Article Information

Authors: Craig Subocz, Tim Clark
Service: Corporate & Commercial, Cyber Security, Dispute Resolution & Litigation, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Attorney-General Department's Review puts proposals to significantly reform the Privacy Act on the table

On 16 February 2023, the Attorney-General released his Department's Report into a review of the *Privacy Act*. The Report contains 116 proposals to amend the *Privacy Act*. The Department has released a call for submissions in response to the Report (including the proposals). The period to make submissions closes on 31 March 2023. In order to implement the proposals, the Government will need to prepare legislation to go before Parliament to amend the *Privacy Act*. The Report represents a significant step in the path towards privacy law reform in Australia. However, the final form in which the proposals are implemented, and whether they are implemented at all, remains to be seen.

Australia's Attorney-General released his Department's Report into a review of the *Privacy Act* on 16 February 2023. The Report outlines the results of the Department's review which commenced in October 2020. It considers whether the *Privacy Act* and its enforcement mechanisms are still "fit for purpose" in Australia's growing digital economy.

The Report notes that there have been significant developments in data protection laws internationally and that the proposals are intended to "better align Australia's laws with global standards of information privacy protection and properly protect Australians' privacy".

The Report outlines no less than 116 proposals to reform the *Privacy Act*. The overarching theme of these proposals is to increase the protections for an individual's personal information. We look at the key proposals below:

Broaden the definition of "personal information"

The Report sets out proposals that would (if adopted by the Government) broaden the definition of "personal information". Currently, information or an opinion is personal information if the information or opinion is about an identified individual or an individual who is reasonably identifiable. The key proposal would replace the word "about" with the phrase "relates to", so that information or an opinion would be personal information if the information or opinion relates to an identified individual or an individual who is reasonably identifiable.

If this proposal is adopted by the Government, then Australia's definition of "personal information" would be more closely aligned with the definition of "personal data" under the General Data Protection Regulation (**GDPR**) that applies in the European Union.

Introduction of a new "fair and reasonable" test

The Report proposes a new "fair and reasonable" test to underpin the collection, use and disclosure of personal information. The test would provide a principles-based means of determining whether the handling of individuals' personal information is permissible, particularly in relation to certain practices of concern.

Under the proposal, the "fair and reasonable" test would be an objective test, to be assessed from the perspective of the reasonable person.

Based on the Report, it appears that it is intended that the individual's consent to the handling of personal information would not necessarily be a relevant factor to whether the handling of the information satisfies the "fair and reasonable" test that would apply if this proposal were accepted. Accordingly, those businesses who have an approach to privacy compliance based merely on an individual ticking a box to indicate his/her consent to the entity's collection and handling of the individual's personal information will likely need to reconsider this approach. This could represent a significant shift for many businesses as to the manner in which personal information is handled in Australia.

Tighter timeframes on the notification of "eligible data breaches"

The Report proposes that further amendments be made to the *Privacy Act* with respect to the notification of "eligible data breaches" (i.e., data breaches that give rise to a risk of serious harm to one or more affected individuals).

In particular, entities would be required to notify the Commissioner of an eligible data breach not later than 72 hours after the entity becomes aware of the breach, with an allowance for further information to be provided to the Commissioner if such information is not available within 72 hours. The *Privacy Act* would also be amended to allow the entity to provide information about the eligible data breach to affected individuals in phases. This tightening of the timeframes for data breach notification replaces a more obligation of an entity to notify as soon as reasonably practicable after an entity becomes aware of an eligible data breach. Such a change to the Privacy Act raises some obvious practical issues around the ability to identify whether a data breach gives rise to a risk of serious to affected individuals and reinforces the need for entities to have in place clear, and well thought out, data breach notification plans.

The Report also proposes that the *Privacy Act* be amended to require the entity to set out the steps it has taken (or intends to take) in response to the breach, including (where appropriate) steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

Right of individuals to object to the collection, use and disclosure of personal information

In the Report, the Department outlined a proposal that would (if accepted by the Government) allow individuals to object to the collection, use or disclosure of personal information and, if an individual exercises that right, require the entity to provide a written response to an objection (with reasons).

