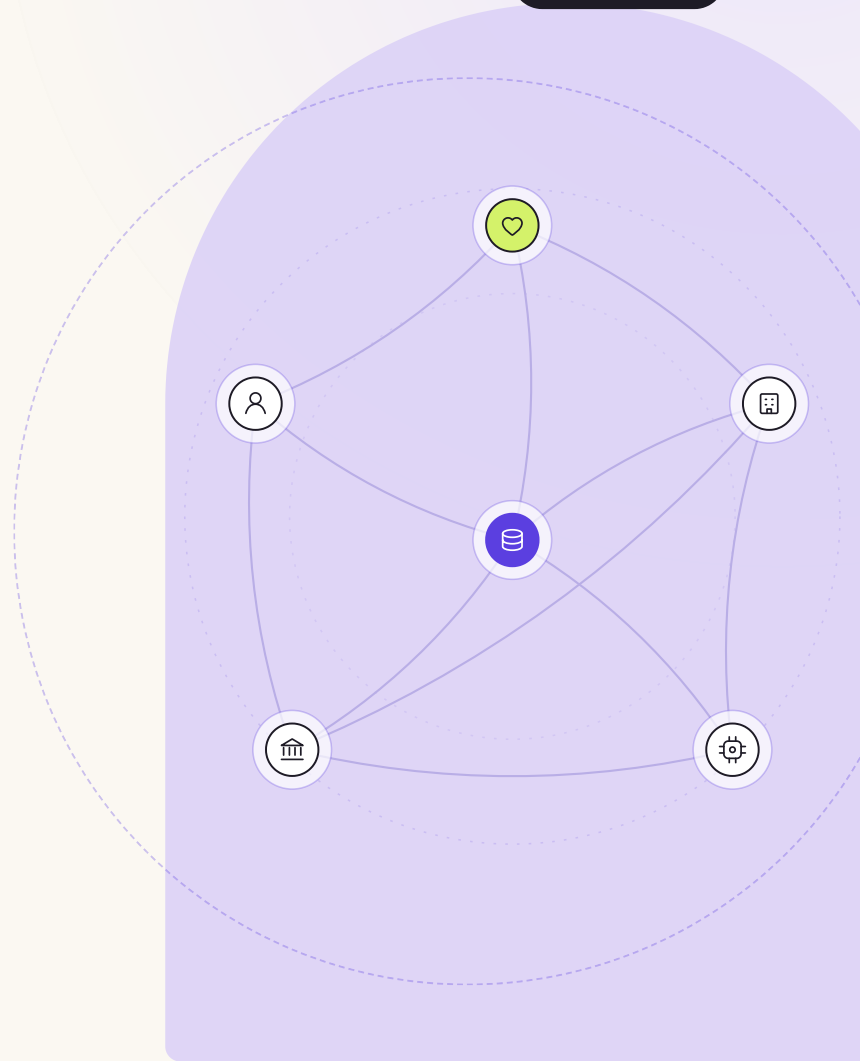




● EXPLAINER · PRIVACY & DATA PROTECTION

The statutory privacy tort, explained

A plain-English guide to Australia's statutory tort for serious invasions of privacy. It covers what must be shown, the defences and exemptions, the remedies, and where organisations are exposed.

Since **10 June 2025**, individuals in Australia have been able to sue for a serious invasion of their privacy. The cause of action was inserted as Schedule 2 of the Privacy Act 1988 by the Privacy and Other Legislation Amendment Act 2024.

The tort is separate from the Australian Privacy Principles (APPs). It is brought in the courts by the individual, not enforced by the OAIC, although the Information Commissioner may intervene or assist the court with leave. The OAIC notes that the tort reaches further than the rest of the Privacy Act: a defendant does not need to be an APP entity, so it can apply to businesses and individuals that the APPs do not cover.

What a plaintiff must show

An individual has a cause of action if all five elements are met.

