www.accan.org.au
info@accan.org.au
02 9288 4000

Submission

March 2023

Privacy Act Review Issues Paper

Submission by the Australian Communications Consumer Action Network (ACCAN) to the Attorney General's Department

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

PO Box A1158
Sydney South NSW 1235
Email: info@accan.org.au
Phone: (02) 9288 4000
Contact us through the National Relay Service

Contents

Introduction

ACCAN welcomes the opportunity to respond to the Attorney-General's consultation on the Government response to the Privacy Act Review Report. We are pleased to note that the proposals put forward in the Discussion Paper positively reflect many of the positions we voiced in our earlier submissions to previous Privacy Act review consultations.

Currently, the information and power asymmetries between consumers and digital platforms can make it challenging for individuals to make informed decisions about how personal information is handled online.[1] Thus it is critical that Australia's Privacy Act provide clarity to both entities that collect personal information and individuals about how personal information is to be collected, used and protected.

Response to Discussion Paper proposals

Part 1: Scope and application of the Privacy Act

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. **Proposal 3.2** Amend the objects of the Act to recognise the public interest in protecting privacy.

ACCAN supports the two proposals put forward in the Discussion Paper (proposals 3.1 and 3.2). In our earlier submissions to the Privacy Act review, we argued that the objective of section 2a to protect individual privacy was often being overridden by the interests of entities and the increasing amount of individual's data being collected limited the ability of the Act to appropriately protect individuals.[2]

ACCAN expects that these amendments to the Act will empower greater protection of individual's data. Moreover, highlighting in the Act that data protection is in the public interest will alleviate potential distrust by consumers.

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. **Proposal 4.2** Include a non-exhaustive list of information which may be personal information to assist Australian Privacy Principle (**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.

[1] Falk, Angelene, '2020 Vision: Challenges and opportunities for privacy regulation', 29 October 2019, www.oaic.gov.au/updates/speeches/2020-vision-challenges-and-opportunities-for-privacy-regulation/

[2] ACCAN, 2022, *Submission to the Privacy Act review*, https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation.

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.
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.
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.
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 Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify 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.

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.
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.

Proposal 4.9

(a) Amend the definition of sensitive information to include 'genomic' information.
(a) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.
(b) Clarify that sensitive information can be inferred from information which is not sensitive information.

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.

ACCAN supports the adoption of proposals 4.1 - 4.10. Implementing these proposals in the Act will help to clarify for both consumers and business exactly what is considered 'personal information'. Amending the definitions of 'collection' (proposal 4.3) and 'de-identified' (proposal 4.5) are significant improvements in clarifying how the collection of data and the de-identification of data need to be considered in the context of data privacy.

Whilst ACCAN did not endorse the re-introduction of the *Privacy Amendment (Re-identification) Offence Bill 2016* in our previous feedback,[3] ACCAN supports proposal 4.7, consultation on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit with appropriate exceptions.

Flexibility of the APPs

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.

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.

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 practices.

Proposal 5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 5.1 – 5.5). Our position that any industry Code will have better outcomes when consumer input is included throughout the development process has not changed. However, ACCAN acknowledges that with the inclusion of an extended 40-day public consultation period in proposals 4.1 and 4.2 there will be an opportunity for consumer input and public scrutiny of any potential over-reach.

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

[3] Ibid.

(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.

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.

ACCAN has previously advocated that the Small Business exemption should be removed.[4] As is outlined in the Discussion Paper, the exemption was implemented in 2000, in the intervening decades, consumer data collection by businesses of all size has exponentially increased. Thus, the rationale for a Small Business exemption is no longer appropriate. ACCAN supports the proposals put forward in the Discussion Paper (proposals 6.1 and 6.2), however ACCAN recommends that a timeframe be included in proposal 6.1 to ensure that the public interest objective of the Act is maintained with the least delay.

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.

ACCAN has previously advocated for the Employee Records exemption to be removed.[5] As such, we support proposal 7.1.

[4] Ibid.
[5] Ibid.

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.
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.
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.
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.

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.

Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.

ACCAN has previously advocated for the removal of the Political exemption from the Act. Considering the proposals put forward in the Discussion Paper (proposals 8.1 – 8.6), ACCAN is not convinced that there is any public value in retaining the Political Exemption in the Privacy Act. As noted in ACCAN's earlier feedback to earlier Privacy Act reviews, removing this exemption will bring Australia in-line with other democratic nations which require political parties to abide with their respective privacy regulations.[6]

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.

