Baker McKenzie.

Legal Update

December 2024

Australia: Tranche 1 of New Privacy Laws commence

In brief

The Privacy and Other Legislation Amendment Act 2024 (Cth) ("**Act**") received Royal Assent on 10 December 2024.

These changes have been referred to as the "Tranche 1" of amendments to Australia's privacy laws, with the majority of the changes taking effect on 11 December 2024.

In this issue

Key takeaways and next steps

The Tranche 1 amendments have introduced:

- A new tort for serious invasion of privacy
- "Doxxing" offences into the Criminal Code Act 1995 (Cth) ("**Criminal Code**")
- New penalties and enforcement powers
- The structure to establish a children's online privacy code (and other updates on code making powers)
- Requirements to include in privacy policies information about using personal information for automated decision making
- Other updates to the Australian Privacy Principles (APPs).

The Tranche 1 amendments have come more than two years after the Attorney-General Department's report ("**Review**") proposed 116 recommendations to reform the Privacy Act 1988 (Cth) ("**Privacy Act**"). The Government's response to the Review, in September 2023 ("**Response**"), "agreed" 38 proposals to be implemented first and these new laws address 23 of those proposals. Tranche 1 amendments set the foundations for later changes.

The new laws also include a small number of amendments made to the initial Bill introduced into Parliament, including (notably) changes to the statutory tort for serious invasion of privacy and the granting to the Office of the Australian Information Commissioner (OAIC) powers to issue compliance notices.

Alongside the new laws, the Privacy Commissioner has been active in issuing guidance on matters such as artificial intelligence, as well as decisions on the use of facial recognition technology and data scraping, which we provide further detail on below.

Despite speculation that the Government might be more ambitious with this initial tranche of amending legislation, the Tranche 1 amendments do not encompass the kind of comprehensive legislative shift that was initially anticipated following the Review.

Significant reforms in the new laws include:

- For regulated entities that use personal information in automated decision-making (ADM), there will be an additional notification obligation if the resulting decisions would reasonably be expected to significantly affect the rights or interests of the relevant individual.
- A framework for the introduction of a Children's Online Privacy Code (the content of which is to be developed following commencement of the new laws).

- Increased regulator enforcement powers, along with a new statutory tort for serious invasions of privacy under the Privacy Act and a new offence of "doxxing" under the Criminal Code.

Most of the Tranche 1 amendments come into effect on 11 December 2024. However, some are subject to deferred commencement, notably:

- The statutory tort for serious invasions of privacy will commence on a date to be Proclaimed, but within six months of 10 December 2024.
- The provisions relating to automated decision making will commence two years after 10 December 2024.

Reform	Commencement
Anti-doxxing offences	11 December 2024
New tiered penalties and infringement notices	10 December 2024
Enhanced regulator powers including search and seizure	11 December 2024
Uplifts to cyber security, reasonable security steps including technical and organizational measures	11 December 2024
Information sharing emergency declarations	11 December 2024
Statutory tort for serious invasion of privacy	The earlier to occur of Proclamation or at the expiry of 6 months from 10 December 2024
Transparency of automated decisions	24 months from 10 December 2024
New code-making powers and the development of a Children's Online Safety Code	Code Making Powers: 11 December 2024 Code to be developed: 24 months following 11 December 2024

While the Tranche 1 amendments include some significant reforms, many of the "agreed in-principle" proposals from the Response have not been dealt with in Tranche 1 and are expected to be addressed in future "Tranche 2" amendments.

There are also a number of actions that remain outstanding to implement the proposals "agreed" in the Response as addressed in the Tranche 1 amendments. In particular:

- The OAIC has indicated it will issue new guidance relevant to the first tranche of reforms agreed in the Response, much of which will support amendments included in the Act. This includes guidance on:
    - Treatment of new technologies
    - Factors that make an individual "vulnerable" to higher risk of harms from interference with personal information
    - Capacity and consent
    - The requirements for destruction and de-identification of personal information
    - What "reasonable steps" are to secure personal information
    - What types of decisions would be captured by the new ADM requirements.

We also expect further consultation in relation to:

- A potential criminal offence of malicious re-identification of de-identified information

- Enhanced risk assessment for facial recognition technologies and other uses of biometric information
- The "Australian Link" requirement
- Allowing a broad consent for research.

The Attorney-General stated in September 2024 that the Attorney-General's Department intended to prepare draft Tranche 2 legislation for consultation, likely to occur in 2025. However, the upcoming Federal election is a key factor that may affect this timeline and it is unclear whether any further legislative reforms will be introduced before the Federal election.

