Australian Government

Government Response
| Privacy Act Review Report

ISBN (Online): 978-1-921241-74-1

Table of contents

Introduction

The digital economy has led to innovation, advances in productivity and efficiency and a range of other benefits for Australians. However, the vast data flows underpinning digital ecosystems have also created the conditions for recent major data breaches affecting millions of Australians, with their sensitive personal information being exposed to the risk of identity fraud and scams. Strong privacy protections are critical to building the security, confidence and trust necessary to drive innovation and economic growth.

Australians are seeking greater protection in the handling of their personal information. The 2023 Office of the Australian Information Commissioner (OAIC) Australian Community Attitudes to Privacy Survey (2023 ACAP survey) makes clear the high priority Australians place on the security of their personal information. Three in five (62%) of Australians surveyed see the protection of their personal information as a major concern in their life, and 75% consider that data breaches are one of the biggest privacy risks they face today (increasing by 13% since 2020). Only 32% feel in control of their data privacy, and 84% want more control and choice over the collection and use of their personal information. 89% would like the Government to provide more legislation in this area.

The Privacy Act Review Report (the Report) is the culmination of over two years of extensive consultation. The Report concluded that it is necessary to overhaul Australia's privacy laws, as many other countries have done, to ensure they remain fit-for-purpose in the digital age. Feedback following the release of the Report has reiterated a clear expectation that Government will strengthen privacy laws to ensure the collection, use and disclosure of people's personal information is reasonable, reflects community expectations and is adequately protected from unauthorised access and misuse. Industry and other stakeholders have raised concerns about the potential regulatory impact and the need for reforms to strike an appropriate balance.

The Government is committed to uplifting privacy protections while encouraging digital innovation. Australia can no longer afford to have inadequate privacy protections. Privacy uplift is needed to guard against identity fraud, scams and the risk to businesses of failing to manage personal information appropriately. Business sustainability relies on the ability to protect personal information. A failure to uplift Australia's privacy standards to more closely align with global standards also has the potential to adversely impact the international competitiveness of Australian businesses.

This Response indicates the Government 'agrees' to a number of the Report's proposals. Once draft legislative provisions have been developed for these measures, we will undertake targeted consultation with entities prior to settling their final form.

The Response indicates the Government 'agrees in-principle' with other proposals. This agreement is subject to further engagement with regulated entities and a comprehensive impact analysis to ensure the right balance can be struck between privacy benefits for Australians and other impacts on regulated entities. It is important that the benefits and economic costs are understood including any appropriate adjustments. This further exploration, which will be led by the Attorney-General's Department, in consultation with Treasury, will inform Government's further consideration of these proposals.

The Attorney-General's Department will continue to lead this work across government into 2024, including considering the interaction with related but separate work on strengthening cyber security, the use of artificial intelligence (AI) including automated decision-making and digital identity (A summary table of the responses to proposals is at Attachment A).

Overview

The Government will progress consideration of reforms to Australia's privacy framework under five key focus areas:

1. **Bring the Privacy Act into the digital age**

   Bring the scope and application of the Privacy Act into the digital age by recognising the public interest in protecting privacy and exploring further how best to apply the Act to a broader range of information and entities which handle this personal information.

2. **Uplift protections**

   Uplift the protections afforded by the Privacy Act by requiring entities to be accountable for handling individuals' information within community expectations, and enhancing requirements to keep information secure and destroying it when it is no longer needed. Reforms to the Notifiable Data Breaches (NDB) scheme will assist with reducing harms which may result from data breaches and new organisational accountability requirements will encourage entities to incorporate privacy-by-design into their operating processes. New specific protections will also apply to high privacy risk activities and more vulnerable groups including children, especially online.

3. **Increase clarity and simplicity for entities and individuals**

   Provide entities with greater clarity on how to protect individuals' privacy, and simplify the obligations that apply to entities which handle personal information on behalf of another entity. The reforms will increase the flexibility of code-making under the Act, reduce inconsistency and improve coherence across different legal frameworks with privacy protections, and simplify requirements for transferring personal information overseas, particularly to those countries with substantially similar privacy laws.

4. **Improve control and transparency for individuals over their personal information**

   Provide individuals with greater transparency and control over their information through improved notice and consent mechanisms. We will also explore the scope and application of new rights in relation to personal information and increased avenues to seek redress for interferences with privacy, through a direct right of action permitting individuals to apply to the courts for relief for interferences with privacy under the Privacy Act and a new statutory tort for serious invasions of privacy.

5. **Strengthen enforcement**

   Increase enforcement powers for the OAIC, expand the scope of orders the court may make in civil penalty proceedings and empower the courts to consider applications for relief made directly by individuals. A strategic assessment of the OAIC and further consideration of its resourcing requirements, including investigating the effectiveness of an industry funding model and establishing litigation funds, will enhance the effectiveness of Australia's privacy regulator.

Next steps

The Attorney-General's Department will lead the next stage of implementation which will involve:

- development of legislative proposals which are 'agreed', with further targeted consultation to follow
- engagement with entities on proposals which are 'agreed in-principle' to explore whether and how they could be implemented so as to proportionately balance privacy safeguards with potential other consequences and additional regulatory burden
- development of a detailed impact analysis, to determine potential compliance costs for regulated entities and other potential economic costs or benefits (including for consumers), and
- progressing further advice to Government in 2024, including outcomes of further consultation and legislative proposals.

The Government acknowledges that entities covered by the Privacy Act will require sufficient time to be in a position to comply with new requirements when reforms commence. Consideration will be given to appropriate transition periods as part of the development of legislation as well as appropriate guidance and other supports which could be developed to help entities understand their compliance requirements.

An impact analysis will be undertaken to more comprehensively determine the costs and benefits for Australians, including consumers as well as businesses and organisations. Given the diversity of entities required to comply with the Privacy Act, the impact analysis will consider the costs to different sectors of the economy and whether particular industries may require additional support to comply with new requirements. It will also facilitate a more detailed understanding of the practical implications for entities in transitioning to meet new obligations. Transition periods will be critical to ensure entities are in a position to comply with new obligations on their commencement.

The Government's role in strengthening privacy regulation, enforcing privacy protections and assisting with coordinating responses to significant data breaches must be complemented by Australians' increased understanding of privacy risks, and improved privacy practices of both individuals and entities. There is also an important role for the Government in conducting its own activities – including its use of data and digital technologies – in an appropriately careful manner. The Government will adopt robust and appropriate privacy and security settings as set out in this response and its Data and Digital Government Strategy.

Reforming Australia's privacy framework will complement other reforms being progressed by the Government, including the 2023-2030 Australian Cyber Security Strategy, Digital ID, the National Strategy for Identity Resilience, and Supporting Responsible AI in Australia. All these initiatives recognise the critical importance of Government working with stakeholders on reforms which will assist entities to manage risks appropriately and enable Australians to safely and securely engage in the digital economy. In progressing privacy reforms, the Government will continue to work closely with all stakeholders to ensure appropriate implementation.

1. Bring the Privacy Act into the digital age

Purpose of the Privacy Act

Feedback on the Act's objects indicated a need to recognise that protecting individuals' privacy is critical for building public trust and facilitating participation in public life, and that this understanding should factor into the interpretation of the rights and obligations in the Privacy Act. The Government **agrees** that the objects of the Privacy Act should be amended to recognise the public interest in protecting privacy (*proposal 3.2*). This does not preclude broader conceptions of privacy being recognised elsewhere, nor mean that other public interests will be irrelevant when considering the public interest in privacy. In relation to recognising a human right to privacy, the Government notes the position paper issued by the Australian Human Rights Commission earlier this year, 'A Human Rights Act for Australia' and the work of the Parliamentary Joint Committee on Human Rights into Australia's Human Rights Framework. The Committee will consider whether the Framework remains fit for purpose, if improvements can be made and if the Australian Parliament should enact a federal Human Rights Act. The Committee's final report is due in 2024.

