LEGISLATIVE CHEATSHEET FOR PRIVACYLAW

A Quick Guide

DIGITAL RIGHTS WATCH©

Glossary

LEGISLATION FLOW CHART

Step 1: What is the Conduct being complained of?

Access to government documents?

→ Go to FOI pathway (Freedom of Information Act 1982 (Cth))

Destruction/alteration/non-release of Commonwealth records?

→ Archives Act 1983 (Cth)

Health information collection/use/disclosure or access?

→ If in Victoria more generally (health info outside My Health Record): Health Records Act 2001 (Vic)
→ If it's the national My Health Record system: My Health Records Act 2012 (Cth)

Surveillance or recordings?

→ If Commonwealth law-enforcement activity (warrants, computer access warrants, data disruption/network warrants): Surveillance Devices Act 2004 (Cth)
→ If private/commercial/individual recording or tracking in Victoria (listening/optical/tracking in private settings): Surveillance Devices Act 1999 (Vic)

Interception of communications / stored communications / metadata?

→ Telecommunications (Interception and Access) Act 1979 (Cth) (interception, stored comms, journalist information warrants, civil remedies)
→ Telecommunications Act 1997 (Cth) (carrier/customer information confidentiality, location info, disclosure exceptions)

Border search/seizure or device copying by Australian Border Force /immigration?

→ Customs Act 1901 (Cth) + Migration Act 1958 (Cth)

Consumer data portability/sharing under Consumer Data Right?

→ Competition and Consumer Act 2010 (Cth) — Consumer Data Right Rules (CDR)

Otherwise: suspected unlawful collection, use, disclosure, or mishandling of personal information?

→ Go to Step 2 (Who is the actor?)

Step 2: Who carried out the conduct being complained of?

Victorian Bodies

Victorian public sector (departments, councils, VicPol, statutory bodies) or a contracted service provider to them?

→ Privacy and Data Protection Act 2014 (Vic) (check scope/exemptions; then apply IPPs, PIDs, IUAs, VPDSS)
If the conduct also raises privacy, correspondence, reputation, or expression concerns:
→ Victorian Charter of Human Rights and Responsibilities (section 13 privacy; section 15 expression)

Health service/provider or any entity handling *health information* in Victoria?

→ Health Records Act 2001 (Vic) (HPPs; access/complaints)

Commonwealth Bodies

Commonwealth agency OR private organisation with ≥ AUD $3m turnover (or otherwise covered by the Act)?

→ Privacy Act 1988 (Cth) (APPs; OAIC complaints; remedies)

Commonwealth public-sector?

→ Data Availability and Transparency Act 2022 (Cth)

ASIO (search/surveillance/communication of intelligence)?

→ ASIO Act 1979 (Cth)

Australian Border Force?

→ Customs Act 1901 (Cth) + Migration Act 1958 (Cth)

Private entities

Telecommunications companies?

→ Telecommunications (Interception and Access) Act 1979 (Cth) (interception, stored comms, journalist information warrants, civil remedies)
→ Telecommunications Act 1997 (Cth) (carrier/customer information confidentiality, location info, disclosure exceptions)

Companies who handle sensitive information or make more than 3 Million in annual revenue?

→ Privacy Act 1988 (Cth)

Natural persons?

→ Privacy Act 1988 (Cth)

Health service/provider or any entity handling *health information*?

→My Health Records Act 2012 (Cth)

STATE LEGISLATION

Health Records Act 2001 (Vic)

Part 1, sections 1–9 – Preliminary
Purpose, definitions, interpretive provisions, and interaction with other laws.
When to use: Use when clarifying scope, definitions, or the Crown's obligations.

Part 2, sections 10–17 – Application
Explains when the Act applies to public, private, and outsourced bodies. Lists exemptions (courts, tribunals, FOI, media).
When to use: Start here if you're unsure whether the Act binds the organisation in question.

Part 3, sections 18–21 – Privacy of Health Information
Defines interference with privacy and introduces the Health Privacy Principles (HPPs).
When to use: Central provision when assessing whether conduct breaches the Act. Refer to sections 20–21 when applying the HPPs.

Part 4, sections 22–24 – Guidelines
Enables the Commissioner to issue binding or advisory guidelines.
When to use: Important where obligations extend beyond the HPPs.

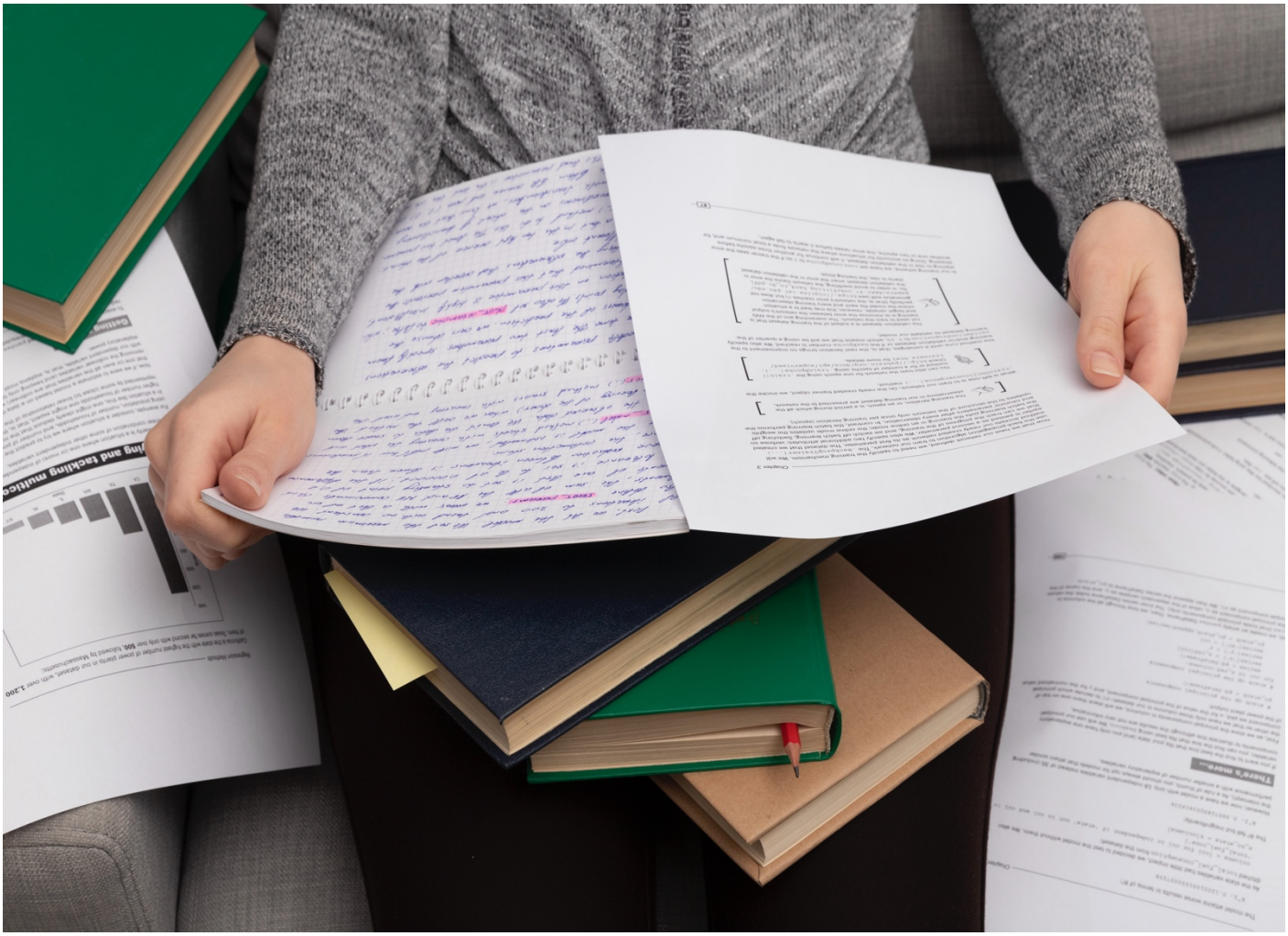
Part 5, sections 25–44 – Access to Health Information
Creates the right to access health information (section 25), subject to limits (risk to life/health, confidentiality). Includes procedures, fees and ID verification for health information access.
When to use: Start here in access/refusal disputes.

Part 6, sections 45–78 – Complaints
Framework for complaints, conciliation (Division 3), investigation (Division 4), and tribunal referral (section 65). Includes interim orders (Division 5).
When to use: Essential for litigation or dispute resolution strategy.

Part 7, sections 79–84 – Offences
Criminalises certain conduct (false representation (section 79), destruction (section 81), obstruction (section 83)).
When to use: Relevant where criminal liability may arise.

Part 8, sections 85–100 – General
Covers miscellaneous matters such as consent capacity, liability protections, the Commissioner's powers, secrecy, and prosecutions.
When to use: Provides the administrative backbone of the Act.

Schedule 1 – Health Privacy Principles (HPPs)
Collection, use, disclosure, security, identifiers, transfers.
Victorian equivalent of the APPs with some variances, tailored to health information.



Victorian Charter of Human Rights and Responsibilities.

section 13 – Privacy and reputation
Protects privacy, family, home, correspondence, and reputation from unlawful interference.

section 15 – Freedom of expression
Relevant to censorship and information controls.
When to use: Use the Charter where privacy issues intersect with broader rights arguments.

Privacy and Data Protection Act 2014 (Vic)

Part 3, Division 1, section 13 – Definition of Victorian Public Sector Organisations (VPSOs)
When to use: Whenever using Part 1 as section 13 establishes scope.

Part 3, Division 1, section 16 – Defines interference of privacy:
Restricts liability to organisations and defines breaches as violations of IPPs, Public Interest Determinations, Information Usage Agreements, or relevant certificates.
When to use: Use when determining if a VPSO has interfered with privacy.

