HawkerBritton
Government Relations Strategy

Privacy Act Review Report

Introduction

On 16 February 2023, the Attorney-General publicly released the Privacy Act Review Report (The Report). A one-page review of the report is available here. The aim of the report was to consider whether the act and its enforcement mechanisms are adequate.

The report summarises a two-year review of the Privacy Act 1988 (The Act) in Australia, which was initiated following the Australian Competition and Consumer Commission's (ACCC) 2019 Digital Platforms Inquiry final report.

The report was informed by feedback received in response to an Issues Paper released in October 2020 and a Discussion Paper, released in October 2021.

The proposed reforms are all-encompassing and touch on every aspect of how personal information is collected and managed, and introduce a multitude of new rights for individuals.

The recommendations are designed to align Australia's privacy laws with global standards and properly protect Australians' privacy, while also enhancing cross-border data flows and benefiting the economy.

A number of changes to the Australian Privacy Principles (or APPs) are proposed in the Report.

APPs' are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers.

There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

The Government is now seeking feedback on the 116 proposals. Submissions on the report are due on 31 March 2023.

The proposals are summarised below.

Key Recommendations

Personal information, de-identification and sensitive information

Several changes to the definitions of personal information, de-identification, and sensitive information under the Privacy Act have been suggested.

Proposed changes include:

- Using "relates to" instead of "about" in the definition of personal information
- Providing a non-exhaustive list of information that may be considered personal information
- Amending the definition of collection to cover information obtained from any source
- Providing a non-exhaustive list of circumstances for reasonably identifiable information, and extending protections under the Privacy Act to de-identified information.

The flexibility of the Australian Privacy Principles (APPs)

The review recommends giving the Information Commissioner the power to make an Australian Privacy Principal's code when there is no industry representative to develop the code. The Commissioner would be required to consult with the public and relevant parties as part of the code development process.

Additionally, the Commissioner would gain the ability to issue a temporary APP code for a maximum of 12 months when it is both in the public interest and urgently required.

The recommendations also suggest amending the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.

Small Business Exemption

The review proposes to remove the small business exemption from the Privacy Act, but only after:

- conducting an impact analysis to understand its impact on small businesses
- Developing appropriate support in consultation with small businesses
- Determining the most appropriate way for small businesses to meet their obligations proportionate to the risk
- Ensuring small businesses can comply with these obligations.

In the short term, it recommends:

- Exempting from the Act for small businesses that obtain consent to trade in personal information is removed
- prescribing the collection of biometric information for use in facial recognition technology as an exception to the small business exemption,

Employee Records Exemption

Enhanced privacy protections for private sector employees are proposed including providing transparency to employees regarding what personal and sensitive information is collected and used.

Further consultation with employer and employee representatives will be undertaken to clarify obligations and explore privacy codes of practice.

Political Exemption

The review recommends amending the definition of 'organisation' under the Act to include registered political parties and subjecting them to privacy protections.

Political entities would be required to publish a privacy policy and ensure that acts and practices under the exemption are fair and reasonable.

Individuals will be given the ability to opt out of direct marketing and receive targeted advertising from political entities.

The OAIC will develop guidance materials to help political entities understand and comply with their obligations, including what reasonable steps should be taken to protect personal information and comply with the NDB scheme in case of a data breach.

Journalism Exemption

The following changes to the journalism exemption are suggested.

- Allowing media organisations to handle personal information in certain circumstances without complying with the Privacy Act.
- Media organisations must be subject to privacy standards overseen by a recognized oversight body or have adequate privacy standards.
- The OAIC should develop criteria for adequate media privacy standards, and media organisations should comply with security and destruction obligations in line with APP 11 and reporting obligations in the NDB scheme.
- An independent audit and review of the operation of the journalism exemption should be conducted three years after the amendments come into force.

Privacy policies and collection notices

An express requirement for APP 5 to ensure collection notices are clear, up-to-date, concise and understandable with appropriate accessibility measures in place will be implemented.

OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.

It is further suggested that the development of standardised templates, layouts, terminology, and icons for privacy policies and collection notices across the economy, to maintain consistency and ensure clarity.

Consent and Privacy Default Setting

Amendments to the definition of consent in the Act to make it voluntary, informed, current, specific, and unambiguous are proposed.

The OAIC is encouraged to develop guidance on how online services should design consent requests, and there should be the ability to withdraw consent easily. Additionally, online privacy settings should reflect the privacy by default framework of the Act, and be clear and easily accessible to service users.

Fair and reasonable personal information handling

The report suggests amending the Act to require that collection, use, and disclosure of personal information must be fair and reasonable in the circumstances.

It identifies the factors to be taken into account when determining whether a collection, use, or disclosure of personal information is fair and reasonable.

It also proposes that the requirement for fairness and reasonableness in the circumstances should apply regardless of whether consent has been obtained.

Additional Protections

APP entities will be required to conduct a privacy impact assessment before undertaking activities with high privacy risks.

