

Article Information

Author: Jan David Hohmann

Service: Corporate & Commercial, Cyber Security, Dispute Resolution & Litigation, Privacy & Data Protection

Sector: Financial Services, Health & Life Sciences, Infrastructure, IT & Telecommunications, Not-for-Profit, Transport & Logistics

Federal Government outlines its vision for reforming Australia's privacy law

In September 2023, the Federal Government set out its in-principle approach to reforming Australia's privacy law by releasing its response to the Privacy Act Review Report recommendations.

In February 2023, the Attorney-General's Department released its comprehensive review report into Australia's *Privacy Act 1988* (Cth), setting out 116 proposals to amend the *Privacy Act*, as discussed in our February 2023 insight.

After considering the Report and public submissions, the Government has released its response. The Government agrees to 38 proposals, and "agrees in-principle" with a further 68 proposals. The Government "noted" the remaining 10 proposals (mainly dealing with political exemptions and specific protections for de-identified information), but chose not to accept them.

The Government collated its response under five pillars.

"Bring the Privacy Act into the digital age"

This pillar focuses on issues including the definition of "personal information". The Government agrees in-principle that the concept of "personal information" should expand to include "technical and inferred information (such as IP addresses and device identifiers) if the information can be used to identify individuals" and to amend the *Privacy Act* to set out (non-exhaustive) lists to assist entities determine when information will be personal information. Further, the Government agrees in-principle that "collection" should be amended to cover information obtained from any source and by any means, including inferred or generated information.

"Entities covered by the Privacy Act"

Currently, most businesses with an annual turnover of \$3 million or less are exempt from the *Privacy Act*. The Government agrees in-principle to remove this "small business exemption". However, the exemption will not be removed until the Government has consulted further with small businesses on what obligations should be modified to "ease the regulatory burden" and what support would be required to facilitate compliance.

Records of current or former private sector employees are exempt from the *Privacy Act*. The Government agrees in-principle to consult on how privacy and workplace relations law should interact as part of its assessment of enhanced privacy protections for private sector employees.

"Uplift protections"

According to the Government, individuals must "largely self-manage" their privacy but feedback to the Review suggests that many individuals do not feel they have control over their personal information. Accordingly, the Government agrees in-principle that the collection, use and disclosure of personal information must be "fair and reasonable in the circumstances" (with the *Privacy Act* to outline factors relevant to this assessment), regardless of whether the entity obtained the individual's consent.

Currently, entities must take "reasonable steps" to protect personal information they hold. The Government agrees in-

principle that this should be enhanced by amending the *Privacy Act* to specify that “reasonable steps” include technical and organisational measures. Notably, the Government also agrees in-principle that entities must set out their own minimum and maximum retention periods for personal information they hold, with these periods to be specified in privacy policies.

The Government acknowledged that most Australians expected that entities should be better prepared to rapidly respond when a serious data breach occurs and do more to help affected individuals. The Government agrees in-principle that data breaches must be notified not later than 72 hours after the entity becomes aware. Further, entities will be required to explain the steps taken (or to be taken) in response to a breach. The Government intends to consult on whether entities must take reasonable steps to prevent or reduce the harm likely to arise as a result of the breach.

The Report outlined several proposals to increase organisational accountability for managing privacy of personal information. The Government agrees in-principle that entities should be required to determine and record the purposes for which personal information will be collected, used and disclosed at or before the time the information is collected. To improve processes and systems, the Government agrees in-principle that entities must appoint or designate a senior employee as having specific responsibility for privacy within the entity. Further, the Government agrees in-principle that entities must take reasonable steps to ensure personal information collected by third parties was collected lawfully.

To manage the risks inherent in high privacy risk activities, the Government agrees in-principle that non-government entities must conduct a privacy impact assessment for such high risk activities.

The Government agrees that entities must explain in their privacy policies the types of personal information that are used in substantially automated decisions which have a legal or similarly significant effect on an individual’s rights.

The Government agrees in-principle to increase the protection of children’s privacy, including by requiring entities to have regard to the child’s best interests as part of considering whether collecting, using or disclosing a child’s personal information is fair and reasonable in the circumstances.

“Increase clarity and simplicity for entities and individuals”

The Government agrees in-principle to define (or re-define) key terms such as “collection”, “disclosure” and “consent” to broaden the protection granted to personal information. The Government also agrees in-principle to simplify the obligations for “processors” as opposed to “controllers” of personal information. To facilitate overseas data flows, the Government agrees to introduce a mechanism to prescribe overseas countries with substantially similar privacy laws.

“Improve transparency and control”

In its response, the Government acknowledged that individuals have “limited transparency and control over their personal information” and considers that relying on consent places “an unrealistic burden on individuals”. The Government agrees in-principle to amend the *Privacy Act* to clarify that consent should be voluntary, informed, current, specific and unambiguous, and that individuals should have the ability to withdraw consent in an easily accessible manner. The Government also agrees in-principle that privacy notices should be clear, up-to-date, concise and understandable.

The Government acknowledged that Australians expect that they will have additional rights to control how their personal information is used. The Government agrees in-principle that individuals will have new individual rights, including a “right of erasure”.

Importantly, the Government agrees that individuals have limited capacity to seek redress for interferences with their privacy. The Government agrees in-principle that the *Privacy Act* should confer on individuals a direct right of action for interference with privacy (subject to the individual first filing a complaint with the Privacy Commissioner) as well as a capacity to take legal action for “serious invasion of privacy”.

“Strengthen enforcement”

The Government accepts proposals to improve the effectiveness of enforcement action. In particular, the Government agrees to amend the *Privacy Act* to introduce a new mid-tier civil penalty provision to cover interferences with privacy that do not meet the threshold of being “serious” and a low-tier civil penalty provision for specific administrative breaches of the *Act*.

The Government also agrees to amend the *Privacy Act* to broaden the scope of “serious or repeated” interferences with privacy by removing the word “repeated” and clarifying that a “serious” interference can include repeated interferences with privacy.

The Government's response to the Report indicates that the Attorney-General's Department plans to develop legislative proposals to implement the proposals which are "agreed", with further targeted consultation to follow. The Government will engage with the public on proposals which are "agreed in-principle" to assess whether (and how) those proposals can be implemented to balance privacy safeguards with other consequences and additional regulatory burden. A detailed impact analysis will be developed to determine potential compliance costs and other potential economic costs and/or benefits. The Government intends that these steps will be completed in 2024, including the outcomes of consultation and the legislative proposals of the "agreed" proposals.

Key Takeaways

- On 16 February 2023, the Report of a review of the *Privacy Act* was released by the Attorney-General, setting out 116 proposals to reform the *Privacy Act*.
- On 28 September 2023, the Government released its response to the Report.
- The Government indicated it agrees with 38 proposals, and agrees in-principle with a further 68 proposals.
- The Government has either agreed to or agreed in-principle to a broader definition of "personal information", the removal of the "small business" exemption, the introduction of specific rights for individuals (including the right to erasure), greater transparency on how personal information is used in automated decision making processes, and an obligation that the collection, use and disclosure of personal information be "fair and reasonable".
- In addition, the Government has agreed in-principle with the introduction of a statutory cause for invasion of privacy, and has agreed to the greater protection of children's privacy, as well as more timely notification of serious data breaches by affected entities.
- The Government flagged that further consultation is required before legislation is introduced into Parliament. This will give organisations and businesses the opportunity to participate in the privacy law reform process.