Part 3, Division 1, section 17 – When private organisations can be bound by the act:
State contracts may require that the contractor abide by the IPPs. State contractors may be held to the same standard as the VPSO they are contracted by.
When to use: Use when state government contractors are being scrutinised for their privacy practices.

Sections 10–22 – Exemptions & modifications
Details the application of the Act to courts (section 10), royal commissions (section 10A), and law enforcement (section 15). Lists circumstances whereby information sharing is already covered by other acts and therefore the Privacy and Data Protection Act applies in a modified capacity, eg. Child welfare (section 15B), health services (section 15C) family violence (section 15A) and terrorism (section 15D).
When to use: Use when an agency asserts exemption from an IPP.

Part 3, Division 5, sections 29-42 – Public Interest Determinations (PIDs)
Refer to the Office of the Victorian Information Commissioner for guidance on PIDs Temporary PIDs. Unfortunately, they do not have a publicly available list of current PIDs and temporary PIDs.

- **Subdivision 1, sections 29-3 – PIDs**: Long-term authorisation of non-compliance, where public interest outweighs privacy.
  When to use: Consider where systemic or ongoing data-sharing projects are in play.

- **Subdivision 2, sections 37-41 – Temporary PIDs**: Short-term exemptions for urgent or trial projects.
  When to use: Engage in emergency/pilot scenarios (e.g. Digital ID trials, data sharing during crises).

- **Contexts for Temporary Public Interest Determinations (TPIDs)**
  - Government digital pilots (AI, smart cities, digital ID).
  - Public health and safety emergencies.
  - Research and innovation projects.
  - Cross-border data transfers.

Part 3, Division 8, sections 57–77 – Complaints and Reviews

- **Section 57:** Explains the protocol for filing a privacy complaint.
- **Sections 59 and 60:** Details how the complaints process may be undertaken by children (section 59) and individuals with a disability (section 60).

When to use: To ensure that the complaints process is equitable and accessible. Use these sections if a child or a person with disability is being denied equitable access to make a privacy complaint.

Part 3, Division 8, Subdivisions 2–5: Outlines Commissioner's obligations, conciliation, and VCAT's review powers.

When to use: Essential for advising on remedies and review pathways.

Part 4, sections 84–90 – Protective Data Security

- **Section 84-86 –** Section 86 empowered the Office of the Victorian Information Commissioner (OVIC) to create protective Data standards. The Victorian Protective Data Security Standards (VDPSS) were born from this and represent the minimum standards for handling public sector data. OVIC can issue guidelines, and then the VPDSS itself is the more substantive content. Section 84 outlines the scope of the part and therefore the scope of VPDSS as well.

- **Sections 89–90 –** Section 80 establishes reporting and planning obligations for VPSO data security, while section 90 establishes an exemption for freedom of information requests.

When to use: Look here when assessing cyber breach liability or "reasonable steps" compliance.

Part 6, sections 106–116 – Commissioner's Powers

Oversight, compliance notices, enforcement.

When to use: Relevant for investigations and challenges to agency conduct.

Part 7, section 118 – VPSO employee and agents: VPSOs are liable for the conduct of its employees and agents unless those employees or agents perform the act of their own independent volition. Section 118(3) expresses how the legislation applies to Victoria Police.

When to use: Engage to determine to what extent the VPSO is liable to its employees actions. Look here when the party being investigated is Victoria Police.

Schedule 1 – IPPs: Ten principles governing the collection, use, disclosure, data accuracy, security, access, and correction of personal information held by VPSOs.
When to use: Go here for baseline privacy obligations.

Surveillance Devices Act 1999 (Vic)

Part 2 — Regulation of installation, use and maintenance of surveillance devices

Part 2 establishes surveillance device related offences. Penalty provisions apply to both natural persons and corporate bodies. Also establishes the conditions whereby the sections do not apply (e.g. when the action is authorised through another Act (section 8 (2)).

See sections 32 and 32A for defences available to body corporates accused of breaching privacy and matters to be considered when determining liability.

When to use: Establishing if surveillance activities is an offence and what the penalty provision may be.

Part 2A — Workplace privacy

Restricts the actions workplaces can take to monitor employees. An employer must not knowingly install, use, or maintain an optical surveillance device or a listening device to observe, listen to, record or monitor the activities or conversations of a worker in a toilet, washroom, change room or lactation room.

Part 2A creates offences with corresponding penalty provisions relating specifically to workplace privacy, however, corporations may still be subject to offences under Part 2.

When to use: An individual has had their breaks observed, listened to or monitored by a surveillance device. For example, in Amazon warehouses employees have had their bathroom breaks tracked and employees penalised if they take too long. If this surveillance occurred within the washroom it would violate Part 2A.

Part 3 — Restriction on communication and publication of private conversations and activities

Part 3 restricts the actions individuals may take to publish or communicate private conversations or activities recorded with optical or audio surveillance technology. The key defence to the offences in this part is the subject of the surveillance's consent. Section 12 concerns itself with surveillance footage resulting from police activity.

When to use: If an individual has had a private interaction unknowingly recorded and shared. This includes intimate moments with partners.

Part 4, Division 1, Subdivision 1, section 13 – Types of warrant

Two types of warrants may be issued under Division 1: Surveillance device warrants and retrieval warrants. A warrant may relate to one or more kinds of surveillance devices (listening, optical, data, or tracking).

When to use: When determining the lawful basis for installing or retrieving any form of surveillance device in Victoria. Lawyers should check which of the two authorisations applies to the client's matter.

Part 4, Division 1, Subdivision 2, section 15 – Application for a surveillance device Warrant

A law-enforcement officer may apply if they reasonably suspect an offence has been, is being, or is likely to be committed; and a surveillance device is necessary to obtain evidence or identify an offender. Applications must be approved by a senior officer or authorised police officer and are made to a Supreme Court judge (any warrant) or a magistrate (tracking device only).

When to use: To confirm whether police complied with approval and affidavit requirements, or where emergency applications were made without a sworn affidavit.

Part 4, Division 1, Subdivision 2, section 17 - What a judge must consider when determining an application for a surveillance device warrant

Section 17 sets out the criteria and considerations a Supreme Court judge or magistrate must apply before issuing a surveillance device warrant. A warrant may only be issued if the issuing authority is satisfied that:

- there are reasonable grounds for the suspicion or belief forming the basis of the application;
- in the case of an unsworn application, it was impracticable to prepare or swear an affidavit beforehand; and
- in the case of a remote application, it was impracticable to make the application in person.

When determining whether a warrant should be granted, the judge or agistrate must consider:

- the nature and gravity of the alleged offence;
- the extent to which any person's privacy will be affected;
- whether there are alternative means to obtain the same evidence or information and whether those means would assist or prejudice the investigation;

- the evidentiary or intelligence value of the information sought;
- any previous warrants sought or issued for the same offence (under this Act or
- similar laws); and any submissions made by a Public Interest Monitor.

When to use: Challenging the validity of a warrant (e.g., on grounds that reasonable suspicion or necessity was not established).

Part 4 Division 1, Subdivision 2, section 18 – What a surveillance device warrant must contain

A valid warrant must specify:

- the applicant's name and the offence investigated;
- the kind of device authorised and where it may be used;
- the person or premises subject to surveillance;
- duration (maximum 90 days);
- the executing officer; and
- any conditions or reporting obligations.

When to use: To verify warrant scope, expiry, and conditions before arguing misuse of a device or overreach.

Part 4, Division 1, Subdivision 2, section 19 – What a surveillance device warrant authorises
A surveillance device warrant may authorise:

- Installation, use, and maintenance of a surveillance device on specified
- premises, objects, or persons;
- Entry (by force if necessary) onto those premises or adjoining premises for that
- purpose;
- Retrieval of devices and installation of "enhancement equipment";
- Temporary removal of objects to install or retrieve devices.

It does not authorise surveillance beyond what is specified, nor entry onto unrelated premises.

When to use: When analysing whether police exceeded warrant powers (e.g. installing devices at unlisted locations, or using devices after expiry).

Part 4, Division 1, subdivision 3 — Retrieval Warrants

A retrieval warrant authorises law-enforcement officers to enter premises (using reasonable force if necessary) to recover a surveillance device previously installed under a warrant, or where the device's location is known or suspected. Under section 19(3)(a) every surveillance device warrant authorises the retrieval of the device. It does not authorise new surveillance, only retrieval or maintenance actions.

When to use: Where a device remained in place after expiry or malfunction; or to argue that continued recording breached the prohibition on post-warrant surveillance.

COMMONWEALTH LEGISLATION

My health records act 2012 (Cth)

Part 4 — Authorised collection, use and disclosure of health information

Sets out when My Health Record information can be collected, used, or disclosed. Tightly linked to privacy because it governs the circumstances in which agencies, health providers, or others can access a record.

When to use: Go here when testing if an access or disclosure was lawful.

Part 5 — Offences and Civil penalties

- Section 75 relates to data breaches.
- Section 76-78 relates to health record obligations, rules and penalties.

When to use: Relevant when addressing data breaches relating to health information or privacy interferences.

Part 6, sections 79–81 — Enforcement of penalties

- Division 1 - Civil penalties
- Division 1A - Infringement notices
- Division 2 - Enforceable undertakings
- Division3 – Injunctions

When to use: If an offence or civil penalty occurs under Part 5, look here to understand the process to follow, including possible outcomes.

Consumer Data Right (CDR) under the Competition and Consumer Act 2020 (Cth)

Australia's Consumer Data Right (CDR) was introduced to increase competition by allowing consumers to access and share their data between service providers, particularly in the banking, energy, and telecommunications sectors. The CDR allows individuals and small businesses the right to access and control their own data held by companies and securely share that data with accredited third parties, such as banks. The CDR legislation is complicated, so here it will be broken up into three topics; When does the CDR apply? What are the privacy safeguards? How do I complain if they are breached?