[6] Ibid.

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.
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.
Proposal 9.4 Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.
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.

As stated in ACCAN's earlier feedback to Privacy Act reviews, ACCAN has not previously taken a position on the Journalism Exemption.[7] However, ACCAN supports the proposals put forward in the Discussion Paper (proposals 9.1 – 9.5). ACCAN considers that implementing these proposals in the Act will provide an appropriate balance between privacy and the public interest value of journalism.

Part 2: Protections

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.
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.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 10.1 – 10.3). In our previous submissions to Privacy Act consultations, we have commented that providing consumers clear and easy to understand information about the collection of their personal data will have beneficial outcomes for both consumers and business.[8] Informed consumers can make better

[7] Ibid.
[8] Ibid.

choices about how they interact with services and business which in turn will lead to more competitive markets.

Consent and online privacy settings

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.
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.
Proposal 11.3 Expressly recognize 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.
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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 11.1 – 11.4). In our earlier submission to the Privacy Act review we made the following recommendation:

> Recommendation 3: Organisations should provide consumers with brief and easily understandable privacy notices when requesting consent to data collection.[9]

ACCAN is particularly pleased to see the inclusion of Proposal 11.3, a Right to Withdraw Consent. ACCAN expects that consumers should always have the choice to change permissions and providing a Right to Withdraw Consent will provide greater levels of consumer trust.

Fair and reasonable test

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.
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

[9] ACCAN, 2021, *ACCAN Submission to Privacy Act Review Issues Paper Consultation.* https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

(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.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 12.1 – 12.3). Amending the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances (proposal 12.1) will assist in alleviating consumer concerns of over-collection of their data.

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.

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.

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.

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.

In principle ACCAN supports the proposals put forward in the Discussion Paper (proposals 13.1 – 13.4). However, should these proposals be implemented in the Act it will be critical that ongoing and timely review of what constitutes a high-risk activity be conducted by the OAIC. Additionally, the recommendation in proposal 13.2 that consideration of enhanced risk assessment requirements for bio-metric technologies be considered as part of a broader Government review of regulating biometric technologies must include broad community consultation.

Research

Proposal 14.1 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.

Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.

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.

In principle, ACCAN supports the proposals put forward in the Discussion Paper (proposals 14.1 – 14.3). However, ACCAN's support of proposals 14.2 and 14.3 is contingent on the inclusion of broad community consultation in the development of these two proposals.

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.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 15.1 and 15.2). In our earlier comments to Privacy Act consultations, we have strongly emphasised the need for consumers to be made aware of when and for what purpose their data is being collected.[10]

Children's privacy

Proposal 16.1 Define a child as an individual who has not reached 18 years of age.

[10] Ibid.

Proposal 16.2 Existing OAIC guidance on children and young people and capacity[11] 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).
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.
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.
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.

ACCAN in principle supports the proposals put forward in the Discussion Paper (proposals 16.1 – 16.4). However, proposal 16.4 needs to be strengthened. ACCAN considers the phrase 'have regard to' as being too vague as to have any real impact. This proposal would be stronger if it was re-phrased to ensure that the interest of the child was paramount in the consideration of data collection.

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.
Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.

[11] Office of the Australian Information Commissioner (**OAIC**), *APP Guidelines (July 2019*), [B.55]–[B.61], https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 17.1 – 17.3). Consideration of an individual's circumstances at times of vulnerability is key in ensuring consumer protection and fairness.

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

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.

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.

Proposal 18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.

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.

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.

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.
Proposal 18.8 An APP entity must provide *reasonable assistance* to individuals to assist in the exercise of their rights under the Act.
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.
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.

ACCAN supports the proposals put forward in the Discussion Paper relating to Access and Explanation (proposal 18.1), Objection (proposal 18.2), Erasure (proposal 18.3) and Correction (proposal 18.4). These amendments to the Act will provide greater fairness which in turn will potentially lead to greater consumer confidence when entities collect their personal information. Additionally, implementing these proposals will bring the Act closer in line with Article 17 of the General Data Protection Regulation (**GDPR**). The GDPR's exceptions to the right to erasure are driven by public interest imperatives.

ACCAN also supports the additional proposals put forward in the Discussion Paper in this section (proposals 18. 4 - 18.10).