In more detail

What should regulated entities be aware of?

The new laws include a number of changes relevant to all regulated entities, These include changes in relation to:

- Enforcement and investigation powers and increased penalties
- The obligation to disclose in privacy policies any use of automated decision making that would significantly affect an individual's rights or interests
- Changes to management of personal information, including the standard of "protection" for personal information held by regulated entities and more specific requirements regarding overseas data flows.

1. *Enforcement and investigation powers, and increased penalties*

   Some of the key amendments intended to strengthen the powers of the OAIC include:

   - **New infringement notices and civil penalties apply for privacy breaches that are not 'serious' or 'repeated'** (which was the threshold for the imposition of civil penalties under the prior law). Regulated entities need to be aware that there is now a long list of Privacy Act breaches that could trigger an infringement notice or civil penalty. For example, sections 13K(1) and (2) of the Privacy Act impose civil penalties for breaching the requirement to have an APP privacy policy in place (APP 1.3) or to include the required contents of an APP privacy policy (APP 1.4)). Consequently, if (for example) a regulated entity fails to disclose in its privacy policy that automated decision-making is applied, it may be subject to a civil penalty.
   - **The Commissioner will be empowered to conduct public inquiries** into matters relating to privacy, on the direction or approval of the Attorney-General (in respect of systemic or industry-wide issues).
   - A **compliance notice regime** has been added by Senate amendments to the Bill. This allows the OAIC to give a regulated entity a notice if the OAIC reasonably believes that the entity has contravened certain APPs Failure to comply with a compliance notice may result in the imposition of a civil penalty. However, an entity that complies with the notice is not taken to have admitted to, or engaged in, the relevant contravention. If an entity fails to comply with a notice, the OAIC may issue an infringement notice or seek a civil penalty order.

2. *Automated decision making*

   From 10 December 2026, regulated entities will be required to specify in their privacy policies the kinds of personal information used in, and types of decisions made by, computer programs that use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual.

   Such decisions could include:

   - A decision to grant or refuse a benefit, such as admission to a country or an entitlement to a housing benefit
   - A decision that affects an individual's rights under a contract, agreement or arrangement, such as a contract for a life insurance policy
   - A decision that affects an individual's access to a significant service or support, such as access to healthcare.

   This reform is broadly in line with the Voluntary AI Safety Standard and the draft Mandatory Guardrails for AI in High-Risk Settings.

Notably, this is a disclosure obligation only and does not prevent or otherwise regulate the use of such artificial intelligence (AI) processes. We expect to see further guidance from the OAIC on what types of decisions would be caught by these ADM notification obligations. We note the OAIC has also recently issued some guidance in respect of generative AI and the use of commercially available AI products.

3. *Management of personal information*

The new laws also change how personal information is managed by regulated entities, including:

- A requirement for the **Information Commissioner to develop and register a Children's Online Privacy Code ("COP Code")** by 11 December 2026. The purpose of the COP Code will be to detail how relevant APPs apply to children and their online privacy. The OAIC will be funded with an additional $3 million over three years for work relating to this new code.
- **An ability to whitelist in regulations countries that are deemed to have equivalent privacy protections to Australia,** enabling the transfer of personal information to such countries without restriction. This aligns Australia's position with the EU's General Data Protection Regulation and removes the requirement to assess whether a foreign privacy regime is adequate, or otherwise design contractual safeguards for the purpose of the transfer.
- Amendment of APP 11, which requires entities to take reasonable steps to keep personal information secure, and to destroy or de-identify personal information that is no longer required for a lawful business purpose, **to explicitly include "technical and organizational measures" as reasonable steps**.

Statutory tort for serious invasion of privacy

The new laws create a long-awaited cause of action in tort for serious invasions of privacy, which will commence within six months of 10 December 2024. The commencement date will be the first to occur of Proclamation for the new tort or at the expiry of six months (being 10 June 2025). The model of the statutory tort is informed by the Australian Law Reform Commission's 2014 report Serious Invasions of Privacy in the Digital Era.

Individuals will have a cause of action if they suffer an invasion of their privacy, either by an intrusion into their seclusion (e.g., being photographed without consent) or by misuse of information, when:

- A person in their position would have had a reasonable expectation of privacy in all the circumstances
- The invasion of privacy was intentional or reckless
- The invasion of privacy was serious
- The public interest in the person's privacy outweighs any countervailing public interest (such as freedom of expression or freedom of the media).

