Making privacy core business

Review of the Australian Privacy Act – Key areas of business interest

4 May 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

Review of the Australian Privacy Act –

Key areas of business interest

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

The Attorney-General's Department published more than 200 submissions in response to the Discussion Paper covering a broad spectrum of stakeholder views. Sixty-seven proposals for change are tabled in the Discussion Paper.

Privcore has reviewed key business submissions from a range of industries. The top ten areas for reform as proposed by the Attorney-General's Department that business stakeholders appeared to comment on the most are outlined below. There was a range of diverging views, where some businesses are in favour of change and others are not. The divergence of views, even just from the private sector alone, will make it challenging for decisions to be made as to what will be reformed in the Privacy Act.

Government, regulator and civil society perspectives are not covered in this paper and will be the subject of future work and discussions.

1) Changing the objects of the Privacy Act

pp.19-20 AGD Discussion Paper – Review of the Privacy Act:

In recognition that the objects should make it clear that the Act is concerned with informational privacy and that the protection of privacy is properly balanced against the protection of other public interests, subsections 2A(a) and (b) could be amended respectively.

Subsection 2A(a) could be amended to make clear that the Act is about protecting the personal information of individuals, and not more general notions of privacy.

Subsection 2A(b) could be amended to make it clearer that the subjective interests of entities are not relevant if their functions and activities are not in the public interest. This would recognise that not all interests should be reconciled with the protection of privacy. This would also be consistent with the Act's recognition of public interests other than privacy, including public health and safety, research, national security, freedom of expression, law enforcement and, regarding commercial entities, the economic wellbeing of the country.

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals with regard to their personal information; and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest.

Key discussion areas in response:

- does this mean privacy trumps when activity is not in the public interest?
- what is the public interest and who determines this?
- why the need to balance with public interest?
- legitimate interest in the GDPR sense and how this may be connected

2) What information is regulated and what is not – meaning of personal information

p.26 AGD Discussion Paper – Review of the Privacy Act:

In light of the uncertainty about how the definition of 'personal information' applies to technical and inferred information, there is a need for reform. It is important that the definition of personal information is clear enough to provide APP entities with confidence about their obligations under the Act.

The proposed changes reflect aspects of the GDPR's definition of 'personal data'. This is in recognition of the high level of support across sectors for the GDPR definition or otherwise harmonising the Australian definition with GDPR.

2.1-2.3 Overview of the proposed definition of personal information
Amend the definition of personal information to make clear that it includes technical and inferred personal information:

> Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:
> a) whether the information or opinion is true or not; and
> b) whether the information or opinion is recorded in a material form or not.
> An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.

This definition would be supported by the following amendments to the Act:

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information
- a list of objective factors to assist APP entities to determine when an individual is reasonably identifiable, and
- a definition of 'collection' that expressly covers inferred information.

Key discussion areas in response:

- is relates to an individual too broad?
- technical identifiers, such as online identifiers, ID numbers and location data, if included should they be within the Act or guidance?
- include deceased people's personal information?
- inferred personal information – where's the line?
- access and correction rights in light of any changes to the definition

3) De-identification and anonymisation

pp.30-31 AGD Discussion Paper – Review of the Privacy Act:

The Act could be amended to require information to be 'anonymous' rather than 'de-identified' for the Act to no longer apply.

Under this proposal, the definition of 'de-identification' would be removed and a definition of 'anonymous information' inserted. This reflects the proposed changes to definition of personal information in Proposals 2.1-2.3. If the definition of personal information is expanded then understandably more will need to be done to 'de-identify' that information so it falls outside that definition. The word 'anonymous' could more clearly signal to APP entities that they are required to meet the higher, irreversible standard reflected by this term.

Information would be considered 'anonymous' if it were no longer possible to identify someone from the information, considering the definition of 'reasonably identifiable' and the factors outlined in Proposal 2.3. This reform would not impose an absolute or unworkably high standard on APP entities that use data for research or service delivery. Information could be considered anonymous provided that the risk of re-identification was extremely remote or hypothetical.

Key discussion areas in response:

- anonymity – is that too high a bar?

4) Introduction of a fair and reasonable test for the collection, use and disclosure of personal information

p.11 AGD Discussion Paper – Review of the Privacy Act:

A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- The sensitivity and amount of personal information being collected, used or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity
- Whether the individual's loss of privacy is proportionate to the benefits
- The transparency of the collection, use or disclosure of the personal information, and
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.

Key discussion areas in response:

- where does this concept come from and what does it mean?
- is this another exception, or does this test have to be met for every collection, use or disclosure?
- how to work out what is fair and reasonable and from whose perspective?
- what would not be fair and reasonable?

5) Security

pp.14-15, 146 AGD Discussion Paper – Review of the Privacy Act:

Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.

Include a list of factors that indicate what reasonable steps may be required.

Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

Note: As part of Australia's Cyber Security Strategy 2020, the Government committed to clarify cyber security obligations for Australian businesses, including in the areas of privacy laws, consumer protection laws and corporate governance. The government is proposing to develop an APP code to specify minimum cybersecurity standards required by APP 11.1. Refer to the discussion paper 'Strengthening Australia's cyber security regulations and incentives', available at www.homeaffairs.gov.au/cyber.

Key discussion areas in response:

- should security requirements be outlined in an enforceable Code or in guidelines?
- clarity on what are reasonable steps, and what would be considered "all" reasonable steps?

6) Consent

pp.78, 104 AGD Discussion Paper – Review of the Privacy Act:

Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16.

Key discussion areas in response:

- the age for consent, where parent/guardian consent required – different to current OAIC guidelines – why is that?
- how current does consent need to be?
- areas where legitimate interest in the GDPR sense could be potentially used instead of consent

7) Controllers and processors

pp.156 AGD Discussion Paper – Review of the Privacy Act:

The introduction of controllers and processors was not proposed in the Discussion Paper and is also not supported by the OAIC. However, many businesses, particularly those that commonly act as processors, would like to see the introduction of the distinction between controllers and processors.

Key discussion areas in response:

- should this be introduced, if so, why?

8) Small business and employee records exemptions

pp.56 AGD Discussion Paper – Review of the Privacy Act:

The removal of the small business exemption was not proposed in the Discussion Paper though many stakeholders support its removal.

The employee records exemption could be modified to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship. However, there is no clear proposal to remove or modify the employee records exemption either.

Key discussion areas in response:

- dealing with access and correction requests in the event the employee records exemption is removed – what would be the appropriate limitations?

9) Direct right of action and statutory tort

pp.190, 195-197 AGD Discussion Paper – Review of the Privacy Act:

The Discussion paper proposes providing an additional forum for addressing alleged breaches of privacy, through a direct right of action, rather than being limited to bringing action through the OAIC.

25.1 Create a direct right of action with the following design elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the Federal Circuit Court.
- The claimant would first need to make a complaint to the OAIC (or FPO)1 and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert

evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

The Discussion paper also presents four different options in relation to a statutory tort of privacy, as follows:

Option 1

Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

Option 2

Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

Option 3

Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

Option 4

In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

Key discussion areas in response:

- extent of litigation that may occur in light of the high number of cyber security incidents leading to data breaches
- need for these options – wouldn't it be better to properly resource the OAIC, rather than create more channels for redress?

10) Industry levies

pp.182 AGD Discussion Paper – Review of the Privacy Act:

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- 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 which operate in a high privacy risk environment.

Key discussion areas in response:

- why don't government budgets fund the OAIC appropriately?

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.