Given the Act's focus on information privacy, the Government also **agrees** that the objects should be amended to clarify that the focus of the Privacy Act is on information privacy (*proposal 3.1*).

Information protected by the Privacy Act

Feedback provided to the Review revealed uncertainty about which information constitutes 'personal information' to be protected by the Privacy Act. The Government **agrees in-principle** that amendments to the Privacy Act are needed to clarify that personal information is an expansive concept that includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals (*proposal 4.1*). The Government **agrees in-principle** that the Privacy Act should include non-exhaustive lists to assist entities determine when information will be personal information and when an individual will be reasonably identifiable (*proposals 4.2 and 4.4*).

Importantly, the Government considers that an individual may be reasonably identifiable where they are able to be distinguished from all others, even if their identity is not known. This will require consideration of whether the information available – whether by itself or in conjunction with other information available to the entity – is sufficient to be linked to a particular individual even if their name is not known, or if there is a reasonable likelihood of identification or re-identification of an individual (that is, whenever the risk of identification or re-identification is higher than low or remote). For example, if a website publisher uses persistent cookies, device fingerprinting, or similar unique identifiers, the publisher may be able to identify a visitor, even if the visitor's IP address is not unique to that visitor.

In implementing these changes, the Government will consult further on how the definition of personal information may improve understanding of when information relates to an individual who is identified or reasonably identifiable. Additional OAIC guidance will also help to clarify when an individual is reasonably identifiable in different contexts and when the connection between information and an individual is too tenuous or remote to be considered personal information. The Government also **agrees in-principle** that the definition of 'collection' should be amended to expressly cover information obtained from any source and by any means, including inferred or generated information (*proposal 4.3*). Additional OAIC guidance will assist with clarifying when an inference is made and the practical implications of how different requirements in the Australian Privacy Principles (APPs) may apply to inferred information.

The Government **agrees in-principle** that the concept of de-identification should be defined in the Privacy Act to clarify that de-identification is a contextual process (*proposal 4.5*). The Government **agrees** that there should be further consultation on introducing a criminal offence for malicious re-identification (*proposal 4.7*). The Government **notes** the proposals to apply specific protections of the Privacy Act to de-identified information; the Government generally agrees with the policy intent of protecting de identified information from unauthorised re-identification (*proposals 4.6 and 4.8*) and will consider further how this objective may be able to be achieved.

The Government **agrees in-principle** that the definition of sensitive information should be amended to include genomic information and to clarify that sensitive information can be inferred from information that is not sensitive information (*proposal 4.9*). As part of this, consideration of additional OAIC guidance will assist with clarifying when an inference is made and the practical implications of how the APPs may apply to inferred information. The Government also **agrees in-principle** that consent should be required for the collection of precise geolocation tracking data over time, and will consider further whether this should be included as a new sub-category of sensitive information (*proposal 4.10*).

Entities covered by the Privacy Act

Submissions to the Review raised concerns about the current broad exemptions from the Privacy Act, which leave Australians' personal information vulnerable and potentially exposed to misuse. The 2023 ACAP survey revealed the majority of Australians surveyed think all organisation types are required to comply with the Privacy Act, indicating a broad community expectation that any entity handling individuals' information should be protecting individuals' privacy.

Small business

Most small businesses with an annual turnover of $3 million or less are currently exempted from the Privacy Act. At the time the Privacy Act was extended to the private sector, it was considered that most small businesses posed a low risk to privacy and that compliance costs would disproportionately and unreasonably burden small businesses. However, feedback provided to the Review is very clear – the community expects that if they provide their personal information to a small business it will be kept safe and not used in harmful ways.

The Government **agrees in-principle** that the small business exemption should be removed in light of the privacy risks applicable in the digital environment (*proposal 6.1*). However, this should not occur until further consultation has been undertaken with small businesses and their representatives on the impact that removing the small business exemption would have. This would inform consideration of what privacy obligations should be modified for small businesses to ease the regulatory burden and what support small businesses would need to adjust their privacy practices to facilitate compliance with new privacy obligations.

Recognising the different impact that compliance with privacy obligations will have for different types of small businesses, depending on the risk profile of their information-handling acts and practices, the Government will continue to work closely with small businesses and their representatives to understand the impact of any proposed changes. This will inform the development of new legislated privacy obligations and dedicated supports for small businesses to assist affected businesses to comply with proposed changes. For example, these supports may include tailored guidance, e-learning modules and other tools. The removal of the small business exemption should also be subject to an appropriate transition period to ensure small businesses are in a position to comply with new obligations.

The Government **agrees in-principle** that in the shorter term, small businesses which engage in activities that pose a significant privacy risk, including small businesses that collect biometric information that is to be used for the purposes of automated biometric verification or biometric identification, such as facial recognition technology, and small businesses that trade in personal information, should no longer be able to rely on the small business exemption (*proposal 6.2*).

Employee records

Employee records of current or former private sector employees are exempt from the Privacy Act. The original rationale for this exemption was that employee privacy was better regulated through workplace relations laws. The Government **agrees in-principle** that further consultation should be undertaken with employer and employee representatives on how enhanced privacy protections for private sector employees may be implemented in legislation (*proposal 7.1*). This should include consideration on how privacy and workplace relations laws should interact. Implementation of reforms to the employee records exemption should consider the impact and timing of new privacy obligations on small businesses.

Political entities

Registered political parties are exempt from the Privacy Act. A more limited exemption applies to political representatives (members of Commonwealth, state and territory legislatures and local government councillors), and their affiliates. The political exemption covers acts and practices done for any purpose in connection with an election, a referendum, or participation in another aspect of the political process. The exemption was introduced to encourage freedom of political communication and enhance the operation of the electoral and political process in Australia. The Government **notes** the Report's proposals to narrow the political exemption (*proposals 8.1–8.6*).

Journalism

The journalism exemption from the Privacy Act recognises the important and beneficial role of journalistic output. The purpose of the journalism exemption is to balance the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media. The Government **agrees** that the exemption for media organisations 'in the course of journalism' should continue, with strengthened self-regulation requirements for media organisations not subject to privacy standards overseen by a recognised oversight body (ACMA, APC or IMC) (*proposal 9.1*). Further consideration will need to be given to how best to support smaller news media organisations engaging in public interest journalism. The Government **agrees in-principle** that 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. These resources should be developed in consultation with industry and the ACMA (*proposal 9.2*).

The journalism exemption will continue to operate to ensure that media organisations are not required to comply with Privacy Act obligations relating to the collection, use, and disclosure of personal information, provided the collection, use or disclosure occurred in the course of journalism. Media organisations would also not be subject to individual rights, including the new individual rights such as the right of erasure in relation to personal information that is covered by the journalism exemption. However, the Government **agrees in-principle** that media organisations should be required to keep personal information secure, destroy it when it is no longer needed and report eligible data breaches to the OAIC (*proposals 9.4 and 9.5*). Media organisations should not be required to notify individuals of a data breach where the public interest in journalism outweighs the interest of affected individuals in being notified. Retaining and publishing personal information in the course of journalism would not constitute a breach of APP 11. Further consultation with media organisations should be undertaken when implementing these reforms.