This 'public interest' element was added to the Act following amendments from the Senate Committee review. In respect of this public interest balancing element, the onus of proof lies on the person bringing the cause of action (i.e., the plaintiff is required to provide that the invasion of privacy was not in the public interest). Specific matters which may constitute a countervailing public interest, include national security, public health and safety and the prevention and detection of crime and fraud.

Importantly, the invasion of privacy tort is actionable without proof of damage, similar to defamation. This means, for example, that a person who invades the privacy of a large number of individuals could be the subject of a claim from those affected individuals without the need for those individuals to prove specific losses (e.g., financial loss).

However, it should be noted that the "intentional" or "reckless" threshold is a high one; harm caused by mere negligence would not be actionable under the statutory tort.

The tort will be subject to a range of defences (including some that align with defamation law, or where the invasion to privacy is authorised by law or consented to by the plaintiff, or reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person) and exemptions for legitimate societal activities (such as the activities of law enforcement, intelligence agencies and journalists). A court may, at any stage of proceedings, determine whether certain exemptions apply. The court can make a determination relating to these exemptions in its discretion or at the application of a party to the proceedings.

Doxxing and harassment

The new laws amend the Criminal Code and introduce targeted criminal offences to respond to "doxxing", which is the deliberate release of personal data (e.g., names, photographs, contact details) in a manner that may be menacing or harassing. In relation to these offences, "personal data" of an individual means information about the individual that enables the individual to be identified, contacted or located.

An offence is committed (and carries a maximum six year imprisonment term) where a person uses a carriage service to make available, publish or distribute personal data, in a way that reasonable persons would regard as being menacing or harassing.

The new laws also introduce an additional more serious offence (with a maximum seven year imprisonment term) in respect of a person or group targeted because of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin.

What is missing?

A number of highly anticipated reforms outlined in the Review and Response (approximately 50) are yet to be addressed and have been deferred to Tranche 2. These include the "agreed" proposals to:

- Impose thresholds on individuals seeking to rely on the "journalism exemption", by requiring that such individuals be subject to privacy standards overseen by a recognized oversight body (the ACMA, APC or IMC), or other standards that adequately deal with privacy; and
- Introduce a legislative provision that permits broad consent for the purposes of research.

A number of "agreed in principle" reforms that would have broader impact on the privacy framework in Australia have not been included in the Tranche 1 new laws. These include the introduction of an overarching "fair and reasonable" requirement for collection, use and disclosure of personal information, the removal of the small business exemption, the amendment of the employee record exemption and the introduction of a controller and processor distinction. No proposed timeline for implementation or further consultation on these reforms has been announced and the upcoming Federal election is a key factor that may affect the timing of these future reforms.

Recent enforcement activity

Finally, the focus on the new laws should not detract from the significance of recent decisions of the Privacy Commissioner, which indicate that enforcement of the Privacy Act is a priority for the Privacy Commissioner.

These decisions are instructive in understanding key areas of risk for entities in the context of fast-moving changes to privacy legislation.

Facial recognition technology

The recent Bunnings Group determination in October 2024 from a Commissioner Initiated Investigation examined the use of a facial recognition technology (FRT) system across Bunnings' stores in Victoria and New South Wales between 2018 and 2021. The system captured and stored the faces of persons who entered the stores, comparing these against images Bunnings had accumulated in a database of individuals identified as posing a risk to the business (for example, due to past criminal activity or violent behavior in and around Bunnings' stores). Where there was no match, storage was very brief.

The Privacy Commissioner found that Bunnings breached a number of APPs through its use of that FRT system, specifically Bunnings:

- Collected sensitive biometric information and criminal history information about individuals without their consent, in breach of APP 3.3
- Failed to provide adequate notification to customers entering its stores about the collection of that information, in breach of APP 5.1
- Failed to implement practices, procedures and systems to ensure that Bunnings complied with the APPs, in breach of APP 1.2(a)
- Failed to include required information in the Bunnings privacy policy, in breach of APP 1.3.

Bunnings was not able to rely on certain permitted general situations (PGS) in the Privacy Act that permit the collection of biometric information without consent in situations where:

- It is unreasonable or impracticable to obtain individual consent for collection, use or disclosure of personal information

- That collection, use or disclosure is ***necessary*** to lessen or prevent a serious threat to life, public health or safety.