1. When does the CDR apply?

Specifically, the CDR applies when:

- a person is a data holder of designated data (e.g. a bank holding account transaction data); or
- an individual or business is a CDR consumer for that data; and
- an accredited data recipient is permitted to receive the data under the Consumer Data Rules.

The CDR framework overlays existing privacy legislation but is administered primarily by the ACCC and the OAIC.

2. What are the safeguards?

There are dozens of safeguards to ensure the data held by CDR entities is secure. This is a noncomprehensive list of the most important safeguards and when you may need to refer to them.

Part 1, Division 1.3, Rule 1.8 — Data minimisation principle

This section imposes an obligation upon CDR entities to limit data collection to what's necessary.

When to use: If arguing a client's data was over collected.

Part 1, Division 1.4, Subdivision 1.4.5 — De-identification / deletion processes

This section provides a framework for CDR data recipients to de-identify and delete redundant CDR data.

When to use: If a client's CDR data is not properly deidentified or excessive information is kept

Part 4, Division 4.2, Subdivision 4.2.3 — How data holders must ask consumers to authorise disclosure / disclosure rules

This section details CDR data holder obligations to obtain consumer approval before disclosure.

When to use: If testing lawfulness of disclosure; joint account issues (see Part 4A where relevant).

Part 4, Division 4.3, Subdivision 4.3.3 — Information on de-identification

This section describes what the consumer must be informed of for the consent for CDR de-identification to be considered meaningful.

When to use: When determining whether meaningful consent for deidentification was obtained.

Part 4, Division 4.3, Subdivision 4.3.4 — Election to delete redundant data

Provides CDR consumers with the right to request the deletion of their data once it is no longer required for the purpose for which it was collected. The obligation to act on such a request applies both at the time consent is first given and throughout the period for which consent remains valid. However, under sections 4.16(3) and 4.16(4), an accredited CDR data holder may retain the data in specific circumstances, for example, where retention is required by law or necessary for dispute resolution or record-keeping purposes

When to use: If assessing whether a deletion request should be made and if its refusal would be lawful

Part 7, Division 7.2, subdivision 7.2.1, rule 7.3 — PS2 — Anonymity / pseudonymity

When to use: Refer here when a CDR data recipient does not have an anonymity or pseudonymity option.

Part 7, Division 7.2, subdivision 7.2.1, rule 7.3A / rule 7.3B — PS4 — Destruction of unsolicited data (separate rules for CDR reps and OSPs)

When to use: When unsolicited CDR data is received.

Part 7, Division 7.2, subdivision 7.2.2, rule 7.4 — PS5 — Notify of collection

When to use: When determining whether collection notices/receipts were valid. Note: There are different obligations if the data was collected by a sponsor (rule 7.4 (2)).

Part 7, Division 7.2, subdivision 7.2.3, rule 7.5 / rule 7.5A — Meaning of "permitted use or disclosure" and limits on disclosure consents

Rule 7.5(1) establishes the general permitted circumstances and conditions of a permitted use or disclosure of CDR data. Rule 7.5(2) requires that for a use or disclosure of CDR data to be permitted it must adhere to the data standards established in Part 8. Rule 7.5(3) describes the circumstances whereby CDR data can be used for direct marketing purposes. Rule 7.5A establishes the limitations upon disclosures of CDR data under a disclosure consent.

When to use: If establishing if a use or disclosure of CDR was permitted, especially relevant where people may not want their CDR data to be used for direct marketing purposes.

Part 7, Division 7.2, subdivision 7.2.3, rule 7.6 / rule 7.7 — PS6 — Use/disclosure by accredited data recipients

Rule 7.6(1) Penalises unpermitted use or disclosure of CDR data through rule 9.8.

When to use: When disputing downstream re-use of CDR data such as internal sharing.

Part 7, Division 7.2, subdivision 7.2.3, rules 7.8 / rule 7.8A / rule 7.8B — PS7/PS8/PS9 — Enforcement variants Direct marketing, representative/OSP failures

Rule 7.8 reiterates that CDR data may be used for permitted direct marketing purposes. Rule 7.8A(1) relates to the offshore storage and transfer of CDR data. Note: rule 9.8 makes breaching this a civil penalty provision.

When to use: Direct marketing disputes.

Part 7, Division 7.2, subdivision 7.2.3, rule 7.9 — PS10 — Notify of disclosure

When to use: In disputes about whether disclosure notifications were sent and if they were sent in a timely manner.

Part 7, Division 7.2, subdivision 7.2.4, rule 7.10 / rule 7.10A — PS11 — Quality of CDR data; representative nuances

R 7.10A is a civil penalty provision under rule 9.8.

When to use: Claims of damage from inaccurate data; obligations to correct.

Part 7, Division 7.2, subdivision 7.2.4, rule 7.11 – rule 7.13 — PS12 — Security; de-identification & deletion of redundant data)

These sections contain the detailed *Steps for PS12* (minimum controls, incident response, reporting).

When to use: Breach response, "reasonable steps" arguments, security control audits.

Part 7, Division 7.2, subdivision 7.2.5, rule 7.14 – rule 7.16 — PS13 — Correction of CDR data; no fee; CDR rep rules

Rule 7.14 forbids data holders from charging a fee for actioning and responding to CDR related requests and rule 9.8 makes this a civil penalty provision. Under rule 7.15 requests must be acknowledged as soon as practicable and responded to through a statement or correction within 10 days of acknowledgement.

When to use: Consumer correction requests and refusals.

Part 9, Division 9.3, subdivisions 9.3.1 and 9.3.2, rule 9.3 / rule 9.4 / rule 9.6 (Records, reporting, and audits)

These sections detail what records must be kept by CDR data recipients, reporting obligations and audit powers (Commission / Info Commissioner). The requirements differ across data holders (rule 9.4(1)), accredited data recipients (rule 9.4(2)) and CDR representative principals (rule 9.4(2A)). However the civil penalties are the same for all.

When to use: Evidence preservation, audit compliance, regulatory investigations, civil penalty provisions.

Schedule 2 — Detailed steps, minimum controls, incident management

The practical benchmark for what "reasonable steps" look like under rule 7.11.

When to use: Breach triage, forensic analysis, regulator/audit defence, were reasonable steps taken?

3. How do I file a complaint?

Having established some of the matters you may find yourself complaining about, let us now examine how you would file this complaint.

Division 1.5, section 1.26, Dispute resolution — Primary data holders and secondary data holders

Where a primary data holder requests relevant information from a secondary data holder in relation to a consumer complaint or dispute with the primary data holder that relates to a 'Sharing Responsibility' data request, the secondary data holder must provide the information to the extent that it is reasonable to do so.

When to use: If determining which data holder to file a complaint against.

Part 7, Division 7.2, Section 7.2(6) — CDR entities must detail their internal dispute resolution complaints process in their CDR Policy

Under Section 7.2(7), the CDR policy of CDR entities must be readily available to consumers. See Schedule 3, Part 5 for context on how this applies to the NBL and Banking sector. See Schedule 4, Part 5 for how this applies to the energy sector.

When to use: To aid in finding CDR entities specific internal dispute resolution process and filing a subsequent complaint.

Data Availability and Transparency Act 2022 (Cth) (DATA Act)

Part 2.2, sections 14–14A – Penalties for unauthorised sharing, collection, or use of public sector data

When to use: In cases of mishandling or unlawful disclosure of public sector data; framing arguments about accountability and consequences of non-compliance.

Part 2.3, section 16 – Data sharing principles

When to use: To determine whether a sharing arrangement was lawful and whether the "Five Safes" safeguards (safe people, projects, settings, data, outputs) were properly applied.

Part 2.4, section 16B and 16E – Link to the Privacy Act 1988

When to use: When testing compliance with Australia's broader privacy framework; ensuring that data sharing cannot bypass or weaken Privacy Act obligations.

Archives Act 1983 (Cth)

Section 3 — Definitions and interpretation

When to use: If establishing whether matters fall into scope of the legislation. This section establishes what is meant by terms such as 'archives','open access period' ,'Cabinet notebook' and 'commission of inquiry'.

Part 5, Division 1 — Establishes the open access period of all document types covered in the act

When to use: If arguing that a document should or should not be openly accessible.

Part 5, Division 2, section 24 — Disposal, destruction etc. of Commonwealth record

When to use: If official records have been altered, destroyed or had ownership transferred without authorisation, look here to establish what obligations may have been breached and the penalty units.

Part 5, Division 3, section 33 — Which records are exempt from open access periods

When to use: If arguing that a document should or should not be openly accessible, particularly in regard to sensitive information or intelligence.

Part 5, Division 3, section 36 — How may records be accessed

When to use: When arguing that a client did not receive fair access to a record.

Part 5, Division 3, section 40 — Applications for access to records.

When to use: In evaluating whether a client's application was appropriately submitted and handled particularly in regards to delay.

Part 5, Division 4, section 43 — Applications to Administrative Review Tribunal.

When to use: When denied access to archival documents in the original application or you failed to receive an outcome of your application you may assess using this section if you are eligible to apply to the ART to review the decision. See section 44 in regards to the powers available to the ART. See also section 54 which mandates the Inspector-General of Intelligence and Security to personally give evidence at the Tribunal if the requested record is considered exempt on the basis of it being intelligence.

Australian Security Intelligence Organisation Act 1979 (Cth)

Part 1, section 4 — Definitions

When to use: If establishing whether matters fall into scope and if applying matters to the legislation.

Part 3, Division 1, section 18 — Communication of intelligence

When to use: If intelligence whistleblowers approach, they will likely be in breach of this section and be liable for up to 10 years imprisonment. See here for exemptions regarding the sharing of intelligence. There are multiple offences of varying seriousness detailed with 18(1) and (2) being the most severe. Section 18A and 18B are lesser offences, look here to see if clients may be able to have sentences reduced. Offenders can be discharged if proceedings are not held in a reasonable time, see section 18(c)(5). Sections 18, 18A and 18B all contain exemptions and 18D provides an exemption applicable to all 3 offences.

