Making privacy core business

What's at stake? Review of the Australian Privacy Act

31 March 2022

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

What's at stake? Review of the Australian Privacy Act

The current review of the Privacy Act has been a work in progress for several years. Recent rounds of consultations saw the release of the Privacy Act Review Discussion Paper in October 2021, following on from the Issues Paper in October 2020.

The Attorney-General's Department published over 200 submissions in response covering a broad spectrum of stakeholder views. Sixty-seven proposals for change are tabled in the Discussion Paper. The top five proposed changes, in Privcore's view are outlined below.

1) Clarifying the broad nature of the definition of 'personal information'

The OAIC interprets the definition of 'personal information' broadly. However, the case of the Privacy Commissioner against Telstra in 2017 created uncertainty. Additionally, increased profiling and use of technical information to identify individuals led to calls to clarify interpretation. The OAIC has explained the history and its broad interpretation of the definition of 'personal information' as part of the review process.

The Discussion Paper reaffirms the OAIC's broad interpretation with proposals to remove any potential narrowing of the definition. This includes confirming that the definition:

- can relate to an individual (not just be about an individual),
- includes technical identifiers, such as online identifiers, ID numbers and location data,
- applies to inferred personal information

This would place Australia in line with global trends, including most recently the California Attorney-General's Decision that inferred personal information needs to be provided as part of access requests under the Californian Consumer Privacy Act.

2) Privacy impact assessments for large scale processing activities

Privacy impact assessments (PIAs) are designed to identify risks in handling personal information and provide ways to reduce risk. Some processing activities have greater privacy risks than others, and therefore need greater controls.

Australian government agencies are required to conduct PIAs for high-risk processing activities. The Discussion Paper presents the option of extending this requirement to the private sector, in particular to large scale processing involving:

- sensitive, location, biometrics or children's personal information
- direct marketing or sale of personal information
- influencing individual behaviour
- automated-decision making
- high privacy risk or risk of harm to individuals

3) Handling children's personal information

Based on current OAIC guidance, children are presumed to lack the capacity to consent to the handling of their personal information if they are under the age of 15.

Generally, consent is needed to:

- send direct marketing emails
- use or disclose personal information for purposes other than for which it was collected
- collect sensitive personal information
- send personal information overseas (in some cases)

The Discussion Paper proposes to legislate OAIC guidance and lift the age to 16. Thus requiring parent/guardian consent for the handling of personal information for those under the age of 16.

Additionally, there are expected to be further requirements in relation to the handling of children's personal information by large online platforms, social media and data brokerage services. This is outlined in exposure legislation.

4) A new fair and reasonable test for the collection, use and disclosure of personal information

Currently under APP 3.5 personal information must be collected by lawful and fair means. The purpose of collection, however, does not necessarily have to be fair and reasonable. Personal information under APP 6 can currently be used or disclosed for the primary purposes for which it was collected and secondary purposes where an exception is satisfied. A potential new requirement that the collection, use or disclosure is also fair and reasonable may be required.

What is fair and reasonable is likely to be the subject of much interpretation, debate and litigation. The Discussion Paper proposes setting out in legislation the factors to be taken into account in determining what is fair and reasonable.

5) A range of penalties

The Government has already agreed to penalties in the Privacy Act mirroring those in the Competition and Consumer Act. As such, for serious interferences with privacy the penalty would be the greater of:

- $10 million
- 10% of domestic annual turnover
- 3 times benefit received for breaching the Privacy Act

Penalties have to date not been routinely issued under the Australian Privacy Act. Indeed, only one case is currently before the courts for serious interferences with privacy, namely Facebook (Meta). The Discussion Paper proposes an additional penalty regime for interferences with privacy that are not serious or repeated - a new mid-tier civil penalty provision. A new power to issue infringement notices for administrative breaches is also proposed.

With the increased regulatory work that such changes will bring, the introduction of a levy scheme has been proposed. The scheme incorporates two components:

- a cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments; and

- a statutory levy to fund the OAIC's investigation and prosecution of entities operating in high privacy risk environments.

For more information on the review visit the Attorney-General's Department and Privcore's submission.

About Privcore

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.