The Government **agrees in-principle** that an independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the exemption (*proposal 9.3*).

2. Uplift protections

Fair and reasonable information handling

The current framework requires individuals to largely self-manage their privacy on the assumption that individuals engage with and comprehend the privacy policies and collection notices of entities. Feedback provided to the Review has revealed that people often do not understand the risks of complicated information handling practices and do not feel they have control over their personal information. Relying exclusively on notice and consent to regulate personal information-handling may be placing an unrealistic burden on individuals to decipher lengthy policies and collection notices that outline complex practices.

The Government **agrees in-principle** that this imbalance be addressed through a new requirement that collections, uses and disclosures of personal information are fair and reasonable in the circumstances (*proposal 12.1*), and **agrees in-principle** to the legislated factors relevant to assessing the requirement (*proposal 12.2*). An entity will still be permitted to collect personal information, however the fair and reasonable test will ensure that the impact on individuals resulting from an entity's handling of personal information and the public interest in protecting privacy are considered alongside the entity's interest in carrying out its activities or functions. This new requirement will help protect individuals when their personal information is used in complex data processing activities which have emerged through technological advancement, such as screen scraping and AI. OAIC guidance and enforcement through determinations and judicial consideration will map the contours of the fair and reasonable test over time. The Government **agrees in-principle** that the fair and reasonable test should apply irrespective of whether consent has been obtained, should not apply to the exceptions in APPs 3.4 and 6.2(b)–(e) and the reference to a 'fair means' of collection in APP 3.5 should be repealed (*proposal 12.3*).

This new test will also help to protect individuals from the use of 'dark patterns' which may nudge users towards consenting to more privacy intrusive practices. Dark patterns can also encourage users to choose more privacy intrusive settings. To address these concerns, the Government **agrees in-principle** that privacy settings for online services should reflect the 'privacy-by-default' framework of the Privacy Act, as determined by what is fair and reasonable in the circumstances, and be clear and easily accessible for users (*proposal 11.4*). Additional OAIC guidance will assist entities in understanding what is meant by privacy by default and how online settings should incorporate the Privacy Act's privacy by default requirement.

Security and destruction of personal information

Security and destruction of personal information are areas of increasing concern. This is driven by the volume of data being handled, the pace of technological advancement and the increasing prevalence of data breaches involving malicious or criminal attacks. The impact of recent significant data breaches affecting millions of Australians have been devastating. Almost half of the respondents to the 2023 ACAP survey had been directly impacted by a data breach in the 12 months prior to completing the survey, and three quarters of those said they had experienced some form of harm as a result. The significance of data breaches underscores the importance of privacy reforms which will reduce the amount of personal information being collected and held by entities.

The Government **agrees** the Privacy Act's existing security obligations should be enhanced by specifying that 'reasonable steps' in the context of APP 11 include both technical and organisational measures (*proposal 21.1*), and **agrees in-principle** that entities should be required to comply with a set of baseline privacy outcomes, aligned with relevant outcomes of the Government's 2023–2030 Australian Cyber Security Strategy (*proposal 21.2*).

The Government **agrees** the OAIC should provide additional guidance to entities about what reasonable steps an entity should take to keep personal information secure (*proposal 21.3*), and what reasonable steps an entity should take to destroy or de-identify personal information (*proposal 21.5*).

When entities hold personal information for longer than is necessary, 'honey pots' of valuable data are created which may increase the risk of the entity's information systems being compromised. In addition, there is increased risk that a greater number of individuals would be impacted in the event of a data breach. The Government **agrees in-principle** that entities should be required to establish their own maximum and minimum retention periods for personal information they hold (*proposal 21.7*) and specify these retention periods in privacy policies (*proposal 21.8*). Retention periods should take into account the type, sensitivity and purpose of the information being retained as well as the entity's organisational needs and any obligations they may have under other legal frameworks.

The Government **agrees in-principle** to review all legal provisions requiring retention of personal information, subject to further consultation across the Commonwealth and with states and territories to determine the appropriate scope and scale of such a review. This review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 (Cth) and the independent reviews and holistic reform of electronic surveillance legislative powers (*proposal 21.6*). In implementing this proposal, the Government will align the objectives of the review with relevant outcomes of the Government's 2023–2030 Cyber Security Strategy.

The Government **notes** the proposal to require entities to take reasonable steps to protect de-identified information (*proposal 21.4*) and will further consider how the policy intent of protecting against risks of re-identification may be achieved.

Notifiable data breaches scheme

The 2023 ACAP survey results indicated that the majority of Australians surveyed feel data breaches are one of the biggest privacy risks they face. The Review found that the NDB scheme has been generally effective in achieving its original policy objective of enabling individuals to protect themselves from the serious harm that may result from a data breach. However, with the increasing prevalence and scale of these breaches, there is a community expectation that entities should be better prepared to respond rapidly when a serious data breach has occurred and do more to assist individuals exposed to harm.

The Government **agrees in-principle** that entities should be required to (*proposal 28.2*):

- notify the Information Commissioner as soon as practicable, and not later than 72 hours, after becoming aware that there are reasonable grounds to believe there has been an eligible data breach, but will further explore appropriate timeframes with stakeholders and alignment with other relevant reporting frameworks,
- notify individuals as soon as practicable, including providing information to individuals in phases if it is not practicable to provide the information at the same time, and
- take reasonable steps to implement practices, procedures and systems to respond to a data breach.

The Government also **agrees in-principle** that entities should be required to set out the steps taken or to be taken in response to a data breach, including steps to reduce any adverse impacts on the individuals to whom the relevant information relates in their statement for an eligible data breach (*proposal 28.3*). Further consultation should be undertaken on whether entities should be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

The current provisions in the NDB scheme are heavily focused on the initial reporting and notification of a data breach. However, in light of recent large-scale data breaches, questions have been raised about whether the scheme needs to do more to facilitate the response to a breach. The Government **agrees** the Attorney-General should be able to permit the sharing of information with appropriate entities (such as banks) that may be able to reduce the risk of harm in the event of an eligible data breach – for specified purposes and for a limited time (*proposal 28.4*). This will support coordinated responses to future data breaches. Implementation of this proposal should take account of proposals related to enhancing the Act's emergency declaration powers (*proposals 5.3, 5.4 and 5.5*), which will also facilitate enhanced information-sharing in certain circumstances.

To ensure data breaches are reported correctly and that entities with multiple reporting obligations are not unnecessarily burdened, the Government **agrees** further consideration is necessary to determine how best to streamline multiple reporting obligations (*proposal 28.1*). Further consideration of proposal 28.1 will occur in conjunction with Government initiatives to enhance cyber security across the economy.

Organisational accountability

Organisational accountability requires entities to implement privacy management processes which reflect their responsibility for ongoing management of privacy risks. Organisational accountability measures can encourage the proactive mitigation of privacy-related risks and build community trust in the entity as a responsible steward of personal information. Feedback to the Review suggested further organisational accountability measures are needed to shift the emphasis from individuals being primarily responsible for self-managing their privacy onto entities.

The Government **agrees in-principle** that entities should be required to determine and record the purposes for which they will collect, use and disclose personal information at or before the time they collect it and record secondary purposes at or before the time of undertaking the secondary use or disclosure (*proposal 15.1*). Determining and recording the primary and secondary purposes for which personal information is collected, used and disclosed will assist entities with internal measures to assess the adequacy of current practices and comply with new obligations.