Part 3, Division 2, subdivision A, section 23 — Requesting information or documents from operators of aircraft or vessels

When to use: Under section 23(1)(b) ASIO may request an operator of an aircraft or vessel to produce documents relating to crew and passengers that are in the possession or under the control of the operator. Under section 23(3) failing to comply is an offence. Section 23(5) provides 2 exemptions.

Part 3, Division 2, subdivision B, section 25 — Search warrants

When to use: If a client has been subject to a search, peruse this section to ensure that appropriate warrants were obtained and the search was administered lawfully. Note that under 25(4B) Subsection (4A) does not authorise a strip search or a search of a person's body cavities.

Part 3, Division 2, subdivision B, section 26 — Surveillance Device warrants

When to use: Section 26(3) describes the test to ensure that a warrant is required. When arguing that a client was unlawfully surveilled, one can turn to these requirements and argue that they were not met. Section 26A details what paperwork and signatures is required to authorise a warrant. If section 26A is not adhered to the surveillance may have been unlawful. Section 26B relates to what actions are authorised by a surveillance device warrant, look here to ensure that all surveillance activities were lawful. Section 26C,D and E relate to what surveillance may occur

without a warrant. Ensure that surveillance activities that fall outside of 26B's scope do not fall into the scope of 26C,D and E.

Part 3, Division 2, subdivision DA — Use of tracking devices under internal Authorisation

When to use: Section 26G(6) describes the test to ensure that a warrant is required. When arguing that a client was unlawfully tracked, one can turn to these requirements and argue that they were not met (Note: The bar here is lower than for surveillance device warrants). Section 26H details the requirements to have such a obtain authorisation to use such devices. (Note: The bar here is again lower than in regards to surveillance devices). Section 26J lists the activities that can lawfully be carried out using a tracking device once authorisation is received. Section 26K Lists the acts which are exempt from tracking activities. Such as 'entering premises without permission from the owner or occupier of the premises'. Section 26, L, P and R all relate to the cessation of tracking activities. Look here to ensure that tracking devices were lawfully obtained for disposal and tracking activity has not continued past the authorised timeframe.

Surveillance Devices Act 2004 (Cth)

Part 1, section 6 — Definitions

When to use: If establishing whether matters fall into scope and when applying matters to the legislation. See section 6A for what the Act considers a law enforcement agency.

Part 2, Division 1, Section 10 — Types of warrants

When to use: If establishing whether surveilled activities fit into a warrant category.

Part 2, Division 2, section 14 — Application for surveillance device warrants

When to use: Sections 14(1)-(3E) relate to when different subwarrants may be sought. Identify the type of warrant acquired by law enforcement and then cross reference to ensure that requirements for granting such warrant were met.

Part 2, Division 2, section 16 — Determining if warrants are granted

Section 16(1) outlines what a judge or ART member must be satisfied of before granting a warrant. Sections 16(2)-(5) outlines what a judge or ART member will consider when making a determination.

When to use: Useful when compiling evidence or building an argument, as you may tailor it to the factors the judge will consider.

Part 2, Division 2, section 17 — What must a surveillance device warrant contain?

When to use: If looking to establish the un/lawfulness of a warrant on an administrative basis.

Part 2, Division 2, section 18 — What a surveillance device warrant authorises

When to use: Look here to ensure that all surveillance activities carried out by law enforcement were authorised by the warrant.

Part 2, Division 2 and 3, sections 20,21,22,26 — Cessation of tracking activities

When to use: Look here to ensure that tracking devices were lawfully obtained for disposal and tracking activity has not continued past the authorised timeframe.

Part 2, Division 4, section 27A — Computer access warrants

When to use: Sections 27a(1)-(6A) relates to the requirements of different types of warrants a sworn applicant may utilize. Sections 27a (9)-(13A) relates to the requirements of different types of warrants a sworn applicant may utilize. Ensure that the warrant issued for clients computer access adhered to the requirements established and were filed by a sworn officer.

Part 2, Division 4, section 27C — Matters for consideration when issuing a Computer Access Warrant

When to use: Section 27C(1) relates to the matters that a judge or ART officer must be satisfied of prior to authorising a warrant. Sections 27(2)-(6) relate to the matters that the Judge or ART officer must consider when issuing a warrant. This is relevant if you wish to challenge the grounds upon which the warrant was issued.

Part 2, Division 4, section 27D — What must a Computer Access Warrant contain?

When to use: If looking to establish the un/lawfulness of a warrant on an administrative basis.

Part 2, Division 4, section 27E — What a computer access warrant authorises

When to use: Sections 27E(1)-(4) detail actions that are permitted under the warrant. Ensure that all actions undertaken by authorities are captured in this.

Part 2, Division 4, section 27E (5) — Actions that are not to be undertaken under the warrant

When to use: If determining whether a warrant was carried out lawfully

Part 2, Division 5 — Data Disruption Warrants

When to use: Under the sunset clause section 27KAA this Division ceases to have effect in 2026. These powers are only actionable by ACIC and the AFP

Part 2, Division 6 — Network activity warrants

When to use: Under the sunset clause section 27KKA this Division ceases to have effect in 2026. These powers are only actionable by ACIC and the AFP.

Part 3, sections 33-35 — Application for approval of emergency authorisation

When to use: Under section 33(1) agencies (e.g. AFP, ACIC) can act first under emergency authorisation and only seek judicial approval afterwards. Consider if actions took place under emergency when considering if actions were lawful.

Part 4, section 37 — Use of optical surveillance without warrant

When to use: To establish if a warrant is required for optical surveillance.

Part 4, section 38 — Use of surveillance devices without warrant for listening to or recording words in limited circumstances

When to use: To establish under what circumstances listening devices can be used without a warrant. Relevant when establishing if an individual was unlawfully surveilled.

Freedom of Information Act 1982 (Cth)

Part 1, section 4 — Definitions

When to use: If establishing whether matters fall into scope and if applying matters to the legislation.

Part 3, sections 11, 11A — Right of access and Access to documents on request

When to use: Creates a general right to access government documents, subject to exemptions. Privacy litigants can use these to obtain their own records (e.g. surveillance files, immigration notes, data sharing with third parties).

Part 3, section 11B — Public interest exemptions

When to use: When evaluating if an exemption to comply with an FOI request is valid. These specific sub-types are then detailed in Division 3.

Part 3, sections 15(5),(6), 15AA and 15AB — Appropriate FOI timeframes

When to use: When evaluating if an FOI has been responded to, when evaluating if due procedure was followed.

Part 4, Division 1, section 31A — Access to exempt and conditionally exempt Documents

When to use: There is a useful table here which explains how the act applies to conditionally exempt documents. See section 31B for definition of an exempt document.

Part 4, Division 2, sections 33 - 47A — Exempt documents

When to use: When assessing if documents can be accessed through a FOI.

Part 4, Division 3, sections 47B - 47J — Exemptions based upon public interest

When to use: When assessing if documents can be accessed through a FOI. See section 47F in regards to conditional exemptions for documents where disclosure would involve the *unreasonable disclosure of personal information* about any person. Can be litigated where agencies redact personal data of staff, contractors, or third parties.

Telecommunications (Interception and Access) Act 1979 (Cth)

Chapter 1, Part 1-2 — Interpretations

When to use: If establishing if matters fall into scope and if applying matters to the legislation. See section 6E for lawfully intercepted information. See section 5B for exempt proceedings and section 6 for interception of a communication.

Chapter 2, Part 2-1, section 7 — Telecommunications not to be intercepted

When to use: This section is key to establishing if telecommunications were lawfully intercepted. Section 7(1) establishes that no person shall intercept, authorise the interception, or conduct a preparatory action to intercept a communication passing over a telecommunications system. Section 7(2) then establishes the scenarios where doing this is okay. Broadly, anything that is not done in relation to: building and maintaining telecommunications equipment and lines and warranted law enforcement activities is likely forbidden. However this is a very complicated section with many exceptions to exceptions.

Chapter 2, Part 2-2 — Warrants authorising the Organisation to intercept Telecommunications

When to use: This part establishes the procedure for filing, receiving and enacting interception warrants (telecommunications service warrants (see: Section 9 and 11A) and Named Person warrants (see sections: 9A, 11B and 16).

Chapter 2, Part 2-2, section 9 — Telecommunications service warrants

The warrant allows ASIO to intercept (listen to, record, or access) communications made to or from a specific telecommunications service. It can also authorise ASIO officers to enter premises in order to install, maintain, use, or recover equipment for interception (section 9(1)(b)). Importantly, section 9(3) dictates that such a warrant should only be issued if the Attorney-General is satisfied the measure is a last resort.

When to use: If evidence obtained under such a warrant is being challenged in court (e.g. questions about lawfulness, scope, or admissibility). If a person subject to interception alleges unlawful surveillance and seeks judicial review.

Chapter 2, Part 2-2, section 9A — Named person warrants

The warrant authorises interception of a person's communications (calls, messages, stored communications). It also allows physical entry onto premises to install and recover interception equipment (see section 9A1(b)). Under section 9A(1)(c) prior to authorisation the Attorney-General must be confident relying on a telecommunications service warrant to obtain the intelligence would be ineffective. Under section 9(3) the Attorney-General must also be satisfied that the measure is a last resort.

When to use: If evidence obtained under such a warrant is being challenged in court (e.g. questions about lawfulness, scope, or admissibility). If a person subject to interception alleges unlawful surveillance and seeks judicial review.