The OAIC will develop guidance on the factors that indicate a high privacy risk and provide examples of activities that require a privacy impact assessment. Enhanced risk assessment requirements will be in place for facial recognition technology and other uses of biometric information.

The review also states that the OAIC should develop practice-specific guidance for new technologies and emerging privacy risks.

Research

The review recommends introducing a legislative provision that permits broad consent for the purposes of research.

Further consultation will be required in order to develop a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.

Organisational Accountability

Proposal 15 requires that an organisation must dictate and record the purposes for which it will collect, use and disclose personal information at the time of collection. If the organisation wants to use or disclose personal information for a secondary purpose, it must record that secondary purpose before undertaking it.

Organisations will be required to appoint or designate a senior employee responsible for privacy.

Children and People Experiencing Vulnerability

Suggested changes to protect vulnerable people include:

- Defining a child as someone under 18 years old
- Requiring entities to assess if an individual under 18 can consent on a case-by-case basis.
- Collection notices and privacy policies will need to be clear and understandable for children

- Requiring entities to consider the best interests of the child when collecting, using or disclosing personal information.
- Creating a Children's Online Privacy Code with requirements on how to design an online service that considers the best interests of child users.
- Creating an OAIC guide that indicates a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability will be created

Rights of the Individual

The report aims to provide individuals with more control over their personal information. This includes the right to access, an explanation, an objection, erasure, correction, and de-indexing of personal information.

APP entities will be required to notify individuals of their rights and provide assistance in exercising them. They must also respond to requests within a reasonable timeframe and provide reasons for refusal.

Automated Decision Making

Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

Direct Marketing, Targeting and Trading

The report recommends amending the Act to introduce definitions for direct marketing, targeting, and trading.

It also proposes:

- Giving individuals the right to opt out of their personal information being used or disclosed for direct marketing and receiving targeted advertising.
- Introducing a requirement for obtaining an individual's consent before trading their personal information.
- Prohibiting direct marketing to children unless it's in their best interests
- prohibiting targeting based on sensitive information
- Requiring entities to provide clear information about the use of algorithms and profiling to recommend content to individuals.

Security, Retention and Destruction

Numerous amendments relating to securing personal information are proposed including that:

- APP entities should take "reasonable steps" to protect personal information, which includes technical and organisational measures
- The guidelines on securing personal information should be enhanced.
- APP entities should establish their own maximum and minimum retention periods for personal information
- APP 11 should be amended to require entities to take reasonable steps to protect de-identified information and to provide guidance on destroying or de-identifying personal information.

- The Commonwealth should review all legal provisions that require the retention of personal information.

Controllers and Processors of Personal Information

The report recommends introducing the concepts of APP entity controllers and APP entity processors into the Privacy Act.

This means that a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller.

Overseas Data Flows

The proposals suggest various measures to strengthen the protection of personal information in Australia. Including:

- Adding an "Australian link" requirement for personal information connected to Australia.
- A mechanism to identify countries and certification schemes that provide substantially similar protection to Australia's privacy laws.
- Making standard contractual clauses available to entities transferring personal information overseas.
- Strengthening the informed consent exception to overseas disclosures by considering risks and informing individuals of privacy protections.
- Suggests requiring entities to specify the countries and types of personal information disclosed when disclosing personal information overseas.
- Proposes defining "disclosure" consistently with current guidelines and potentially excluding online publications from the requirements of APP 8 if in the public interest.

Enforcement

To improve the regulation of privacy interference in Australia, the review suggests:

- The creation of tiers of civil penalty provisions
- Introduction of infringement notice powers
- Amendments to the Act to allow for better targeted regulatory responses.

Additionally, the Information Commissioner would have the powers to:

- Investigate civil penalty provisions
- Conduct public inquiries and reviews
- Identify and mitigate actual
- Reasonably foreseeable loss.

The Federal Court will have the power to make any order after a civil penalty provision was established.

The OAIC will undergo an internal review to ensure a greater enforcement focus.

The Information Commissioner would have the discretion not to investigate complaints already dealt with by an EDR scheme.

A direct right of action

Proposal 26 aims to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy.

A statutory tort for serious invasions of privacy

The introduction of a statutory tort for serious invasions of privacy is recommended by the Australian Law Reform Commission.

Notifiable Data Breaches Scheme

Numerous proposals are made in relation to the reporting of data breaches:

- Requiring entities to notify the Commissioner and affected individuals within 72 hours of becoming aware of an eligible data breach.
- Requiring entities to outline the steps they have taken or will take in response to a data breach.
- Introducing a provision in the Privacy Act that would allow information to be shared with appropriate entities to reduce the risk of harm in the event of an eligible data breach.

Next steps

Feedback is being sought on the Government's response to the Privacy Act Review Report. The deadline for feedback is 31 March 2023. Organisations can submit feedback here.

Proposal 30 of the report states that there should be a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.

For more information, please contact Hawker Britton's Managing Director Simon Banks on +61 419 648 587.