To improve information management governance processes and systems, the Government **agrees in-principle** that entities should be required to appoint or designate a senior employee as having specific responsibility for privacy within the organisation (*proposal 15.2*). The Government also **agrees in-principle** that entities should be required to take reasonable steps to ensure personal information collected by third parties was collected lawfully (*proposal 13.4*) in recognition of the concerns about the continued use and disclosure of personal information that was originally sourced from the perpetrator of a data breach. Further consideration will be given to how this requirement can be implemented without unduly restricting the ability of entities to perform their core functions and activities.

High privacy risk activities

There are certain types of personal information-handling that pose higher privacy risks to individuals. Feedback provided to the Review revealed a community expectation that high-risk practices should be subject to additional requirements under the Privacy Act. Ensuring Australia's regulatory settings which apply to new and emerging technologies are fit-for-purpose in the digital age is crucial to promote public trust and confidence in the adoption and ongoing use of these technologies. The Government **agrees** the OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks (*proposal 13.3*).

Commonwealth Government agencies are currently required to complete a Privacy Impact Assessment (PIA) for all high privacy risk projects. A PIA is a systematic assessment that identifies the impact that a project might have on the privacy of individuals and sets out recommendations for managing, minimising, or eliminating that impact. The Government **agrees in-principle** that non-government entities should also be required to conduct a PIA for activities with high privacy risks and that OAIC guidance should be developed on factors that may indicate a high privacy risk with examples of activities that will generally require a PIA to be completed (*proposal 13.1*). A PIA should be undertaken prior to the commencement of the high-risk activity and made available to the OAIC on request. The Government **agrees** that further consideration should be given to enhanced risk assessment requirements in the context of facial recognition technology and other uses of biometric information and that this work should be coordinated with the Government's ongoing work on Digital ID and the National Strategy for Identity Resilience (*proposal 13.2*).

Automated decision-making (ADM)

The safe and responsible development and deployment of automated decision-making (ADM) presents significant opportunities for enhancing productivity and facilitating economic growth, and improving outcomes for Australians across health, environment, defence and national security. ADM systems offer the potential to increase the efficiency, accuracy and consistency of decisions. However, feedback to the Review raised concerns about the transparency and integrity of decisions made using ADM systems.

The Government **agrees** that 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 and that 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 Privacy Act and supplemented by OAIC guidance (*proposals 19.1 and 19.2*). This could include decisions on denial of consequential services or support, such as financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities and health care services, or access to basic necessities such as food and water. Further consideration will be given to ensure that the parameters of 'substantially automated' are appropriately calibrated.

The Government also **agrees** that individuals should have a right to request meaningful information about how automated decisions with legal or similarly significant effect are made (*proposal 19.3*). The information provided to individuals should be jargon-free and comprehensible and should not reveal commercially sensitive information.

In relation to the proposals relating to ADM, the Government acknowledges the recommendations of the Royal Commission into the Robodebt Scheme in relation to the use of ADM by Commonwealth agencies. Consideration of how to best implement these reforms will occur as part of the Government's response to the Royal Commission, and work on Supporting Responsible AI in Australia being led by the Department of Industry, Science and Resources. Implementation should also consider the work being progressed by the Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts in response to recommendations in the House of Representatives Select Committee on Social Media and Online Safety report to understand the operation of algorithms on digital platforms. The work being conducted by the Digital Platform Regulators Forum on these issues should also be considered.

Direct marketing, targeting and trading

Since the introduction of the APPs, new privacy risks have emerged due to the use of high volumes of data to deliver targeted (or personalised) advertising and content on websites and apps. Entities yield revenue from user engagement with targeted content and advertising, which enables them to provide consumers with access to content or services for free or at a lower monetary cost. The trading of personal information underpins these activities.

The 2023 ACAP survey indicated that 88% of Australians consider online tracking, profiling and targeted advertising to vulnerable individuals (such as gambling companies targeting gamblers) and 87% of Australians considered that sale of personal information, or trading in personal information to not be fair and reasonable. 84% of Australians consider targeted advertising based on sensitive information (e.g. health information, racial or ethnic origin) to not be fair and reasonable and 69 % of Australians consider online tracking, profiling and targeted advertising to adults based on personal (but not sensitive) information to not be fair and reasonable.

There was strong support in submissions to the Report for distinguishing between more traditional forms of direct marketing such as email and SMS communications and the targeting of personalised content and advertising online. The Government **agrees in-principle** to defining direct marketing, targeted advertising, targeting and trading (*proposal 20.1*), noting the critical importance of refining the scope of these definitions through further consultation to ensure regulation effectively balances the protection of privacy of individuals and the public interest in protecting privacy and the interests of entities in carrying out their functions or activities. It is also important that interest-based advertising which relies on tracking the online behaviour of users over time is distinguished from other forms of advertising such as contextual advertising which is based on the content of the webpage a user views in real time.

Direct marketing

The Government **agrees in-principle** that individuals should have an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes (*proposal 20.2*), subject to refining the definition of direct marketing. Consideration will be given to how to best harmonise the requirements across the Privacy Act, *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth).

Targeting and trading

To address particular concerns about harmful targeting, the Government **agrees in-principle** that targeting should be subject to the following requirements (*proposal 20.8*):

- targeting individuals should be fair and reasonable in the circumstances, and
- targeting individuals based on sensitive information should be prohibited, with an exception for socially beneficial content.

These requirements would enable privacy harms associated with targeting to be addressed while ensuring targeting for socially beneficial purposes is not prevented, such as public health campaigns and preventing individuals from being exposed to harmful content. Further consideration will be given to how best to provide certainty in relation to what constitutes 'socially beneficial content' to assist entities in complying with these obligations.

The Government acknowledges the importance of individuals having more choice and control and **notes** that the proposal to provide individuals with an unqualified right to opt-out of receiving targeted advertising (*proposal 20.3*) is directed at this objective. Further consideration will be given to how to give individuals more choice and control in relation to the use of their information for targeted advertising, including layered opt-outs and industry codes which could specify how to give individuals more control over how their information is used in online advertising. Consideration will also be given to providing clarity on what is meant by 'targeted advertising' as distinct from 'targeted content'. To prevent individuals from losing control of their information, the Government **agrees in-principle** that an individual's consent should be required in order to trade their personal information (*proposal 20.4*), subject to refining the scope of what is considered to constitute 'trading'.

In order to provide individuals with greater awareness and understanding about how targeting systems work and why they are being targeted with certain advertising and content, the Government **agrees in-principle** that entities should provide information to online users about the use of targeting systems, including clear information about the use of algorithms and profiling to recommend content to individuals (*proposal 20.9*). This information will assist regulators to ensure compliance with the Privacy Act. Further consultation through the Government's work on Supporting Responsible AI in Australia being led by the Department of Industry, Science and Resources is required to inform the most effective way to implement this requirement to ensure individuals are provided with meaningful information. Implementation should also take into account the work being progressed by the Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts in response to recommendations in the House of Representatives Select Committee on Social Media and Online Safety report to understand the operation of algorithms on digital platforms. It should also consider the work being conducted by the Digital Platform Regulators Forum on these issues.