Chapter 2, Part 2-2, sections 11A, 11B, 11C and 11D — Telecommunications warrant for collection of foreign intelligence

Section 11A pertains to the acquisition of telecommunications service warrants whereas section 11B pertains to named persons warrants. Under section 11A(3)(a), section 11B(4)(a) and section 11C(3A)(a) if the subject of the requested interception is an Australian citizen the director-general of security must in writing provide the reasons why they suspect the citizen is acting for, or on behalf of, a foreign power. Under section 11A(3)(b), section 11B(4)(b) and section 11C(3A)(b) the Attorney-General must only provide authorisation if she is satisfied there are reasonable grounds for suspecting the citizen. There is no obligation for Australia to comply with the request of a foreign power, nor is there a requirement for Australia to ensure that such communication interception does not facilitate human rights abuses (e.g. the retaliatory killing of the suspect's family or the foreign power seeks to punish the individual for their sexual identity). Under section 11C(5) all intercepted communications not relevant to the purpose in the warrant must be destroyed.

When to use: Section 11 is relevant to Australia's compliance with other nations' wishes particularly in regards to surveillance of political refugees in Australia.

Chapter 2, Part 2-4, section 31A — Attorney-General may authorise interception for developing and testing interception capabilities

This section provides the Attorney-General with the power to authorise random interception of telecommunications for testing capabilities. There are no restrictions described regarding who is targeted for interception. Section 31(2) details the request process. Notably under section 31(2)(g) the interception may span for up to 6 months. Under section 31AA the carrier must be notified of authorisation. The information that was obtained during the interception is no longer required in relation to the development or testing; the head of the security authority must cause the information

or record to be destroyed as soon as practicable. There is no penalty described for failure to comply with section 31AA, nor is 'development and testing' defined. This creates a potential avenue for interception without a warrant and hoarding of data.

When to use: When determining whether a random interception was conducted lawfully, officials must be able to justify the retention or use of any personal information obtained through that interception beyond the six-month period. If a client's personal information was collected through a random interception and retained or used after six months, the agency must demonstrate that the data was necessary for development or testing purposes.

Chapter 2, Part 2-10 — Civil remedies

Section 107A(2) — Defining an aggrieved person

To be considered an aggrieved person the plaintiff must have been party to the intercepted communication or the communication was made on their behalf.

When to use: This section is key to understanding whether an individual may pursue a civil remedy.

Section 107A(3) — Civil remedy

Defines the "defendant" as anyone who has unlawfully intercepted a communication (such as listening in, recording, or otherwise capturing it without authority). It also covers someone who authorises or enables such an interception (not just the person who physically does it).

The Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception. To achieve this they may make such orders against the defendant as the court considers appropriate.

The statutory limitation under section 107B(1) applies to the initiation of proceedings which must occur within 6 years after the end of the interception.

When to use: Refer to section 107A(3) when a client's private communications have been unlawfully intercepted, recorded, or accessed without authority, and you are assessing whether to pursue a civil remedy for that breach. See section 107B(1) to confirm that an unlawful interception occurred within the statutory limitation period before commencing further legal action.

Section 107A (4) — Civil remedy for communication

Remedial action may be taken by the courts if the defendant communicated intercepted information and breaches section 63.

The statutory limitation under section 107B(2) applies to the initiation of proceedings which must occur within 6 years after the end of the communication.

When to use: If an individual's communications have been intercepted and then unlawfully communicated.

Section 107A(5) — Criminal court remedy

If the state prosecutes the defendant and they are convicted of the criminal offence of unlawful interception under section 7(1), the same criminal court can also, on application, award remedies to the victim. So the remedy is civil in nature (damages, injunctions, declarations), but it is available within a criminal prosecution context.

When to use: If an individual wishes to pursue both civil and criminal action prior to an unlawful interception of communications.

Section 107A(6) – Criminal court remedy for unlawful communication

This section is very similar to section 107A (4). The key difference is that in section 107A(6) the defendant has already been convicted in a criminal prosecution of that offence. Key point: Relief is tied to a criminal conviction and is granted in the criminal trial setting, not through separate civil proceedings.
Under section 107B(3) An application under section 107A(5) or (6) for the grant of remedial relief is not subject to any limitation period, but must be made as soon as practicable after the conviction concerned.

When to use: Refer to section 107A(6) when a person has already been convicted of unlawfully communicating or disclosing intercepted information, and the aggrieved party seeks a remedy within the criminal proceedings themselves rather than through a separate civil action.

Section 107A(7) – Orders

Without limiting the orders that may be made under this section against a defendant a court may make an order of one or more of the following kinds:

a) an order declaring the interception or communication to have been unlawful;
b) an order that the defendant pay to damages (punitive damages inclusive according to section 107A(10));
c) an order in the nature of an injunction (including a mandatory injunction);
d) an order that the defendant pay to the aggrieved person an amount not exceeding the amount that, in the opinion of the court, represents the total gross income derived by the defendant as a result of the interception or communication, as the case requires.

The terms of such orders are laid out in section section 107 (8).

When to use: Refer to section 107A(7) when determining what remedies or orders a court may issue following an unlawful interception or communication. Use this section to assess potential outcomes or relief to seek on behalf of an aggrieved person. This section is also useful when advising a client on the range of remedies the court may impose on a defendant.

Chapter 4, Division 4B — Privacy to be considered when making authorisations

Section 180F — Authorised officers to consider privacy

When to use: Refer to this section in a case whereby the interception of communications has egregiously violated privacy. Ensure that these standards have been met. An authorised officer must be satisfied on reasonable grounds that any interference with the privacy resulting from the disclosure or use of intercepted information is justifiable and proportionate, having regard to the following matters:

- the gravity of any conduct in relation to which the authorisation is sought, including:
    - the seriousness of any offence in relation to which the authorisation is sought; and
    - the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and
    - the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and
    - whether the authorisation is sought for the purposes of finding a missing person;
- the likely relevance and usefulness of the information or documents;
- the reason why the disclosure or use concerned is proposed to be authorised.

Division 4C (Sections 180G–180X) — Journalistic Information Warrants

When to use: If your client is a journalist and has been subject to communication intercept. This Division provides heightened protections where law enforcement seeks to access a journalist's metadata to identify confidential sources. These sections require a special warrant and allow Public Interest Advocates to make submissions on whether issuing the warrant is appropriate

Chapter 4A — Oversight by the Commonwealth Ombudsman

When to use: Under section 186B(1) the Ombudsman must inspect law enforcement records to determine the extent of compliance with Chapter 4. Section 186C and section 186D provide the Ombudsman with investigative powers to interview law enforcement agents. The penalty for failing to comply with such a request is imprisonment for 6 months.

Part 5-1A (Sections 187A–187P) — Telecommunications data retention

When to use: These sections mandate service providers retain certain telecommunications data for at least two years. This obligation will become relevant if the 'right to delete' is implemented, as the right will impose a conflicting regulation on the company. The purpose of the data retention is for law enforcement, however these provisions are controversial for their impact on mass surveillance and privacy. Section 187LA explicitly applies the Privacy Act 1988 to retained data, which could be a key reference point for litigation. See section 187AA (1) for a useful table on information that is to be kept.

Customs Act 1901 (Cth)

Volume 3, Part 12, Division 1, Subdivision B, section 186 — Examination of goods Allows

Customs/ABF officers to examine any goods subject to customs control. 'Goods' is defined broadly and includes documents, and by extension, electronic storage devices such as mobile phones, laptops, or USB drives.

When to use: When establishing if technology was legally searched by officers.

Volume 3, Part 12, Division 1, Subdivision B, section 186A – Copies of Documents

Following a search under section 186 a customs officer may make an electronic copy of material on searched phones if they are satisfied with the conditions under section 186A(1)(b). Broadest of these conditions is section 186(1)(b)(v) which refers to any information relevant to security as defined by section 4 of the Australian Security Intelligence Organisation Act 1979.

When to use: Refer here if an individual has had an electronic copy of material stored on their phones created.

Volume 3, Part 12, Division 1, Subdivision J, Section 214AB — What are monitoring powers?

When to use: Monitoring powers enable custom officers to search premises, take photos at a premise, inspect a document or record, make copies of records/documents.

Volume 3, Part 12, Division 1B, Subdivision A, section 219N — Power to require the production of things

A customs officer conducting a frisk search of a person detained for suspicion of being in possession of prohibited goods may require the production of anything found, including devices, as a result of that search. Under section 219Q the individual may be detained for the purpose of being searched.

When to use: When a client is questioning the legality of the search they received and the taking of their belongings by customs officers. Note that the officer only needs to suspect the individual of being in possession of contraband for a search.

Migration Act 1958 (Cth)

Volume 1, Part 2, Division 13A, Subdivision B, sections 261B–261E — Seizure of goods.

Authorised officers may seize items forfeited to the Commonwealth (including devices) where they are reasonably suspected of being used in contraventions of the Migration Act (e.g. people smuggling and unlawful entry). Note here that unlawful entry includes coming to Australia under a different visa and then applying for asylum upon arrival. Therefore, the seizure of electronic devices has disproportionately affected refugees coming to Australia. Some of which experienced long periods of time with their phones confiscated.

When to use: Look here if a client has had electronics goods seized.

Part 8E, Division 3, Subdivision A, section 487F — Powers relating to electronic equipment

This section sets out general search powers for authorised officers, including powers to inspect, examine, and seize evidential material. Search powers include operating electronics on the premises if the officer reasonably suspects that the equipment contains evidential material. If equipment has been damaged in the course of a search refer to section 487F(3) Whereby it is established that an authorised officer may operate electronic equipment only if the officer reasonably believes that the operation of the equipment can be carried out without damage to the equipment. Under section 487F(4) documents or disks must only be seized if it is not practicable to create a copy or the possession of the device or content on it violates the law of the commonwealth.

When to use: When a client's electronic devices have been seized by officers.

Part 8E, Division 3, Subdivision C, section 487T — Compensation for damage to electronic equipment

When to use: If authorised officers damage equipment, data, or programs during a search due to carelessness, the Commonwealth must pay reasonable compensation, either by agreement or through the courts.