The Privacy Commissioner was resolute in construction of 'necessary' as a word that greatly limited the availability of the PGS exception to general positive consent requirements. Bunnings could not have held a reasonable belief that the use of FRT to collect sensitive information was necessary under the PGS, particularly as other methods for detecting high-risk individuals in stores were available, and the mass collection of facial data on all Bunnings customers was not a reasonably proportionate measure to detect a small number of high-risk individuals. The Privacy Commissioner took particular issue with Bunnings' lack of public signage or notification to customers of the use of facial recognition technology in stores.

Bunnings has been ordered to cease use of the FRT systems and publish a statement on its website detailing the impugned collection and use of the images, as well as to provide customers with pathways for registering complaints. Bunnings has indicated it will seek a review of the determination at the Administrative Review Tribunal.

This is potentially a highly significant test case on the scope of the APPs.

Data scraping

In a Commissioner Initiated Investigation into Master Wealth Control Pty Ltd t/a DG Institute (Privacy) and a Commissioner Initiated Investigation into Property Lovers Pty Ltd (Privacy) decided in November 2024, the companies (linked by their common directors and held to be related bodies corporate) provided training courses to members of the public with a focus on property investment. Paying participants of the companies' 'Elite Mentoring Program' were encouraged to find distressed properties in circumstances where a property owner might be incentivized to sell their property at below market value due to personal circumstances of distress/bankruptcy or a deceased estate. The respondents were found to have collected individuals' personal information contrary to the terms and conditions of the third parties' websites and databases and in circumstances where those individuals had no knowledge or awareness of the collection. Further, those individuals were in or perceived to be in vulnerable positions and could not have reasonably expected the respondent to collect their personal information.

While the companies did remove individual names from their lead lists of some prospective property owners in distressed situations for 'privacy', they continued to provide instructions and guidance to participants of the program on how to re-identify individuals later in the 'Program'.

The Privacy Commissioner found that the respondents:

- Failed to collect personal information by fair means, in breach of APP 3.5
- Failed to take reasonable steps to notify or otherwise ensure that those individuals subject to personal information collection were aware of the relevant APP 5.2 matters, in breach of APP 5.1
- Failed to take reasonable steps to ensure the personal information they used and disclosed via their lead lists was accurate, up-to-date, complete and relevant, in breach of APP 10.2.

This led to a declaration under s 52(1A)(a) of the Privacy Act that the respondents' acts and practices constituted an interference with the privacy of individuals and a declaration under s 52(1A)(b) that the respondents must immediately cease information collection, destroy all lead lists relevant to the Elite Mentoring Program and, in the case of Property Lovers Pty Ltd, publish a written apology. Master Wealth Control was also found to have breached APP 1.3 by failing to have a clear and up to date privacy policy that satisfied APP 1.4, and was ordered to promptly amend and update that policy.

These decisions reflect an increased regulatory focus on regulated entities where they collect data on individuals without their knowledge.

What is next?

The Tranche 1 amendments may not enact fundamental or sweeping changes to Australia's privacy compliance framework. However, the implementation of broader investigatory and enforcement powers increase practical enforcement risks for regulated entities and should encourage a renewed focus on privacy compliance. Specifically, we recommend regulated entities:

- Ensure their relevant teams are aware that it is now much easier for the regulator to penalize regulated entities for some areas of non-compliance such as breaches of privacy policy content requirements
- Identify and review their practices with respect to automated decision making and update privacy policies accordingly
- Continue to provide training to employees in respect of Privacy Act compliance, focusing in particular on the changes enacted by the new laws and noting the Privacy Commissioner's increasingly active approach to enforcement
- Conduct a data audit to ensure that only personal information necessary for the purposes of the business is being stored

- Review and if necessary uplift technological and organizational security measures with respect to personal information
- Review and assess any 'high-risk' data collection activities and consider whether such activities are genuinely necessary or whether steps can be taken to reduce the possibility of any potential non- compliance with the Privacy Act.

Thank you to Nina Kerwin Roman, Matt Dempsey and Lauren Lancaster for their assistance in preparing this alert.

Contact Us

Adrian Lawrence
Partner
adrian.lawrence
@bakermckenzie.com

Toby Patten
Partner
toby.patten
@bakermckenzie.com

Anne Petterd
Partner
anne.petterd
@bakermckenzie.com

Caitlin Whale
Partner
caitlin.whale
@bakermckenzie.com

Ryan Grant
Partner
ryan.grant
@bakermckenzie.com

Jarrod Bayliss-McCulloch
Special Counsel
jarrod.bayliss-mcculloch
@bakermckenzie.com

Simone Blackadder
Special Counsel
simone.blackadder
@bakermckenzie.com

Allison Manvell
Special Counsel
allison.manvell
@bakermckenzie.com