Children's privacy

Children are particularly vulnerable to online harms. Children increasingly rely on online platforms, social media, mobile applications and other internet connected devices in their everyday lives. While these services provide many benefits to children and young people, there is concern that children are increasingly being 'datafied', with thousands of data points being collected about them, including information about their activities, location, gender, interests, hobbies, moods, mental health and relationship status. The 2023 ACAP survey results showed that protecting their child's privacy is a major concern for 79% of Australian parents and the privacy of their children's personal information is of high importance to 91% of parents when deciding to provide their child with access to digital devices and service.

In light of these concerns, the Government **agrees** that a child should be defined in the Act as an individual who has not reached 18 years of age (*proposal 16.1*). The Government also **agrees in-principle** to the suite of proposed additional protections to apply specifically to children including that targeting to a child should be prohibited, with an exception for targeting that is in the best interests of the child (*proposal 20.6*).
This proposal recognises that a child's right to participate online should not be unduly limited, and there may be some circumstances where targeting is beneficial for children. This reform and any opt-out of targeted advertising which is implemented (*proposal 20.3*) would not prevent platforms from being able to undertake targeting to ensure content is in the best interests of the child, and prevent children from seeing age-sensitive advertisements.

To support the prohibition against targeting to children, the Government **agrees in-principle** that trading in the personal information of children should also be prohibited (*proposal 20.7*). While some forms of direct marketing are unlikely to cause harm, such as a person under 18 signing up for a mailing list to be notified about new products, privacy harms may arise when a person under 18 receives unsolicited marketing materials from a business they have not provided their personal information to or if they receive direct marketing a communication that advertises a harmful product. In response to these risks, the Government **agrees in-principle** that direct marketing to persons under 18 should be prohibited unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests (*proposal 20.5*).

The Government **agrees in-principle** that entities should be required 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 (*proposal 16.4*). The best interests of the child have to be balanced against other interests, including other children. Where it is not reasonable to undertake an assessment of the best interests of an individual child, the best interests may be assessed for the relevant group of children.

To clarify how the best interests of the child should be upheld in the design of online services, and provide further guidance on how entities are expected to meet requirements regarding targeting, direct marketing and trading, the Government **agrees** a Children's Online Privacy code should be developed (*proposal 16.5*) as soon as legislated protections for children are enacted to enable the development of such an APP code. The code would apply to online services that are likely to be accessed by children. To the extent possible, the scope of the code should align with international approaches, including the UK Age Appropriate Design Code, with similar exemptions for particular entities such as counselling services. The code developer should consult broadly with children, parents, child development experts, child welfare advocates and industry in developing the code.

Entities should continue to rely on existing OAIC guidance on children and young people and capacity should continue to be relied upon by entities but to ensure the guidance is more readily enforceable, the Government **agrees in-principle** that the Privacy Act should codify the principle that valid consent must be given with capacity (*proposal 16.2*). It is crucial that there are exceptions for circumstances where a parent's or guardian's involvement in capacity decisions could be harmful to the child or otherwise contrary to their interests.
The guidance provides sufficient flexibility by allowing entities to decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, as a general rule, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

To support children's understanding of potential privacy and safety issues which may flow from certain types of personal information-handling, the Government **agrees in-principle** that entities should be required to provide privacy notices and policies that are clear and understandable for any information addressed specifically to a child (*proposal 16.3*).

To meet requirements in relation to children, it is expected that entities will need to take reasonable steps to establish an individual's age with a level of certainty that is appropriate to the risks, for example by implementing age assurance. Age assurance is an umbrella term which includes both age verification and age estimation solutions. Age verification measures determine a person's age to a high level of certainty, while age estimation technologies provide an approximate age or age range.

People experiencing vulnerability

To provide additional protections for individuals who may be experiencing vulnerability or may be at higher risk, the Government **agrees** OAIC guidance should include:

- 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 (*proposal 17.1*), and
- updated information on capacity and consent to reflect developments in supported decision-making (*proposal 17.2*).

The Government recognises that this would consider how to ensure protections where a person is at risk being subject to adverse treatment, or impeded in accessing products or services, because of their membership of a particular group, or their safety may be at risk – such as for people experiencing domestic and family violence. Entities would not be obliged to collect additional information to establish if someone is experiencing vulnerability.

In response to specific concerns that were raised about the ability for entities to use or disclose personal information to provide extra care with customers who are experiencing vulnerability, the Government **agrees in-principle** further consultation should be undertaken to identify options to ensure financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent (*proposal 17.3*).

3. Increase clarity and simplicity for entities and individuals

Businesses need a privacy regime that allows them to take advantage of the economic opportunities presented by emerging technologies. Amending the Act to provide greater clarity and simplicity to regulated entities about how to protect personal information will give businesses confidence to adopt and develop new technologies.

Clarifying terms

To improve clarity of the Privacy Act, the Government **agrees in-principle** that the following definitions should be introduced or amended:

Collection	captures information obtained from any sources and by any means, including inferred or generated information (*proposal 4.3*)
Disclosure	occurs when an entity makes information accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control (*proposal 23.6*)
Geolocation tracking data	personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time (*proposal 4.10*)
De-identified	amended to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context (*proposal 4.5*)
Consent	amended to provide that it must be voluntary, informed, current, specific and unambiguous (*proposal 11.1*)

Simplifying obligations

Submissions highlighted the problematic nature of compliance with the Privacy Act for entities which process personal information on the direction of another entity. Complexity and regulatory burden for entities acting as 'processors' would likely increase following reforms proposed in the Report. To recognise that different entities have differing degrees of control over the handling of personal information, the Government **agrees in-principle** that a distinction between controllers and processors of personal information should be introduced into the Privacy Act (*proposal 22.1*). This will bring Australia into line with other jurisdictions, reflect the operational reality of modern business relationships, and reduce the compliance burden for entities acting as processors.

Increasing flexibility

Submissions to the Review generally supported the current principles-based nature of the Privacy Act and suggested the APPs should be supplemented with more detailed prescription where required. More detailed prescriptions are often provided through APP codes, which can also impose additional requirements, so long as the requirements are not contrary to, or inconsistent with, the APPs.

The Government **agrees** that the ability for the Information Commissioner to make an APP code on the direction or approval of the Attorney-General should be enhanced (*proposals 5.1 and 5.2*). This will enable the Information Commissioner to respond in circumstances where it is in the public interest for a code to be developed and there is unlikely to be an appropriate industry representative to develop the code or it is urgently required.

The current emergency declaration provisions are very broad and can make it challenging to balance the need to protect the privacy of individuals with the need to share personal information when responding to emergencies and disasters. The Government **agrees** the provisions relating to emergency declarations should be amended to allow emergency declarations to be targeted to certain entities or classes of entities, classes of personal information and acts and practices, or types of acts and practices, and to ensure that emergency declarations are able to be made in relation to ongoing emergencies (*proposals 5.3 and 5.4*). The Government also **agrees** to permitting private sector organisations to disclose information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth, subject to further consultation with states and territories on their legislative frameworks and implications for their agencies (*proposal 5.5*).

Reducing inconsistency

The Privacy Act is one piece of legislation in a broader digital and data regulatory framework. There are a number of other legislative provisions (at both the Commonwealth and state and territory level) that authorise the handling of personal information. In order to reduce complexity and compliance costs, the Privacy Act should provide a baseline set of protections that are interoperable with other frameworks that deal with the handling of personal information. To reduce inconsistencies and guide coherence, the Government **agrees in-principle** the Attorney-General's Department should develop a law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations (*proposal 29.1*). The Government also **agrees in-principle** that a working group should be convened to work towards harmonising key elements of Commonwealth and state and territory privacy laws, with the forward work agenda for the working group subject to agreement with states and territories (*proposal 29.3*). Opportunities for harmonisation of Commonwealth laws that regulate the handling of personal information should also be considered as part of implementing reforms to the Privacy Act.

