Ashurst

Australian Privacy Reforms

A generational change inches closer

12 September 2024

The first brick in the wall

The Australian Government has launched its next round of proposed privacy reforms, aimed at ensuring that **the Privacy Act is fit for purpose in the digital age**. Proposed changes will be introduced in two tranches:

Tranche 1	12 Sep 2024	**Tranche 1 legislation introduced**	→	Tranche 2	"Next few months"	Tranche 2 consultations

What reforms have been introduced?

23 of the proposals that were 'agreed' in the Government Response to the Privacy Act Review (September 2023), out of total of 116 proposals.

1. **Enhanced regulator powers** – with a new menu of investigation and enforcement options, including search and seizure powers, infringement notice powers, and tiered penalties.
2. **Automated decision-making/AI** – new transparency requirements, a first step in broader automated decision-making and AI reforms.
3. **Cybersecurity uplifts** – enhanced information security obligations, with greater information sharing rights, and tools to respond to data breaches.
4. **Code-making framework and Children's Online Privacy Code** – the first cab off the rank under a stronger code-making framework for the OAIC.
5. **Simpler international data transfers** – allowing the regulations to prescribe countries and binding schemes with 'substantially similar' privacy protections.
6. **Statutory tort** – a long-awaited right to make a claim for intentional or reckless serious invasions of privacy brings Australia closer to international regimes, and opens new avenues for litigation.
7. **Anti-doxxing** – broad criminal offences for exposing personal data in a way that is menacing or harassing, capturing the intentional and malicious exposure of personal data online.

Initial takeaways

The tranche 1 reforms involve a focus on consumer safety and social harm, establishing a flexible and agile privacy regime.

- **Focus on uplifting your practices, procedures, and systems** – to make sure that you are ready for closer scrutiny and increased enforcement.
- **The most impactful areas are about consumer safety** – the combination of a statutory privacy tort and anti-doxxing laws result in greater individual rights, providing individuals with an avenue to take direct action.
- **Wider toolbox for the regulator** – with no transition period, new regulatory tools can be brought to bear well before tranche 2 reforms take effect. Expect pro-active intervention, in addition to reactive enforcement
- **Flexible and agile regulation** – through code-making powers allows issues of social concern to be addressed quickly by a pro-active regulator.
- **Automated decision transparency is harder than you think** – there are more automated decision-making and AI laws to come, and the 24-month timeframe to comply may not be enough for many organisations.
- **Just the tip of the privacy reform iceberg** – tranche 1 reforms have direct impacts on some focused areas, but they provide a baseline for enforcing compliance with the full package of tranche 2 reforms.

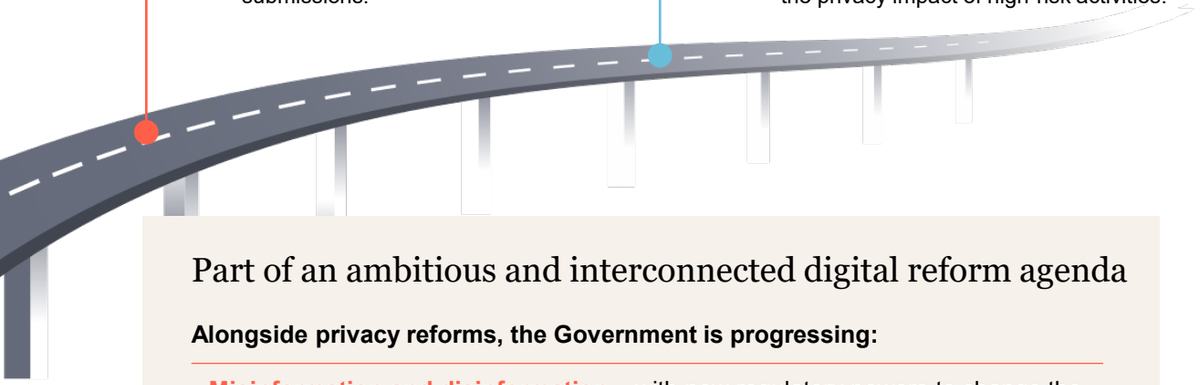
Next steps for the reform pathway:

Tranche 1 reforms are not yet law:

- *Privacy and Other Legislation Amendment Bill 2024* will be before the House again on 8 October.
- The Bill will likely be referred to Senate Committee, who will likely hold public hearings and accept submissions.