The proposed right to object is modelled on the right available to EU residents and others under the GDPR in that the right to object is limited to the handling of personal information for the purpose of direct marketing and, outside the context of direct marketing, the right will simply be the right to query the entity to justify their information handling practices.

If this proposal is implemented, businesses that use personal information to directly market to current and potential customers will need to incorporate into their direct marketing processes the ability to respond to an objection raised by a recipient of their direct marketing efforts. All entities that collect and handle personal information would need to be prepared to justify their information handling processes and procedures should an individual exercise this right to object in a context other than the use of the information for direct marketing purposes.

Right to seek erasure of personal information

Further, the Report outlines a proposal that would (if implemented by the Government) confer on individuals the right to seek erasure of any of their personal information held by an entity about the individual, and to require the entity to notify any third parties that received information about the individual of the erasure request (unless an exception applies). This right is similar to the right that exists under the GDPR.

If the Government introduces such a right into the *Privacy Act*, it is likely that businesses, whose operations are not currently covered by the GDPR, will need to consider and draw on the experience of organisations in the EU on how to act on such erasure requests received from individuals and implement processes in their systems to manage such requests.

Requirement for greater transparency over the use of personal information in automated decision making

The Report outlines several proposals that relate to the use by entities of personal information in "substantially automated decisions which have a legal or similarly significant effect on an individual's rights". An example of such a decision is an automated decision made in relation to an online loan application.

Under the proposals, entities would need to expressly set out the types of information that would be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights. The *Privacy Act* would be amended to set out the high-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights. The Report also proposes that the *Privacy Act* would be amended to introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effects are

made.

If these proposals are accepted, those entities that use automated decision making systems in the course of their business may be required to substantially revise their processes and policies and to prepare responses to individuals who seek meaningful information about how the automated decisions are made by the business. One particular practical issue that may arise is that entities may need to consider how their disclosures about the use of personal information in automated decision-making processes are provided to the individual before the information is collected and used.

Possible removal of the "small business exemption"

Currently, businesses with an annual turnover of less than $3 million are generally exempt from the *Privacy Act*, under the "small business exemption". The Report sets out a proposal for removing this exemption, but only after an impact analysis has been completed, appropriate support has been developed, the most appropriate way for small business to meet their obligations is determined and small businesses are in a position to comply with the obligations imposed by the *Privacy Act*. Therefore, in comparison to other proposals, it seems that the removal of the small business exemption would be unlikely to occur in the short term.

"Processors" and "controllers" to be introduced into the Privacy Act

The Report sets out a proposal to amend the *Privacy Act* to introduce the concepts of "processors" and "controllers" in a manner that is consistent with the GDPR. Accordingly, if adopted by the Government, those entities which are merely processors of personal information under instruction from the controller would be subject to fewer compliance obligations under the *Privacy Act*. In particular, based on the proposal, "processors" would only be required to comply with APP 1 (open and transparent management of personal information), APP 11 (security of personal information) and the notifiable data breach scheme (save that processors would not be required to notify individuals at risk of serious harm as a result of the data breach).

Introduction of a statutory cause of action for invasion of privacy

The Report sets out a proposal for the introduction of a statutory cause of action for individuals for invasion of privacy. The Report however notes that the codification of the cause of action should only occur after consultation with the States and Territories on implementation to ensure a consistent national approach.

The Government is accepting submissions in response to the Report until 31 March 2023, before determining what further steps it will take in response to the proposals set out in the Report. It may be some time before the Government produces draft legislation to amend the *Privacy Act*. Accordingly, it is yet to be determined which proposals will be implemented and, if so, the manner in which the proposals will be implemented into the *Privacy Act*.

Key Takeaways

- On 16 February 2023, the Attorney-General released the Report of a review of the *Privacy Act* which had been conducted by his Department since October 2020. The Report contains 116 proposals to reform the *Privacy Act*.
- Among these proposals include a broader definition of "personal information", the introduction of a statutory cause of action for invasion of privacy, the eventual 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 any collection, use and disclosure of personal information be "fair and reasonable"
- The Government seeks submissions on the proposals for reform, with the deadline for submissions closing on 31 March 2023.
- The Report represents a significant step in the road towards privacy law reform in Australia, but it remains to be seen which proposals will be implemented and the manner in which those proposals will be implemented.