Facilitating overseas data flows

The free flow of information across borders is an increasingly important component of international trade and digital service models. While information data flows are critical to economic growth, concerns about the privacy risks of international data transfers continue to grow. To support the free flow of information with appropriate protections, the Government **agrees** a mechanism should be introduced to prescribe countries with substantially similar privacy laws (*proposal 23.2*). This will allow businesses to disclose personal information to recipients in prescribed countries without the need for contractual provisions or other measures. The Government **agrees in-principle** standard contractual clauses for transferring personal information to countries that are not prescribed should be developed and made available to businesses (*proposal 23.3*). Standard contractual clauses would be voluntary for businesses to use and should be interoperable with those developed by other jurisdictions where possible.

For circumstances where information is being disclosed to a non-prescribed country and the use of standard contractual clauses to ensure the overseas recipient does not breach the APPs is not appropriate, the Government considers that entities should be able to continue to rely on the existing informed consent exception. The Government **agrees in-principle** that this provision should be strengthened (*proposal 23.4*) so that entities consider risks associated with disclosing personal information to an overseas recipient (which may include consideration of the sensitivity and volume of personal information being disclosed) and whether other mechanisms could facilitate the disclosure. This would help to ensure entities do not rely on the consent exception by default. However, consideration should be given to whether the fair and reasonable test may achieve this aim while providing entities with sufficient flexibility.

The Government **agrees in-principle** that entities should be required, when specifying the countries in which recipients of overseas disclosures are likely to be located in APP 5 notices, to also specify the types of personal information that may be disclosed (*proposal 23.5*). This will provide greater transparency to individuals. Consideration will be given to whether this enhanced notice requirement should apply to all disclosures of personal information or be limited to disclosures that rely on the informed consent exception. The Government **agrees** further consultation should be undertaken on the extraterritorial provisions of the Privacy Act to determine if an additional requirement that personal information is connected to Australia is necessary to narrow the current scope (*proposal 23.1*).

4. Improve transparency and control

Currently, individuals are provided limited transparency and control over their personal information through privacy notices, privacy policies and limited access rights. Feedback to the Review demonstrated a community expectation that individuals should be able to access meaningful information about how their personal information is handled and have the ability to exert greater control over personal information that is held about them. The 2023 ACAP survey results showed that 84% of Australians want more control over the collection and use of their personal information. The results also showed a strong desire for transparency around how and why personal information is being collected, held and disclosed.

Consent

An over-reliance on consent can place an unrealistic burden on individuals to understand the risks of information-handling practices and may not result in improved privacy outcomes. The Government notes feedback to the Review consistently emphasised concerns about increasing consent requirements on the basis that consent is ineffective when it is overused. Where individuals are provided with a large volume of consent requests they are less likely to meaningfully engage with these requests.

Unless an exception applies, consent is currently only required to collect sensitive information. Consent can also be relied on as a basis to use or disclose personal information for a secondary purpose and to disclose information overseas. Reserving consent for high privacy risk situations reduces the risk of individuals experiencing consent fatigue and avoids placing an unnecessary compliance burden on entities to obtain consent in situations where a collection, use or disclosure of personal information would be reasonably expected by the individual or broader community.

To improve the quality of consent provided in these circumstances, the Government **agrees in-principle** that the Act should clarify that consent should be voluntary, informed, current, specific and unambiguous (*proposal 11.1*). The Government also **agrees in-principle** that the Act should expressly recognise the ability for individuals to withdraw consent in an easily accessible manner (*proposal 11.3*). To provide clarity on these requirements in online contexts, the Government **agrees in-principle** entities should be provided with OAIC guidance on how online services can design consent requests (*proposal 11.2*).

The Government recognises that the changes to consent may present challenges for research organisations conducting research in the public interest. The Government **agrees** that researchers should also be able to rely on 'broad consent' due to difficulties in obtaining 'specific' consent from individuals in research contexts (*proposal 14.1*). The Government **agrees** further consultation should be undertaken on expanding the scope of the Act's exceptions from requiring consent in research contexts to apply to human research generally that is in the public interest, and on agencies and organisations being covered by a single research exception and set of guidelines developed by the Privacy Commissioner in consultation with relevant stakeholders (*proposals 14.2 and 14.3*).

Privacy policies and collection notices

Privacy policies and collection notices are intended to provide individuals with transparency over personal information practices. Feedback to the Review revealed concerns that privacy policies and collection notices are often complex, lengthy, legalistic and vague. This can undermine individuals' understanding of how their personal information will be handled. The Government **agrees in-principle** that privacy notices should be clear, up-to-date, concise and understandable, with appropriate accessibility measures in place (*proposal 10.1*). To support entities to meet this requirement, the Government **agrees in-principle** standardised templates for privacy policies and privacy notices should be developed for voluntary adoption by entities (*proposal 10.3*). This could include standardised icons, layouts and phrases to better support consumers to make quick and informed decisions. In order to ensure privacy notices inform individuals of relevant information following the implementation of privacy reforms, the Government **agrees in-principle** that collection notices should also specify if information is collected, used or disclosed for high privacy risk activities, how to exercise individual rights and the types of personal information that may be disclosed to overseas recipients (*proposal 10.2*).

Individual rights

Individuals currently have a right to access the personal information that an entity holds about them and to request the correction of information held about them. If an entity is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the entity must take reasonable steps to correct the information. However, at present individuals are not able to request information about how their information is being used or request that their information be deleted.

The Review proposed that the rights which individuals currently have in relation to their personal information be expanded to include additional rights in order to enhance transparency and control for individuals. The 2023 ACAP survey results showed that almost all Australians think they should have additional rights under the Act, including the right to ask a business to delete their personal information (90%); ask a government agency to delete their personal information (79%) and object to certain data practices while still being able to access and use the service (90%). The Government **agrees in-principle** that individuals should have greater transparency and control over their personal information through the creation of new individual rights which would enable them to:

- request an explanation of what personal information is held and what is being done with it through an enhanced right to access (*proposal 18.1*)
- challenge the information handling practices of an entity and require the entity to justify how its information-handling practices comply with the Act (*proposal 18.2*)
- require an entity to delete (or de-identify) personal information through a right to erasure (*proposal 18.3*)
- request correction of online publications over which an entity has control (*proposal 18.4*), and
- require search engines to de-index certain online search results (*proposal 18.5*).

The Government acknowledges concerns expressed by many stakeholders during the Review regarding the potential for expanded individual rights to be burdensome and further consideration will be given to the scope and application of these rights in light of stakeholder feedback.

The Government **agrees in-principle** that these rights should be subject to exceptions (*proposal 18.6*). Exceptions should apply where complying with a request would be contrary to public interests, for example freedom of expression and law enforcement activities. An evaluative exercise would be required when balancing the interests. Exceptions should also apply in circumstances involving legal relationships and legal or related proceedings (such as where complying with a request would be inconsistent with another law or a contract with the individual), and where a request is technically impossible or unreasonable, or a request if frivolous or vexatious. In addition to the general exceptions for rights of the individual, the Government **agrees in-principle** to including specific exceptions to the right of erasure for law enforcement and national security (*proposal 18.3*). The design of exceptions would also need to consider existing exceptions under APPs 12 and 13.