Telecommunications Act 1997 (Cth)

Part 7, Division 7, section 138 — Implied Freedom of Political Communication

This section reaffirms that the Telecommunications act shall not impede upon the implied freedom of Political Communication.

When to use: This section may be relevant if telecommunications carriers were to block political messaging.

Part 13, Division 1, section 270 — Confidentiality of telecommunications must be respected

When to use: section 270 provides an outline of Part 13 Division 1. Carriers and carriage service providers must protect the confidentiality of communications, service details, and personal particulars of users. Disclosure is only allowed in limited cases, such as law enforcement. They must also retain communications data under some circumstances.

Part 13, Division 1, section 275A — Location Information

When to use: Explicitly treats mobile phone location data as “customer affairs” information, which brings geolocation tracking into privacy litigation

Part 13, Division 3 — Exceptions to primary use/disclosure offences

When to use: Sets out exceptions, e.g. implicit consent, emergency needs or business operations.

Part 13, Divisions 4 and 4A — Criminalises secondary disclosure

When to use: This section links to the Privacy Act. Section 300 relates to the disclosure of life saving information without the individual's consent, this is relevant to cases where medical or mental health data has been communicated.

Part 15, Division 5 - Compliance and Enforcement.

When to use: Section 317ZA means the main telcos must follow government orders to assist in law enforcement investigations (e.g. intercepting communications, decrypting data), within the limits of the Act. Section 317ZB extends this to any service or platform involved in communications. Failing to comply with such requests is a civil offence (section 137ZC), however the government can negotiate compliance commitments and enforce them later if broken (section 137ZD). If necessary the Federal Court may compel providers to comply with surveillance assistance obligations (section 137ZE).

PRIVACY ACT 1988

Navigating the Privacy Act (Cth)

Step 1: Does the issue fall into scope?

Refer to scope of the privacy act section.
Yes → Continue to step 2
No → Refer to other legislation

Step 2: Does the issue relate to the collecting, handling, storage or transfer of personal information by an organisation, business or agency?

Yes → Read the Australian Privacy Principles (APPs)
No → Go to step 3

Step 3: Does the issue relate to the privacy complaints and investigative process?

Does a client wish to file a complaint regarding privacy with the OAIC? The OAIC may then investigate the complaint and act on behalf of the complainant to penalise the respondent.
Yes → Read section on complaints and investigations
No → Go to step 4

Step 4: Does the issue relate to the civil penalty provision for serious interference with privacy of an individual?

Has an APP been breached or is there a privacy concern regarding an act or practice?
Note: This is separate from the statutory tort for an invasion of privacy
Yes → read section 13G
No → go to next section

Step 5: Does the issue relate to the statutory tort for invasion of privacy?

Has your client experienced a breach of privacy and wishes to sue the defender directly rather than through the OAIC?
Yes → read section on the privacy tort
No → go to next section

Scope of the Privacy Act (Cth)

Firstly, is your concern in scope? The Privacy Act has strict scope that makes many entities exempt from parts of the act.

Does your concern relate to de-identified data, a registered political party, government body, or business with under 3 million a year in revenue? If so, then it may fall outside of the scope.

The APPs apply strictly to only personal information which is defined by Part 2, Division 1, section 6 of the 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.

Division 2 Section 16 of the act excludes any personal, family or household affairs, similar is section 7B(1) which exempts individuals acting in a non-business capacity.

Section 6D (1) explains A business qualifies as a small business if its turnover in the previous financial year did not exceed this amount, or, in the case of a new business, if its turnover in the current year is $3 million or less.

However, under section 6EA Small business operators can choose to be treated as organisations and opt in to the APPs. They may choose to be considered an organisation under 6EA(2) through writing to the information commissioner. State instruments may also opt to be considered an organisation and fall into scope of the APPs under s6FA.

Section 7B (2) exempts organisations that are acting under commonwealth contracts. For example, if a small accounting firm is hired by the department of defence it must follow the APPs while working under that contract, however if the firm does not have 3 million in annual revenue excluding the contract it does not have to comply with the APPs.

Section 7B(3) exempts actions relating to employee records as defined by: a practice engaged in, by an organisation that is or was an employer of an individual, if the act or practice is directly related to:

a. a current or former employment relationship between the employer and the individual; and
b. an employee record held by the organisation and relating to the individual.

Section 7B (4) exempts journalistic actions on the condition that the act occurred within the course of journalism as long as they have promised the public that they follow certain privacy standards (rules they've written down and shared).

Actions taken by organisations while acting under a state contract are exempt under section 7B(5), provided the purpose of the action is to meet an obligation under the contract.

Under Section 7C political acts and practices are exempt. This is a broad section and encompasses members of parliament (section 7C(1)) and volunteers for registered political parties (section 7C(4)).

Section 7C(2) exempts Contractors for political representatives while Section 7C(3) exempts subcontractors.

The Australian Privacy Principles

The 13 Australian Privacy Principles (APPs) are found in Schedule 1 of the Privacy Act 1988.
See detailed guidance on how the APPs are to be applied here.

APP 1 Open and transparent management of personal information

Establishes the obligation of APP entities to have a free and accessible APP adherent privacy policy available (Schedule 1, Part 1, sections 1.3-1.6). What the privacy policy must address is outlined in Schedule 1, Part 1, section 1.4.

APP 2 Anonymity and pseudonymity

APP entities must provide users with the option of anonymity and pseudonymity unless impractical or the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves.

APP 3 Collection of solicited personal information

Under Schedule 1 Part 1 section 3.1 if an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

Section 3.2 states If an APP entity is an organisation, they must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities. Section 3.3 states An APP entity must not collect sensitive information about an individual unless the individual consents and one of the following applies:

- If the entity is an agency: the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.

- If the entity is an organisation: the information is reasonably necessary for one or more of the organisation's functions or activities

Section 3.4 details the exceptions whereby agencies and organisations may otherwise be permitted to collect personal or sensitive information.

Section 3.5 states An APP entity must collect personal information only by lawful and fair means. This is important and as one can argue that the means of collection was not lawful or fair.

APP 4 Dealing with unsolicited personal information

If an APP entity receives personal information that was not solicited the entity must (within a reasonable period), determine if the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

If the entity could not have collected the information and it is not publicly available they must ensure it is destroyed or de-identified. If the information could be collected under APP 3, the information is now subject to APPs 5-13 as if it had been collected under APP 3.

APP 5 Notification of the collection of personal information

An APP entity must at the earliest possible point, including in some cases after collection, alert the individual whose information is to be collected of the matters outlined in section 5.2.

APP 6 Use or disclosure of personal information

Section 6.1 states that if an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless consent is given or the secondary purpose is directly related to the primary purpose.

The standard exemptions also apply (eg. A permitted general situation or for purposes of law enforcement).

Notably, under section 6.7 This principle does not apply to the use or disclosure by an organisation of:

a. personal information for the purpose of direct marketing; or
b. government related identifiers.

APP 7 Direct marketing

Under section 7.1 If an organisation holds sensitive information about an individual, the organisation must not use or disclose the information without consent (as per section 7.4) for the purpose of direct marketing and may only use personal information if certain conditions are not present under section 7.2: (a) the organisation collected the information from the individual; and (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) the individual has not made such a request to the organisation.

These conditions are expanded upon under section 7.3

Collection and disclosure of personal information by an organisation contracted by the commonwealth with the purpose of fulfilling (indirectly or directly) a purpose of that contract (section 7.5).

Sections 7.6 establish the power of individuals to make specific requests regarding the use and disclosure of their personal information in regards to direct marketing. Section 7.7 requires that the organisation respond in a timely manner.

APP 8 Cross-border disclosure of personal information

Under section 8.1 Before an APP entity discloses personal information about an individual to an overseas recipient the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

Section 8.1 does not apply if the organisation reasonably believes the recipient of the information is subject to a law, or binding scheme, protects the information in a similar way to the APPs. Importantly the law or binding scheme must be accessible to the individual if they wish to take action.

Section 8.2 outlines situations where 8.1 does not apply including:

- (8.2(b)) If the entity informs the individual that the overseas recipient won't be bound by APP 8.1, and the person explicitly consents after being told this.
- (8.2(c)) If disclosure is legally required or authorised by Australian law or court.
- (8.2(d)) If a permitted general situation applies,a section defined by s16A.
- (8.2(e)) If the entity is a government agency and disclosure is required under an international agreement Australia is party to.
- (8.2(f)) If an agency reasonably believes disclosure is necessary for law enforcement, and the overseas recipient is a body with similar enforcement

APP 9 Adoption, use or disclosure of government related identifiers

Under section 9.1 An organisation can't adopt a government identifier (e.g. make someone's Medicare number their customer number). Unless Adoption is required or authorised by law or a court order; or regulations specifically permit it (section 9.2).

APP 10 Quality of personal information

An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

APP 11 Security of personal information

Under 11.1 If an APP entity holds personal information, it must take reasonable steps to protect it against:

- Misuse (using information improperly, outside its purpose).
- Interference (acts that hinder data availability or integrity, e.g. denial-of-service attacks).
- Loss (accidental deletion, misplaced files, or data breaches).
- Unauthorised access (hackers, or staff accessing without permission).
- Unauthorised modification (tampering, editing, or corrupting data).
- Unauthorised disclosure (leaks or breaches to outsiders). If an APP entity no longer needs personal information for a legitimate purpose:
- And it's not a Commonwealth record (which must be preserved under the Archives Act 1983).
- And no law or court order requires it to be kept. Then the entity must take reasonable steps to:
- Destroy the information, or
- De-identify it (remove identifiers so the person can't reasonably be re-identified).

APP 12 Access to personal information

Under section 12.1 If an APP entity holds personal information about someone, it must give that person access on request, however there are exceptions to this;

- (section 12.2) if FOI or other laws allow refusal, agencies can rely on that instead of APP 12.

