particular individual.”*

- The definition should change from information ‘about’ an individual to information that **‘relates to’ an individual** (this is broader).
- The definition of ‘collects’ should expressly extend to information obtained from any source by any means.

Amended definitions: de-identified information and sensitive information

De-identified information

- De-identification is a process informed by best available practice.
- The report proposes protection of de-identified information and prohibition on entities from re-identifying any de-identified information, except through the affected person.

Sensitive information

- Similar to personal information, the definition will change from information 'about' an individual to information that **'relates to' an individual**.
- Sensitive information can be inferred from non-sensitive information.

Collection Notice and Consent Requirements

Privacy Notices/Policies

- Privacy notices are required to be **clear, up-to-date, concise** and **understandable**.
- Entities are required to include information regarding whether data is ‘high risk’ and the types of personal information that may be disclosed overseas.
- Data retention periods are to be stipulated.

Consent Requirement

- Consent needs to be **voluntary, informed, current, specific,** and **unambiguous**.
- Valid consent must be given with **capacity**.
- Consent can be express or implied.

Data breaches and data trading

Data breaches

- To be reported to the OAIC within 72 hours.
- The content of the breach notice will need to include the steps taken to reduce adverse impacts on the affected individuals.

Data trading

- Applies to de-identified and personal information (including that which is unidentified).
- Individuals should be able to opt-out of their personal information being used or disclosed for marketing.

Reduced exemptions

Small businesses

- Individuals expect their data to be responsibly handled even by small businesses
- Consultation on how to extend protections so they apply to small businesses

Employment

- Reduce scope of employee/employer exemption to Act
- Require employers to be transparent about information they collect on employees
- Ensure that employees' personal information is protected from misuse & unauthorised access, and is destroyed when no longer required.

Redress and penalties

Redress

- Direct course of action for individuals to apply to the Federal Court or the Federal Circuit and Family Court of Australia.
  - The complaint will need to be assessed first by the OAIC or an recognised external dispute resolution scheme to ensure that there is no reasonable likelihood of the complaint being resolved by conciliation.
- New tort for serious invasions of privacy.
  - ➢ More litigation

Penalties

- For a person other than a body corporate, to $2.5 million; and
- For a body corporate, to an amount not exceeding the greater of:
  - $50 million;
  - three times the value of the benefit obtained from the conduct constituting the serious or repeated interference with privacy, if the court can determine this value; or
  - if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover in the relevant period.

thompson cooper lawyers

Section 4 – **key State/Territory reforms**

Privacy and Personal Information Protection Act 1988 (NSW)

- Reforms passed by the *Privacy and Personal Information Protection Amendment Act 2022* (NSW):
  - Extending the Act's application to entities established under the *State-Owned Corporations Act 1989* (NSW).
  - New Mandatory Notification of Data Breaches scheme (MNDB) for public sector agencies (immediate notification if "serious harm" likely).
  - Amended transparency requirements (maintain register, publish details on data breaches).
  - Expanding the Commissioner's powers, including to oversee data breach responses and accessing premises to check data handling systems/policies.

Information Privacy Act 2009 (Qld) and *Right to Information Act 2009* (Qld)

- Proposed reforms, modelled off Commonwealth proposals:

  - Consultation period mid-2022, on whether to make "*significant changes … to enhance protections for personal information and remedies for individuals whose privacy is breached*"
  - Amend definition of "personal information" to clarify that technical/inferred information can be "personal" and to be more consistent with the *Privacy Act 1988* (Cth).
  - Adopt a mandatory data breach notification scheme based off the Commonwealth Notifiable Data Breach scheme.
  - Enhanced powers for Information Commissioner to investigate and appear in QCAT complaint proceedings
  - Establish Queensland Privacy Principles in line with the Commonwealth APPs (i.e. consolidation of the QLD information principles).
  - Require agencies to take 'reasonable' steps to protect personal information.

Other jurisdictions

- … watch this space

thompson cooper lawyers

Section 5 – **What to do?**

Next steps

- Review all personal information held by your organisation.
  - Do you really need this personal information?
  - Asset or liability?
  - Consider de-identification, disposal, protocols for hold duration
- Review existing work from home policies
  - Security/storage of personal information.
  - Employee devices, data breaches?
- Cybersecurity defences, policies.
- Governance, culture

Next steps

- Identify regime(s) applying to your organisation
- Staff training, especially around collection, storage, use, security (including IT security) and disclosure of personal information and MNDB regime.
- Review accountabilities, ensuring that a senior person leads or has responsibility for privacy.
- If required, commence public and internal data breach register.
- Ensure records are updated to demonstrate compliance should they be requested.

thompson cooper lawyers

Thank you

priordan@tclawyers.com.au

Q & A

Unimutual Limited
Suite 11.02, Level 11,
56 Pitt Street, Sydney NSW 2000
Phone: (02) 9169 6600

Email: service@unimutual.com.au
Website: www.unimutual.com

ABN: 45 106 564 372
AFS Licence No: 241142