The Government **agrees in-principle** that individuals should be notified about their rights and how to exercise them at the point of collection, and that privacy policies of entities set out procedures for responding to requests (*proposal 18.7*). The Government also **agrees in-principle** that, when responding to a request, entities should:

- acknowledge receipt of the request within a reasonable time and provide a timeframe for responding (*proposal 18.10*)
- provide reasonable assistance to individuals (*proposal 18.8*), and
- take reasonable steps to respond to a request (*proposal 18.9*).

The Government further **agrees in-principle** that where an entity refused a request, it would need to provide an explanation for why it was refusing the request and information on how the individual could lodge a complaint regarding the refusal with the OAIC (*proposal 18.9*).

Ability for individuals to seek redress for interferences with privacy

Individuals have limited avenues to seek redress for interferences with their privacy. Empowering individuals to litigate claims directly would enhance the control people have over their personal information. The 2023 ACAP survey results showed that 89% of Australians believe they should be able to seek compensation in the courts for a breach of privacy.

Direct right of action

The Government **agrees in-principle** that individuals should have more direct access to the courts to seek remedies for breaches of the Act through a direct right of action (*proposal 26.1*). A direct right of action would increase the avenues available to individuals who suffer loss or damage as a result of an interference with privacy to seek compensation. Such a right would be an important measure to enhance individuals' control over their personal information.

To encourage early resolution and minimise the burden on the courts, an individual would need to first lodge a complaint with the OAIC or a recognised External Dispute Resolution scheme. Where there was no reasonable likelihood that a complaint could be resolved by conciliation or a complaint was assessed as unsuitable for conciliation, the complainant would have the option to pursue the matter further in court. The remedies available would be any order the court sees fit, including any amount of damages.

Statutory tort for serious invasions of privacy

At present, there is no recourse for Australians whose privacy is invaded in circumstances which fall outside the scope of the Act. The Government **agrees in-principle** that a statutory tort for serious invasions of privacy should be introduced, based on the model recommended by the ALRC in its Report 123 (*proposal 27.1*). The invasion of privacy would need to be either a serious intrusion into seclusion or a serious misuse of private information. A plaintiff bringing a cause of action should be required to prove:

- the privacy invasion was serious,
- they had a reasonable expectation of privacy,
- that the invasion was committed intentionally or recklessly (not merely negligently), and that
- the public interest in privacy outweighs any countervailing public interest.

A statutory tort for serious invasions of privacy would provide people with the ability to seek redress through the courts for serious invasions of privacy without being limited by the scope of the Act. For example, an individual taking a video of a person where they had a reasonable expectation of privacy (such as in a public bathroom) or an employee misusing sensitive facts about another employee obtained by virtue of their position. While it is possible that an action in the statutory tort would have an overlap with existing legal remedies (such as state-based surveillance laws), these laws usually focus on punishment of the offender and not compensation to the victim. In recognition of the concerns about the balance of prevailing laws adversely impacting public interest journalism and the need to protect public interest journalism, further consultation with media organisations on additional safeguards for public interest journalism should be undertaken when implementing this reform. Consultation should also be undertaken with states and territories on potential implications for state and territory courts and agencies.

5. Strengthen enforcement

Effective enforcement of the Act is essential to protecting the privacy of individuals. The intersection between privacy and digital technologies has seen enforcement action in relation to personal information handling practices taken by regulators other than the OAIC. The Government **agrees** that regulators should continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information, and in this regard notes the ongoing work being conducted by the Digital Platform Regulators Forum (*proposal 29.2*).

To ensure the OAIC can take appropriate action for interferences with privacy, the Government **agrees** section 13G of the Privacy Act which deals with 'serious or repeated' breaches of privacy should be amended to remove the word 'repeated' and clarify that a 'serious' inference can include repeated interferences with privacy (*proposal 25.2*). The Government **agrees** a new mid-tier civil penalty provision should be introduced to cover interferences with privacy which do not meet the threshold of being 'serious' and a new low-level civil penalty provision for specific administrative breaches of the Act and APPs should be introduced with attached infringement notice powers for the Information Commissioner with set penalties (*proposal 25.1*).
The Government also **agrees** that the Federal Court and the Federal Circuit and Family Court of Australia should be given the power to make any order they see fit after a civil penalty relating to an interference with privacy has been established (*proposal 25.6*). The Government **agrees** entities should be required to identify, mitigate and redress actual or foreseeable loss suffered by an individual (*proposal 25.5*). The OAIC should publish guidance on how entities can achieve this.

To ensure the ongoing effectiveness of the OAIC, the Government **agrees**:

- the OAIC should conduct a strategic organisational review to ensure the OAIC is structured to have a greater enforcement focus (*proposal 25.10*)
- the annual reporting requirements in the Australian Information Commissioner Act 2010 should be amended to increase transparency about the outcome of all complaints lodged including the number of complaints dismissed under each ground (*proposal 25.9*), and
- the Information Commissioner should have the discretion not to investigate complaints where it has already been adequately dealt with by an external dispute resolution scheme (*proposal 25.11*).

To ensure the OAIC is resourced sustainably, the Government **agrees in-principle** that further work should be done to investigate the feasibility of an industry funding model for the OAIC (*proposal 25.7*) and further consideration be given to establishing a contingency litigation fund for costs orders against the OAIC, and an enforcement special account to fund high cost litigation (*proposal 25.8*). These reforms will be complemented by a strategic assessment of the OAIC, which will include consideration of its resourcing requirements.

Effective information-gathering powers are essential to developing a case that ensures successful regulatory outcomes. The Information Commissioner's current power to enter premises is inadequate and inconsistent with comparable domestic and international regulators. The Government **agrees** the Information Commissioner should be provided with:

- additional powers for investigations of civil penalty provisions (*proposal 25.3*), and
- the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General (*proposal 25.4*).

Effectiveness of the Review

To ensure the continued effectiveness of Australia's privacy framework, the Government **agrees in-principle** that a statutory review of amendments to the Act will be commenced within three years of the commencement of the amendments (*proposal 30.1*).

Attachment A – List of Government responses to proposals

Proposals	Government Response
Chapter 3: Objects of the Act	
Proposal 3.1 Amend the objects of the Act to clarify that the Act is about the protection of personal information.	Agree
Proposal 3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.	Agree
Chapter 4: Personal information, de-identification and sensitive information	
Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.	Agree in-principle
Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.	Agree in-principle
Proposal 4.3 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.	Agree in-principle
Proposal 4.4 '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.	Agree in-principle
Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.	Agree in-principle
Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information: (a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure. (b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Princi ples in relation to de-identified information, including ensuring that the receiving entity does not reidentify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification. (c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.	Notes

Proposals	Government Response
Proposal 4.7 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.	Agree
Proposal 4.8 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. In addition, the prohibition should not apply where: (a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way. (b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information.	Notes
Proposal 4.9 Sensitive Information (a) Amend the definition of sensitive information to include 'genomic' information. (b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act. (c) Clarify that sensitive information can be inferred from information which is not sensitive information	Agree in-principle
Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.	Agree in-principle
Chapter 5: Flexibility of the APPs	
Proposal 5.1 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: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code. In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.	Agree
Proposal 5.2 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.	Agree

Proposals	Government Response
Proposal 5.3 Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to: (a) entities, or classes of entity (b) classes of personal information, and (c) acts and practices, or types of acts and practice.	Agree
Proposal 5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.	Agree
Proposal 5.5 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.	Agree
Chapter 6: Small business exemption	
Proposal 6.1 Remove the small business exemption, but only after: (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations.	Agree in-principle
Proposal 6.2 In the short term: (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.	Agree in-principle

