HawkerBritton
Government Relations Strategy

Privacy Act Review Report - Government's Response

On the 28th of September 2023, Attorney General Mark Dreyfus KC MP released the Government's response to the Privacy Act Review Report.

The Privacy Act Review Report, available here, summarises a two-year review of the Privacy Act 1988 (The Act) in Australia. The Privacy Act Review Report includes 116 proposals a summary of proposals are available here.

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.

Agree

The Government has committed to 38 of the proposals which have been summarised below.

Objects of the ACT

- Amend the objects of the Act to clarify that the Act is about the protection of personal information
- Amend the objects of the Act to recognise the public interest in protecting privacy

Personal information, de-identification and sensitive information

- Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.

Flexibility of the APPs

- Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made.
- Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.
- Amend the Act to enable Emergency Declarations to be more targeted.
- Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.
- Amend 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.

HawkerBritton
Government Relations Strategy

Journalism Exemption

- To benefit from the journalism exemption a media organisation must be subject to privacy standards that adequately deal with privacy and are overseen by a recognised oversight body

Additional Protections

- Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted.
- The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks.

Research

- Introduce a legislative provision that permits broad consent for the purposes of research
- Consult further on broadening the scope of research permitted without consent for both agencies and organisations.
- Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.

Children

- Define a child as an individual who has not reached 18 years of age.
- Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'.

People experiencing vulnerability

- Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.
- OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.

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.
- High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act.
- Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

Security, retention and destruction

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

- The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information

Overseas Data Flows

- Consult on an additional requirement to demonstrate an 'Australian link' that is focused on personal information being connected with Australia
- Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs

Enforcement

- Create tiers of civil penalty provisions to allow for better- targeted regulatory responses
- Remove the word 'repeated' and clarify that a 'serious' interference with privacy may include those involving 'sensitive information', those adversely affecting large groups of individuals, those impacting people experiencing vulnerability.
- Amend the Act to apply the powers of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.
- Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.
- Amend the Act to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss.
- Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.
- Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged.
- The OAIC should conduct a strategic internal organisational review.
- The Information Commissioner should have the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme

Notifiable data breaches scheme

- Undertake further work to better facilitate the reporting processes for notifiable data breaches
- Introduce a provision in the Privacy Act to enable the AttorneyGeneral to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach.

Interactions with other schemes

- Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

HawkerBritton
Government Relations Strategy

Agree in Principle

The Government has agreed in principle to 68 measures which have been summarised below.

Personal information, de-identification and sensitive information

- Change the word 'about' in the definition of personal information to 'relates to'.
- Include a non-exhaustive list of information that may be personal information to assist APP entities to identify the types of information which could fall within the definition.
- Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.
- 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.
- Amend the definition of 'de-identified' to make it clear that deidentification is a process, informed by best available practice, applied to personal information which involves treating it in such a way that no individual is identified or reasonably identifiable in the current context.
- Sensitive Information
    - Amend the definition of sensitive information to include 'genomic' information.
    - Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.
    - Clarify that sensitive information can be inferred from information which is not sensitive information
- Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice that requires consent. Define 'geolocation tracking data' as personal information.

Small Business Exemption

- Remove the small business exemption.
- In the short term, prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption and remove the exemption from the Act for small businesses that obtain consent to trade in personal information.

Employee Records Exemption

- Enhanced privacy protections should be extended to private sector employees. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact.

Journalism Exemption

- the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.
- An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments come into force.
- Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.
- Require media organisations to comply with the reporting obligations in the NDB scheme.

Privacy policies and collection notices

- Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable.
- The list of matters in APP 5.2 should be retained.
- Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed

Consent and privacy default settings

- Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.
- The OAIC could develop guidance on how online services should design consent requests
- Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent.
- Online privacy settings should reflect the privacy by default framework of the Act.

Fair and reasonable personal information handling

- Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.
- The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained.

Additional Protections

- APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks
- Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Organisational Accountability

- An APP entity must determine and record the purposes for which it will collect, use and disclose personal information.
- Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity.

Children

- Existing OAIC guidance on children and young people should continue to be relied upon by APP entities.
- Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child
- Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.

People experiencing vulnerability

- Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.
- Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

Rights of the Individual

- Provide individuals with a right to access, and an explanation about, their personal information if they request it
- Introduce a right to object to the collection, use or disclosure of personal information.
- Introduce a right to erasure
- Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.
- Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.
- Individuals should be notified at the point of collection about their rights and how to obtain further information
- An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.
- An APP entity must take reasonable steps to respond to an exercise of the right of an individual.
- An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding

Direct marketing, targeting and trading

- Amend the Act to introduce definitions for direct marketing, targeting and trading
- Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.
- Introduce a requirement that an individual's consent must be obtained to trade their personal information.

- Prohibit direct marketing and targeting to a child and prohibit trading in the personal information of children.
- Targeting individuals should be fair and reasonable in the circumstances and targeting individuals based on sensitive information should be prohibited.
- Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals.

Security, retention and destruction

- Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.
- The Commonwealth should undertake a review of all legal provisions that require the retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.
- Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks
- Amend APP 1.4 to stipulate that an APP entity's privacy policy must specify its personal information retention periods.

Controllers and processors of personal information

- Introduce the concepts of APP entity controllers and APP entity processors into the Act.

Overseas Data Flows

- Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.
- Strengthen the informed consent exception to APP 8.1
- Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas
- Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines

Enforcement

- Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.

- Further consideration should be given to establishing a contingency litigation fund to fund any cost orders against the OAIC, and an enforcement special account to fund high cost litigation.

A direct right of action

- Amend the Act 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

- Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC

Notifiable data breaches scheme

- If an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner and must notify the individuals to whom the information relates as soon as practicable.
- A statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach

Interactions with other schemes

- Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Notes

The Government has noted 10 measures which have been summarised below.

Personal information, de-identification and sensitive information

- Extend the protections of the Privacy Act to de-identified information
- Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions

Political Exemption

- Amend the definition of 'organisation' under the Act so that it includes a 'registered political party'.
- Political entities should be required to publish a privacy policy that provides transparency in relation to acts or practices covered by the exemption.
- The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.

Direct marketing, targeting and trading

- Provide individuals with an unqualified right to opt-out of receiving targeted advertising

Security, retention and destruction

- Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.

Next Steps

The government is committed to building upon the legislation enacted last year, which significantly heightened penalties for repeated or severe privacy breaches and granted the Australian Information Commissioner expanded authority to address such breaches.

The Attorney-General's Department will conduct an impact analysis and will continue collaborating with the community, businesses, media organisations, and government agencies to shape legislation and provide guidance during this parliamentary term.

The Government will also consider appropriate transition periods as part of the development of any legislation.

These privacy reforms will complement other initiatives being advanced by the government, including Digital ID, the 2023-2030 Australian Cyber Security Strategy, the National Strategy for Identity Resilience, and efforts to promote responsible AI in Australia.

The Government intends to legislate the changes in 2024.

Furthermore, the government has preliminarily agreed to conduct a statutory review of any amendments to the Act that implement the recommendations outlined in this report within three years of the commencement date of those amendments.

For more information, please contact Hawker Britton's Managing Director Simon Banks on +61 419 638 587.