- (section 12.3) Organisations (e.g. companies, NGOs) can refuse access in limited situations (safety risk, privacy of others, frivolous or vexatious requests, legal proceedings, negotiations, unlawful disclosure, unlawful activity or misconduct investigations, enforcement activity and commercial sensitivity)

Agencies must respond to access requests within 30 days, while organisations are required to respond within a reasonable period. Access should be provided in the manner requested by the individual if it is reasonable and practicable to do so. If access is refused in that form, the entity must take reasonable steps to provide the information in an alternative way, such as through a redacted version or an agreed intermediary.

Agencies cannot charge for requests or access but Organisations can reasonably charge for giving access (section 12.7-8)

Sections 12.9–12.10

If an entity refuses access a written notice must be provided stating reasons for refusal, complaint mechanisms available and any other prescribed matters (section 12.9 - 12.10). For commercial sensitivity refusals (12.3(j)): entity can explain the decision in general terms

APP 13 Correction of personal information

If an APP entity is satisfied that personal information is inaccurate, out of date, incomplete, irrelevant, or misleading, or the individual requests correction the entity must take reasonable steps to correct the information (section 13.1). The corrected information must then be accurate, up to date, complete, relevant, and not misleading for the purposes it is held.

Agencies must respond to such requests within 30 days and organisations must do so within a reasonable period (section 13.5). Individuals cannot be charged for making a correction request, correcting information, or attaching a statement.

If an entity corrects personal information that has been previously disclosed to another APP entity, and the individual requests notification, the entity must take reasonable steps to inform the other entity unless doing so is impracticable or unlawful (section 13.2).

Refusal to correct (13.3)

If the entity refuses to make a correction, it must provide the individual with a written notice that explains the reasons for refusal, complaint mechanisms available, and any other prescribed matters (section 13.3). Upon refusal the individual can request a statement be associated with the personal information noting its inaccuracy. The statement must be visible to users of the information (section 13.4)

Sections 36-40A - OAIC complaints

An individual (section 36(1)) or group (section 36(2)) may make a written complaint (section 36(3)) to the Commissioner about an act or practice that may be an interference with the privacy of the individual. The Commissioners staff must assist those who wish to make a complaint (section 36(4)).

When formulating a complaint:

Respondent:

The complaint must specify the respondent to the complaint (section 36(5)). If the complaint is against an agency which is an individual or body corporate then the agency is the respondent (section 36(6)(a)), whereas if the agency is an unincorporated body the principal executive (for clarification on who this is see section 38) of the agency will be the respondent (section 36(6)(b). If the subject of the complaint is the actions or practices of an organisation, the organisation will be the respondent (section 36(7)). In cases relating to Credit reporting (section 13(2)), TFNs (section 13(4)) and breaches of Part 2 of the Data matching Act or violates s135AA of the National Health Act (section 13(5)) the person or entity that engaged in the practice is to be the respondent (section 13(8)). If the complaint relates to the data sharing scheme under the Data Availability and Transparency Act 2022 the commissioner may share information regarding the case with the National Data Commissioner (section 36B(1)).

Note: Under section 40(1A) the commissioner will not investigate a complaint unless a complaint has first been filed with the respondent. There are 3 exceptions to this rule:

1. it is inappropriate for the complainant to do so;
2. or the case involves sections 20R, 20T, 21T or 21V (which are about access to, and correction of, credit reporting information etc.);
3. or a provision of the registered CR code that relates to that section.

Prior to filing a complaint, individuals should refer to section 41 to see why a complaint may not be investigated.

Representative complaints

Section 38 (1): A representative complaint may only be lodged under section 36 if:

A. The members have complaints against the same respondent
B. All complaints arise from similar or the same circumstances
C. The complaints give rise to a substantial common issue of law or fact.

Note: under section 38(3) A representative complaint may be lodged without the consent of class members.
Section 38(2): A representative complaint must:

a) describe or otherwise identify the class members; and
b) specify the nature of the complaints made on behalf of the class members; and
c) specify the nature of the relief sought; and
d) specify the questions of law or fact that are common to the complaints of the class members.

In describing or otherwise identifying the class members, it is not necessary to name them or specify how many there are.

Complaints may be conciliated (section 40A)

If a complaint is made under section 36 and the Commissioner considers it possible the complaint may be conciliated successfully then the Commissioner must attempt to conciliate the complaint. Everything said and done in the conciliation is confidential and inadmissible unless done in furtherance of the commission of a fraud or an offence, or the commission of an act that renders a person liable to a civil penalty (section 40A(5)). If there is no likelihood of conciliation being successful, the commissioner is to notify the complainant and respondent (section 40A(3)).

Upon the dismissal of a representative complaint

The Commissioner may determine a complaint is not to continue as a representative complaint (section 31A(1)). The Commissioner may only make such a determination if satisfied it is in the interests of justice to do so for any of the following reasons (section 31A(2)):

a) It would cost more to deal with the matter as a representative complaint than it would if each person in the group made their own individual complaint.
b) the representative complaint will not provide an efficient and effective means of dealing with the complaints of the class members;
c) the complaint was not brought in good faith as a representative complaint;
d) it is otherwise inappropriate that the complaints be pursued by means of a representative complaint.

(section 31A(3)) If the Commissioner makes such a determination:

a. the complaint may continue as a solo complaint
b. If you were one of the people included in the original group (a “class member”), you can apply to the Privacy Commissioner to be added as an individual complainant in the new, continued complaint.

Section 40 - Investigations

The Commissioner shall investigate an act or practice if it may be an interference with the privacy of an individual; and a complaint has been made about the matter under section 36 (section 40(1)).

The commissioner may of their own initiative investigate an act or practice if it involves APP1 and deems it desirable to be investigated (section 40(2)).

Commissioner may or must decide not to investigate etc. in certain circumstances (section 41)

if the Commissioner is satisfied that:

(a) the act or practice is not an interference with the privacy of an individual; or

(c) the complaint was made more than 12 months after the complainant became aware of the act or practice; or

(d) the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith; or

(da) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances; or

(db) the complainant has not responded, within the period specified by the Commissioner, to a request for information in relation to the complaint; or

(dc) the act or practice is being dealt with, or has been dealt with, by a recognised external dispute resolution scheme; or

(dd) the act or practice would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme; or

(e) the act or practice is the subject of an application under another Commonwealth law, or a State or Territory law, and the subject-matter of the complaint has been, or is being, dealt with adequately under that law; or

(f) another Commonwealth law, or a State or Territory law, provides a more appropriate remedy for the act or practice that is the subject of the complaint.

(1A) The Commissioner must not investigate, or investigate further a withdrawn complaint

(2) The Commissioner may decide not to investigate, or not to investigate further, a complaint where

(a) the respondent has dealt, or is dealing, adequately with the complaint; or

(b) the respondent has not yet had an adequate opportunity to deal with the complaint.

(3) The Commissioner may defer the investigation or further investigation of a complaint if:
(a) an application has been made by the respondent for a determination under section 72 in relation to the act or practice; and

(b) the Commissioner is satisfied that the interests of persons affected by the act or practice would not be unreasonably prejudiced if the investigation or further investigation were deferred until the application had been disposed of.

If a complaint is dismissed, refer to this list to ensure that the reasoning is compliant with the legislation.

Interested party may request a hearing

The complainant or respondent may, in writing, request that the Commissioner hold a hearing before a determination under section 52 is made in relation to the investigation. If such a request is made the Commissioner must: notify any other interested party of the request; and give all interested parties a reasonable opportunity to make a submission about the request; and decide whether or not to hold a hearing (section 43A).

Section 44 – Power to obtain information and documents.

The Commissioner can compel production of documents, information, or attendance.

When to use: prepare for compulsory disclosure and challenges on scope or confidentiality. Also provides leverage to request evidence from the other side.

Section 45 – Power to examine witnesses.

Witnesses can be examined under oath or affirmation.

When to use: Prepare clients for sworn examination and may advise on rights and obligations when providing testimony.

Section 46 & section 47 – Compulsory conferences.

The Commissioner can direct complainants, respondents, and relevant third parties to attend a conference (section 46) and regulate its conduct (section 47). Failure to attend without a reasonable excuse is an offence (including for corporations).

When to use: Representation may be requested for compulsory conferences, negotiating outcomes, and advice on risks of non-attendance or disclosure.

Section 48 - Notification duties.

The commissioner must inform complainants and respondents of decisions not to investigate (or to stop investigating) and give reasons.

When to use: Lawyers can use these notices to determine grounds for judicial review if an investigation is wrongly discontinued.

Conditions to cause an investigation to cease

Section 49 – Investigation to cease if offences may have been committed.

If the Commissioner thinks the conduct could amount to a criminal offence (tax file number, healthcare identifiers, AML/CTF, or credit reporting offences), the OAIC must stop investigating and refer the matter to police or the DPP (section 49(1)). If the DPP or police decide the case will not be subject to proceedings they may express this in writing to the information commissioner and the investigation under s40(1) may resume (section49(3)).

When to use: Counsel may need to prepare the client for potential criminal exposure (if respondent) or cooperate with a police/DPP investigation (if complainant).

Section 49A – Investigation to cease if PPSA civil penalty may have been contravened.

If the conduct appears to breach the Personal Property Securities Act 2009 (e.g., unlawful database searches), the Commissioner must stop and refer the matter to the PPS Registrar.

When to use: Important in cases involving misuse of credit, financial, or property records

Section 49B – Transfer of complaints from IGIS.

If the Inspector-General of Intelligence and Security (IGIS) transfers a complaint to OAIC, it is taken as though it had been lodged directly with OAIC.

When to use: Establishes jurisdiction for privacy litigation where security and intelligence agencies are involved. May affect which secrecy laws and evidentiary limits apply.

Section 50 – Reference of matters to other authorities.
OAIC can transfer a complaint to another body (e.g. AHRC, Ombudsman, eSafety Commissioner, external dispute resolution scheme) if it would be better dealt with there.

