Article Information

Authors: Craig Subocz, JD Hohmann
Service: Cyber Security, Dispute Resolution & Litigation, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Privacy and cyber security law reforms are live: What you need to do to prepare

In late 2024, Parliament passed the Government's first round of reforms to the *Privacy Act*. After receiving royal assent in December 2024, significant changes to the *Privacy Act* take effect on 10 June 2025, while the mandatory ransomware reporting regime commenced on 29 May 2025. Now is the time to prepare.

After being introduced into Parliament in September 2024, the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**) was passed by Parliament on 29 November 2024 and received royal assent on 10 December 2024. This represents the first tranche of reforms to Australia's privacy laws promised in the previous term of Parliament by the Government.

Similarly, Parliament passed the *Cyber Security Act 2024* (Cth) in late 2024, mandating an obligation on entities with an annual turnover exceeding $3 million to notify the Commonwealth Government of ransomware payments. The *Cyber Security Act 2024* (Cth) received Royal Assent on 29 November 2024, and the mandatory regime took effect six months later on 29 May 2025.

Many of the amendments made to the *Privacy Act* took effect from the date of royal assent, while the remainder took effect six months from the date of royal assent (10 June 2025).

Mandatory ransomware reporting obligations

With effect from 29 May 2025, entities with an annual turnover of $3 million or more must report a payment to an "extorting entity" that seeks to benefit from a cyber security incident affecting the entity.

Under the *Cyber Security Act*, an entity that makes payment to an extorting entity must give the Australian Signals Directorate a report that complies with the statutory requirements within 72 hours of making the payment or becoming aware that the payment has been made. Where a third party (for example, an insurer) makes the payment on behalf of the reporting entity to the extorting entity, then the details of the third party must also be provided to the Government.

Not notifying the Government of a ransomware payment attracts a fine.

Reforms to Australia's privacy laws

Several reforms to Australia's privacy laws are now in effect. These include specific obligations in relation to the protection of personal information under Australian Privacy Principle 11 (**APP 11**), and the new statutory tort of serious invasion of privacy.

Reasonable steps to protect personal information

APP 11 requires APP entities to take "reasonable steps" to protect the security of personal information. Following the reforms implemented by the *POLA Act*, these reasonable steps specifically include "technical and organisational measures".

The nature of these technical and organisational measures will depend on the context of the information collected and the organisation holding that information. Technical measures could include encryption of sensitive information, and the

implementation of multi-factor authentication techniques to minimise the risk of unauthorised persons gaining access to an organisation's IT system.

Secondly, organisations may need to invest in staff training in relation to privacy and data security requirements of the organisation, enacting access privileges to limit access to only those employees with a specific need to access personal information, and ensuring that the accounts of former employees and contractors with access to the information are disabled or deactivated.

Statutory tort of serious invasion of privacy

The tort of serious invasion of privacy commenced on 10 June 2025. It provides individuals with a direct right of action for "serious invasions of privacy". It applies to all individuals or organisations, including private citizens, government agencies, and all businesses, regardless of their annual turnover. Therefore, businesses that are currently not bound by the *Privacy Act* may still be liable for a serious invasion of privacy.

The key elements of the tort

A plaintiff must establish five key elements:

1. The defendant must have invaded the plaintiff's privacy by intruding on the plaintiff's seclusion or through a misuse of the plaintiff's private information.
2. A person in the plaintiff's position would reasonably expect privacy in the relevant circumstances. As an objective test, courts will be able to consider factors including the plaintiff's conduct, the nature of the information, how the information was held and the extent to which the information was already in the public domain.
3. The invasion must be caused by the defendant's intentional or reckless conduct. Negligence is insufficient to establish the claim.
4. The invasion of privacy must be serious, taking into account the level of distress likely to be caused to the plaintiff, whether the defendant knew (or ought to have known) that the invasion was likely to offend, distress or harm the plaintiff's dignity, and whether the defendant acted maliciously.
5. The public interest in the plaintiff's privacy outweighs the countervailing public interest in freedom of expression, freedom of the media, the proper administration of government, open justice, public health and safety, national security or the prevention and detection of crime.

"Intrusion on seclusion" includes a physical intrusion, as well as watching, listening to or recording the plaintiff's private activities.

Misusing private information includes the unauthorised collection, use or disclosure of personal information. Accordingly, businesses should critically review their processes for the collection of personal information, to minimise the risk that an individual claims that the collection of personal information about that individual seriously invades their privacy.

Further, businesses should implement access controls to limit the ability of individual employees to access personal information of individuals held by the business in order to minimise the risk of employees inappropriately accessing or misusing personal information about individuals.

Defences

Certain defences are available, including a reasonable belief that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person, as well as the plaintiff's consent to the invasion of privacy.

In limited circumstances, defences available under defamation law are also available to the defendant for the alleged invasion of privacy. Journalists are exempt to the extent that the invasion of privacy involves the collection, preparation for publication or publication of journalistic material.

Time periods

Plaintiffs have only a short window in which to bring an action for a serious invasion of privacy. Proceedings must be commenced the earlier of one year after the day on which the plaintiff became aware of the alleged invasion of privacy, or three years after the invasion of privacy occurred. If the plaintiff's privacy was invaded before the plaintiff turned 18 years old, the plaintiff will have until they turns 21 to commence proceedings.

Available remedies

If the plaintiff successfully establishes that their privacy was seriously invaded, then the Court may award remedies from a wide range. The plaintiff may be entitled to damages (including for emotional damage, as well as exemplary or punitive

damages where the defendant's conduct demonstrates a "flagrant disregard" for the plaintiff's privacy rights). The court may issue an injunction restraining the ongoing or imminent invasion of the plaintiff's privacy.

Courts also have the power to grant non-financial remedies to serve corrective or restorative purposes. These remedies include an account of profits to require the defendant to surrender gains derived from the invasion of privacy, orders for apologies, correction orders and orders for the destruction or delivery up of material. Courts also have the power to issue declarations affirming that a serious invasion of privacy occurred.

Conclusion

The recent reforms to Australia's privacy laws, together with the introduction of mandatory reporting for ransomware payments, illustrate the need for businesses to be vigilant on both external and internal threats to the security of information they collect and hold.

Businesses should assess whether their technical and organisational measures to protect the privacy of personal information they hold are adequate, having regard to the sensitivity of the information they hold, and the potential adverse consequences to individuals if the security is penetrated.

This will include (but may not be limited to) reviewing and implementing training for all staff and contractors with access to personal information on the importance of protecting the security of personal information.

Given that a serious invasion of privacy might arise from an employee's inappropriate access to and use of personal information held by the employer, all businesses (regardless of their size) should critically review and update their internal policies and practices on access to personal and sensitive information.