1. **An invasion of privacy.** The defendant either intruded upon the plaintiff's seclusion (for example, physically intruding into their private space, or watching, listening to or recording their private activities), or misused information relating to them (including collecting, using or disclosing it).
2. **A reasonable expectation of privacy.** A person in the plaintiff's position would have had a reasonable expectation of privacy in all the circumstances. The court can consider the means used, the purpose, the plaintiff's age, occupation or cultural background, their conduct, and the nature of the information, such as whether it concerned intimate, family, health or financial matters.
3. **Intention or recklessness.** The invasion was intentional or reckless. Negligence alone is not enough.
4. **Seriousness.** The invasion was serious. Relevant matters include the degree of offence, distress or harm to dignity likely to be caused to a person of ordinary sensibilities, whether the defendant knew or ought to have known this, and any malice.
5. **The public interest balance.** The public interest in the plaintiff's privacy outweighed any countervailing public interest, such as freedom of expression, freedom of the media, open justice, public health and safety, national security, or the prevention and detection of crime and fraud.

The plaintiff does not need to prove financial loss or other damage. Where information is misused, it does not matter whether the information was true.

Defences

It is a defence if the invasion was:

- required or authorised by an Australian law or a court or tribunal order
- consented to, expressly or impliedly, by the plaintiff or someone with lawful authority for them

- reasonably believed by the defendant to be necessary to prevent or lessen a serious threat to someone's life, health or safety
- incidental to a lawful defence of persons or property, and proportionate, necessary and reasonable.

Where the invasion involved publication, certain defamation-style defences may also be available: absolute privilege, publication of public documents, and fair report of proceedings of public concern.

Exemptions

The tort does not apply to:

- journalists, their employers and those assisting them, to the extent the invasion involves collecting, preparing or publishing journalistic material
- intelligence agencies and law enforcement bodies, and disclosures to or information from them
- Commonwealth agencies and state and territory authorities (and their staff) acting in good faith in performing their functions or exercising their powers
- people under 18 years of age.

Remedies and time limits

Remedy	Key points
Damages	Including for emotional distress. No aggravated damages. Exemplary or punitive damages only in exceptional circumstances. Damages for non-economic loss plus any exemplary damages are capped at the greater of \$478,550 and the maximum for non-economic loss in defamation proceedings.
Other orders	Account of profits, injunction, apology, correction order, destruction or delivery up of material, and a declaration of serious invasion.

In setting damages the court may consider whether the defendant apologised, published a correction or tried to settle, and whether its conduct after the invasion added to the harm. An apology is not an admission of liability.

Proceedings must generally start within one year of the plaintiff becoming aware of the invasion and no later than three years after it occurred. If the plaintiff was under 18 at the time, the deadline is their 21st birthday. A court may extend time in limited circumstances, but not beyond six years.

Where organisations are exposed

The tort applies to organisations as well as individuals. Points worth reviewing include:

- **Surveillance and monitoring.** CCTV, call recording, workplace and device monitoring, and any monitoring in places people would expect to be private.
- **Deliberate data uses.** Using or sharing personal information in ways people would not expect, particularly sensitive, health, family or financial information.
- **Staff conduct.** Employees accessing or sharing records without a work reason. Clear access controls, logging and consequences matter.
- **Recklessness.** Knowing a risk to privacy exists and proceeding anyway. Documented decisions and impact assessments help show how risks were considered.
- **Response to complaints.** How quickly material is taken down and whether an apology is offered can affect the outcome.

The tort sits alongside, not instead of, your obligations under the APPs and any state or territory laws.

Next step

Understanding the tort is a first step; reducing exposure means looking at how personal information is actually handled across the organisation. Lexora's Privacy Governance Framework helps set the accountability and decision-making structures that support that work.

General information, not legal advice. If you are dealing with a potential claim, contact your legal adviser.

Sources

1. Privacy and Other Legislation Amendment Act 2024 (Cth), Schedule 2
<https://www.legislation.gov.au/C2024A00128/asmade/text>
2. OAIC, Statutory tort for serious invasions of privacy
<https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.