When to use: Raises issues of jurisdictional overlap and may give scope to challenge or judicially review a transfer decision.

Section 50A – Substitution of respondent.

If the respondent organisation ceases to exist (bankruptcy, insolvency), OAIC can substitute the contracting Commonwealth agency as the respondent.

When to use: Ensures complainants are not left without a respondent.

Section 51 – Effect of Auditor-General investigation.

If the Auditor-General is already investigating, the OAIC must pause its investigation unless both agree otherwise.

When to use: Delays proceedings, which may impact strategy, settlement negotiations, or limitation periods.

Determinations of the Commissioner

Section 52 – Determination of the Commissioner.

This is the core remedial section. After investigating a complaint, the OAIC can dismiss the complaint (section 52(1)(a)), or if it's substantiated, order remedies such as:

- Declarations that the respondent must stop or not repeat conduct (section 52(1)(ia)).
- Declarations requiring steps to be taken to prevent recurrence (section 52(1A)(b)). Compensation for loss or damage, including for humiliation or injury to feelings (section 52(1AB)).
- Publication of corrective statements (section 52A).
- A determination may include any order the Commissioner considers necessary or appropriate (section 52(3A)).

Importantly: A determination of the Commissioner under section 52(1) or 52(1A) is not binding or conclusive between any of the parties to the determination (section 52(1B)).

When to use: This is the section you would rely on to argue for compensation, systemic fixes, or reputational remedies.

Section 52A – Requirement to notify and publish.

If the Commissioner orders a declaration requiring notification, the organisation must prepare and publish a statement about the conduct and corrective steps within 14 days. The entity must give the Commissioner evidence that the actions required by

the determination were taken in accordance with this section and the declaration.

When to use: Important for clients concerned with reputation (either corporate clients resisting publication, or complainants wanting acknowledgement and transparency).

Section 53B – Substituting an agency for a provider.

If a contracted service provider goes bankrupt, dissolves, or becomes insolvent, the OAIC can substitute the Commonwealth agency as the respondent for compensation orders.

When to use: Protects complainants by ensuring there's still a solvent respondent to pay compensation. For government lawyers, it flags potential exposure when providers fail.

Division 3—Enforcement of determinations

Section 54 - Application of Division

Clarifies that this enforcement division applies to determinations against organisations and small businesses, not agencies.

Section 55 – Obligations of organisations and small business operators

Outlines what respondents must do once a determination is made; stop the conduct (section 55(a)), take corrective steps (section 55(b)), pay compensation (section 55(c)), publish statements (section 55(d)). The section is a checklist of what the respondent can be held to.

Section 55A – Enforcement in Federal Court or Federal Circuit and Family Court

This is the key enforcement mechanism of determinations. It allows either the complainant or the Commissioner to take the matter to court to enforce a determination. The court hears the matter de novo (afresh) but can use OAIC materials as evidence. The court can order remedies, including injunctions and declarations, and no undertaking as to damages is required for interim injunctions. Under section 55B The OAIC can issue a certificate of facts from its investigation, which serves as prima facie evidence in court proceedings under section 55A.

Section 13G - Civil penalty provision for serious interference with privacy of an individual

An entity contravenes section 13G 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.

If the court is satisfied that paragraph (a) is met but not paragraph (b) the court may make a pecuniary penalty order against the entity for contravening section 13H, instead of section 13G.

Section 13G(1B) – Factors to be taken into consideration regarding the seriousness of the privacy invasion

a) the kind of information involved in the interference with privacy;
b) the sensitivity of the personal information;
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.

When to use: Before referring a privacy matter to the OAIC for investigation, consider which aggravating factors are present. Cross reference with the factors listed or the statutory tort of privacy, as that may be a better avenue for redress.

Section 13G(2) – Maximum pecuniary penalty

The penalty for breaching section 13G(1) by a person other than a body corporate is an amount not more than $2,500,000. If a body corporate breaches section 13G(1) the penalty should not exceed $50,000,000. If the body corporate profited from the breach of privacy, the profit is to be calculated and tripled to determine the penalty. If the profit attributable to the privacy breach cannot be determined, 30% of the adjusted turnover (for the meaning and math of this, refer to section 13G(5)) of the body corporate during the breach period (see definition in section 13G(7)) will be the penalty.

Section 13K – Civil penalty provision for breaching Australian Privacy Principles

If an entity breaches an APP the amount of the penalty payable must not exceed 200 penalty units (section 13K(1) and (4)).

Section 13K – Civil penalty provision for non-compliant eligible data breach statement

An entity contravenes this subsection if (section 13k(2)):

a) the entity prepares a statement under section 26WK (eligible data breaches); and
b) the statement does not comply with subsection 26WK(3).

The penalty payable by the breaching entity must not exceed 200 penalty units (section 13K(4)).

Statutory Tort for the Invasion of Privacy, Schedule 2 of the Privacy Act

What must the plaintiff prove to have cause of action? (Schedule 2, Part 2, section 7)

a) The defendant intruded upon their seclusion or misused personal information;
b) It was reasonable to expect privacy in the circumstances. Section 7(5) lists factors that can be considered by the court when determining this:

a) By what mechanism was the privacy invaded?
b) What was the purpose of the invasion of privacy?
c) Plaintiff characteristics such as age and cultural background.
d) The plaintiff's conduct, 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:

- The nature of the information, including whether the information related to intimate or family matters, health or medical matters or financial matters;
- How the information was held or communicated by the plaintiff;
- Whether and to what extent the information was already in the public domain.

c) The invasion was intentional or reckless; d) The invasion was serious. Section 7(6) lists factors the court will consider when deciding the seriousness of the breach;

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.

e) The public interest in privacy outweighed the public interest in disclosure. Section 7(3) provides examples of countervailing public interest;

a) freedom of expression, including political communication and artistic xpression;
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.

Note: A breach is actionable even without proof of damages.

What defenses to cause action exist? - Schedule 2, Part 2, section 8

• lawful authority (section 8(1)(a))
• Expressed or Implied consent (section 8(1)(b))
• the invasion of privacy was necessary to lessen or prevent a serious risk to life, health or safety (section 8(1)(c))
• The invasion of privacy occurred incidentally during a proportionate and necessary exercise of the right to defend a person or property. (section 8(1)(d)(i) and (ii))

Section 8(2) – The Privacy act connects with defamation law here as defamation defences can be "carried over" into privacy law.

If someone sues for invasion of privacy because their personal information was published and the same publication could also have been the basis for a defamation claim, then the defendant can rely on the defamation defences available under Australian law.

3 conditions must be present to utilise this section:

(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.

Section 8(3) – Related defences.

(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.

Exemptions

Section 15 – Journalists etc.

(section 15(1)) The tort does not apply to the following:

(a) a journalist (see section 15(2) for definition);
(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.

To the extent that the invasion of privacy involves the collection, preparation for publication or publication of journalistic material (see section 15(3) for definition).

NOTE: The definition of both journalist and journalistic material are quite broad. Under section 15(4) the journalists do not have to abide by the code of practice they are subject to, they just have to be subject to it.

Section 16 – Agencies and State and Territory authorities (other than intelligence agencies and law enforcement bodies).

The tort does not apply to an invasion of an individual's privacy by an agency or a State or Territory authority to the extent that the invasion occurs 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.

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

A staff member of a government agency or a State/Territory authority (except for staff of intelligence agencies or law enforcement bodies) invades someone's privacy in good faith while carrying out (or claiming to carry out):
(a) The official functions of the agency or authority, or
(b) The official powers of the agency or authority.

Section 16B – Law enforcement bodies.

The tort does not apply to:

(a) an invasion of privacy by a law enforcement body; or
(b) an invasion of privacy by a staff member of a law enforcement body in the performance of the person's duties, powers or functions; 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.

Section 17 – Intelligence agencies.

The tort 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.

Section 18 – Persons under 18.

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

Section 20 – Privacy for deceased persons.

Privacy rights end with the person's life. You can't sue over someone else's privacy being breached after they've died, and you can't continue suing someone who has died for a past invasion of privacy. But if a case gets cut short for this reason, the court can still sort out who pays the lawyers' bills.

Statutory limitations

If the plaintiff was under 18 years of age when the invasion of privacy occurred proceedings must commence before the plaintiff's 21st birthday (section 14(1)(a)).

Adults must commence proceedings—before the earlier of:

- 1 year from when they became aware of the invasion (14(1)(b)(i)).
- 3 years after the invasion of privacy occurred (14(1)(b)(ii)).

However, the plaintiff may apply for an order that allows them more time to bring the case (section 14(2)) in circumstances where it wasn't reasonable in the circumstances for the plaintiff to bring the case earlier (e.g. they lacked capacity) (section 14(3)). There is an absolute cap that the proceedings cannot be bought after 6 years since the privacy breach (section 14(4)).

Outcomes

Section 9 - Injunctions.

The court may, at any stage of the proceedings, grant an injunction restraining the defendant from invading the plaintiff's privacy. If the invasion of privacy involves

publishing information relating to the plaintiff the court must consider the public interest in publication of such material.

Section 10 - Summary judgments.

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.

Section 11 - Damages.

The court may award damages to the plaintiff.

The court may award:

- Damages for emotional distress (section 11(3))
- Exemplary damages in exceptional circumstances (section 11(4))
- Punitive damages in exceptional circumstances (section 11(4)) The court must not award
- Aggravated damages (section 11(2))

(section 11(5)) The sum of any damages awarded for non-economic loss and 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.

Section 11(6) – When determining the amount of damages, the court may consider the following:

a) whether the defendant apologised to the plaintiff (see note);
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.

NOTE: An apology made by or on behalf of the defendant in connection with the invasion of privacy does not express an admission of fault or liability and is not relevant to the determination of fault or liability (section 13).

Section 12 - Other remedies

The court may grant such remedies, in addition to or instead of damages awarded in accordance with clause 11. 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.