Consultation on Tranche 2:

- Consultation and draft changes expected "over the next few months".
- Broad spread of reforms – including a new "fair and reasonable" requirement, consent reforms, individual rights, small businesses and employee exemptions, and assessing the privacy impact of high-risk activities.



Part of an ambitious and interconnected digital reform agenda

Alongside privacy reforms, the Government is progressing:

Misinformation and disinformation – with new regulatory powers to change the way platforms manage these risks.

Hate crimes – expanded offences for urging, or directly threatening, violence against particular groups.

Cyber security – including ransom payment reporting and mandatory standards for digitally-connected devices.

Security of critical infrastructure reforms – including to focus on data storage systems and telecommunications.

The two things to do to reduce your risk and increase customer trust:

The proposed changes materially increase your risk by introducing a wider toolbox of regulator enforcement options and a statutory tort for serious invasions of privacy. This puts the onus on your practices, procedures and systems to provide a defensible position for collection, use, and disclosure.

Uplifting practices, procedures, and systems

1. **Current State Assessment**
   Conduct an assessment to evaluate the effectiveness of your current privacy risk management framework, including PIAs, privacy by design, third-party risk and roles and responsibilities allocation, legal obligations, and where gaps exist
2. **Gap Analysis**
   Identify the gaps between your current state and your new obligations under the reforms and where you may need to uplift your practices, procedures, and systems
3. **Uplift to new standard**
   Develop a plan to remediate any gaps between your current state and your internal and external practices, procedures, and systems to understand and manage your privacy risks

Automated decision-making

1. **Identify legal and risk obligations**
   The legal obligations contained in the Privacy Act reform and the AI Guidelines need to be understood to define the scope of work. The obligations will guide the risk scope of work to control the risk
2. **Map use cases and personal information**
   Develop a plan to identify any use cases of automated decision-making and AI in the business. A use case review should be undertaken to determine if each requires risk assessment. Personal information used and created must be mapped for each use case
3. **Monitor and Review**
   Privacy risk management is not a one-off exercise – it requires constant monitoring and review to ensure the ongoing mitigation of emerging risks and uplift to the new privacy obligations in Tranche 2 of the Privacy Act reforms and other AI guidance

Getting the foundations right will give you an advantage

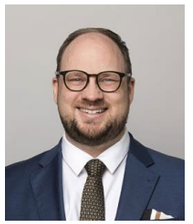
Ensuring you have the practices, procedures and systems in place and helping you outpace change

The privacy reforms mark the beginning of **significant changes in Australian privacy law**, increasing the risk for businesses in the digital economy.

Business leaders who adapt effectively to these changes by **implementing reliable and provable privacy practices, procedures, and systems** can mitigate risks and gain a competitive edge through enhanced customer trust.

Ashurst offers comprehensive support in data privacy and risk management, leveraging legal and risk advisory expertise to help clients **achieve operational resilience and compliance.**

Privacy



Geoff McGrath
Partner
Digital Economy

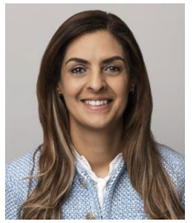
Emma Butler
Practice Group Head
Digital Economy

Chris Baker
Partner, Regulatory
Risk & Privacy
Risk Advisory

Leon Franklin
Director
Privacy
Risk Advisory

Cyber and data risk

John Macpherson
Partner
Cybersecurity
Risk Advisory



Sonia Haque-Vatcher
Partner
Data and Analytics
Risk Advisory