Proposals	Government Response
Chapter 7: Employee Records Exemption	
Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of: (a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for (b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information (c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and (d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. 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. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.	Agree in-principle
Chapter 8: Political Exemption	
Proposal 8.1 Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.	Notes
Proposal 8.2 Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.	Notes
Proposal 8.3 The political exemption should be subject to the following requirements: (a) Political acts and practices covered by the exemption must be fair and reasonable. (b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union. The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108.	Notes

Proposals	Government Response
Proposal 8.4 The political exemption should be subject to a requirement that individuals must be provided with the means to: (a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and (b) opt-out of receiving targeted advertising from a political entity.	Notes
Proposal 8.5 The political exemption should be subject to a requirement that political entities must: (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.	Notes
Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.	Notes
Chapter 9: Journalism Exemption	
Proposal 9.1 To benefit from the journalism exemption a media organisation must be subject to: (a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), or (b) standards that adequately deal with privacy.	Agree
Proposal 9.2 In consultation with industry, and the ACMA, 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.	Agree in-principle
Proposal 9.3 An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force.	Agree in-principle
Proposal 9.4 Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.	Agree in-principle
Proposal 9.5 Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.	Agree in-principle

Proposals	Government Response
Chapter 10: Privacy policies and collection notices	
Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.	Agree in-principle
Proposal 10.2 The list of matters in APP 5.2 should be retained. 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. The following new matters should be included in an APP 5 collection notice: (a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.	Agree in-principle
Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	Agree in-principle
Chapter 11: Consent and privacy default settings	
Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.	Agree in-principle
Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.	Agree in-principle
Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	Agree in-principle
Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.	Agree in-principle

Proposals	Government Response
Chapter 12: Fair and reasonable personal information handling	
Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.	Agree in-principle
Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (b) the kind, sensitivity and amount of personal information being collected, used or disclosed (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) 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, and (g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and (c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.	Agree in-principle
Proposal 12.3 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. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.	Agree in-principle

Proposals	Government Response
Chapter 13. Additional protections	
Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.	Agree in-principle
Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.	Agree
Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.	Agree
Proposal 13.4 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. OAIC guidelines could provide examples of reasonable steps that could be taken.	Agree in-principle
Chapter 14: Research	
Proposal 14.1 Broad consent for research Introduce a legislative provision that permits broad consent for the purposes of research: (a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply. (b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.	Agree
Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.	Agree

Proposals	Government Response
Proposal 14.3 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.	Agree
Chapter 15: Organisational Accountability	
Proposal 15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.	Agree in-principle
Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.	Agree in-principle
Chapter 16: Children	
Proposal 16.1 Define a child as an individual who has not reached 18 years of age.	Agree
Proposal 16.2 Existing OAIC guidance on children and young people and capacity15 should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise. The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).	Agree in-principle
Proposal 16.3 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. In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.	Agree in-principle
Proposal 16.4 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.	Agree in-principle

Proposals	Government Response
Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services. The code developer should be required to consult broadly with children, parents, child development experts, child welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted. The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.	Agree
Chapter 17: People experiencing vulnerability	
Proposal 17.1 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.	Agree
Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.	Agree
Proposal 17.3 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.	Agree in-principle
Chapter 18: Rights of the individual	
Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features: (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act) (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual.	Agree in-principle
Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.	Agree in-principle

Proposals	Government Response
Proposal 18.3 Introduce a right to erasure with the following features: (a) An individual may seek to exercise the right to erasure for any of their personal information. (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.	Agree in-principle
Proposal 18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.	Agree in-principle
Proposal 18.5 Introduce a right to de-index online search results containing personal information which is: (a) sensitive information [e.g. medical history], or (b) information about a child, or (c) excessively detailed [e.g. home address and personal phone number], or (d) inaccurate, out-of-date, incomplete, irrelevant, or misleading. The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.	Agree in-principle
Proposal 18.6 Introduce relevant exceptions to all rights of the individual based on the following categories: (a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. (b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual. (c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.	Agree in-principle
Proposal 18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.	Agree in-principle
Proposal 18.8 An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.	Agree in-principle
Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.	Agree in-principle

Proposals	Government Response
Proposal 18.10 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. An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	Agree in-principle
Chapter 19: Automated decision-making	
Proposal 19.1 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.	Agree
Proposal 19.2 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. This should be supplemented by OAIC Guidance.	Agree
Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	Agree
Chapter 20: Direct marketing, targeting and trading	
Proposal 20.1 Amend the Act to introduce definitions for: (a) Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material. (b) Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class). (c) Trading – capture the disclosure of personal information for a benefit, service or advantage.	Agree in-principle
Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.	Agree in-principle

Proposals	Government Response
Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.	Notes
Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.	Agree in-principle
Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.	Agree in-principle
Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.	Agree in-principle
Proposal 20.7 Prohibit trading in the personal information of children.	Agree in-principle
Proposal 20.8 Amend the Act to introduce the following requirements: (a) Targeting individuals should be fair and reasonable in the circumstances. (b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.	Agree in-principle
Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	Agree in-principle
Chapter 21: Security, retention and destruction	
Proposal 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.	Agree
Proposal 21.2 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.	Agree in-principle
Proposal 21.3 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.	Agree
Proposal 21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.	Notes

Proposals	Government Response
Proposal 21.5 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	Agree
Proposal 21.6 The Commonwealth should undertake a review of all legal provisions that require 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. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial. However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers.	Agree in-principle
Proposal 21.7 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. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.	Agree in-principle
Proposal 21.8 Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.	Agree in-principle
Chapter 22: Controllers and processors of personal information	
Proposal 22.1 Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, 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. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.	Agree in-principle
Chapter 23: Overseas data flows	
Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.	Agree
Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).	Agree
Proposal 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.	Agree in-principle

Proposals	Government Response
Proposal 23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.	Agree in-principle
Proposal 23.5 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	Agree in-principle
Proposal 23.6 Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.	Agree in-principle
Chapter 24: Cross-Border Privacy Rules and domestic certification	
Nil	
Chapter 25: Enforcement	
Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses: (a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision. (b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties	Agree
Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature (b) those adversely affecting large groups of individuals (c) those impacting people experiencing vulnerability (d) repeated breaches (e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data. The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.	Agree
Proposal 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.	Agree

Proposals	Government Response
Proposal 25.4 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	Agree
Proposal 25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals. The OAIC should publish guidance on how entities could achieve this.	Agree
Proposal 25.6 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.	Agree
Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.	Agree in-principle
Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.	Agree in-principle
Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Agree
Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Agree
Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.	Agree
Chapter 26: A direct right of action	
Proposal 26.1 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. The model should incorporate the appropriate design elements discussed in this chapter.	Agree in-principle
Chapter 27. A statutory tort for serious invasions of privacy	
Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.	Agree in-principle

Proposals	Government Response
Chapter 28: Notifiable data breaches scheme	
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	Agree
Proposal 28.2 (a) Amend paragraph 26WK(2)(b) to provide that 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 as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable. (c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.	Agree in-principle
Proposal 28.3 Amend subsections 26WK(3) and 26WR(4) to the effect that 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, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates. However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information. Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.	Agree in-principle
Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	Agree
Chapter 29: Interactions with other schemes	
Proposal 29.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.	Agree in-principle
Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.	Agree

Proposals	Government Response
Proposal 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.	Agree in-principle
Chapter 30: Further review	
Proposal 30.1 Conduct 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.	Agree in-principle