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.
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.
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.

In principle ACCAN supports the proposals put forward in the Discussion Paper (proposals 19.1 – 19.3). However, ACCAN is concerned that proposal 19.3 does not have a requirement for entities or agencies to provide individuals with information on how to make complaints or seek redress related

to substantially automated decisions with legal or similarly significant effect. ACCAN recommends that Proposal 19.3 be amended to include this requirement.

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.

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.

Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.

Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.

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.

Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Proposal 20.7 Prohibit trading in the personal information of children.

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.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 20.1 – 20.9). ACCAN has previously advocated for stronger protections of consumer data collected for the purposes of Direct Marketing.[12] ACCAN expects that amending the Act to include these proposals will give consumers greater control over their personal information.

[12] ACCAN, 2022.

Security, Destruction and Retention of Personal Information

Proposal 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.
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.
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.
Proposal 21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.
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.
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.
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.
Proposal 21.8 Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.

In principle, ACCAN supports the proposals put forward in the Discussion Paper (proposals 20.1 – 20.9). However, ACCAN considers the lack of a requirement for entities or agencies to delete personal information as soon as the purpose for its collection has been satisfied is a significant gap in this section. ACCAN recommends that the Act be amended to specifically require all collected data to be deleted as soon as the purpose for its collection has been satisfied.

Additionally, in ACCAN's submission to the Department of Home Affairs, *Strengthening Australian Cyber Security Regulations and Incentives consultation*, we highlighted that:

- The lack of market incentives to include cybersecurity regulation in consumer products means there is a need for a more robust and enforceable system of cybersecurity regulation to protect consumers from privacy and security threats.

- A mandatory cybersecurity standard compatible with international cybersecurity standards and the GDPR should be introduced in Australia.[13]

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.

ACCAN supports the proposal put forward in the Discussion Paper (proposal 22.1).

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. **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). **Proposal 23.3** Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities. **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. **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. **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.

ACCAN supports the proposals put forward in the Discussion Paper (proposal 23.1 – 23.6).

Cross-Border Privacy Rules and domestic certification

Nil proposals

Part 3: Regulation and enforcement

Enforcement

Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

[13] ACCAN, 2021, *ACCAN Submission to Strengthening Australia's Cybersecurity Regulations and Incentives consultation*, https://accan.org.au/accans-work/submissions/1916-cybersecurity-regulations-and-incentives.

(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.

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.

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.

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.

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 <u>identify, mitigate and</u> redress any <u>actual or reasonably foreseeable</u> loss or damage suffered by the complainant/those individuals.

The OAIC should publish guidance on how entities could achieve this.

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.

Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.

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.

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.

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.

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.

ACCAN supports the proposals put forward in the Discussion Paper (proposals 25.1 – 25.11). ACCAN has previously advocated for increased penalties for privacy breaches. Proposal 25.1(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, is

welcome. ACCAN believes that the most appropriate mechanism for review and enforcement activities for the Act are best housed within an appropriately resourced OAIC.[14]

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.

ACCAN has significant concerns with the proposal put forward in the Discussion Paper (proposal 26.1).

While ACCAN has previously advocated for a Direct Right of Action, in our 2021 submission to the Privacy Act review we raised concerns that such a proposal fails to meet the needs of individuals seeking redress for privacy breaches.[15] ACCAN asserts that the right to have the complaint heard by the Federal Court or the Federal Circuit Court is not a financially viable option for the majority of Australians. This is the current framework for disability discrimination complaints through the AHRC. If a complaint is unable to be conciliated or is terminated by the AHRC then the complainant has the right to apply to have the case heard in the Federal Court. The risk of falling liable to costs should the action be unsuccessful routinely leaves disability discrimination complainants with no affordable option.

ACCAN, therefore, recommends that a direct right of action, via a straightforward, easy to access and affordable tribunal should be adopted to provide individuals with an appropriate mechanism for redress.

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.

ACCAN supports the proposal put forward in the Discussion Paper (proposal 27.1). ACCAN has previously advocated for the inclusion of a statutory tort for serious invasions of privacy in the Privacy Act. A Federal statutory tort will address the gaps in the existing framework of Federal, State and Territory privacy legislation.[16]

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. **Proposal 28.2**

[14] ACCAN, 2022.
[15] ACCAN, 2021, *ACCAN Submission to Privacy Act Review Issues Paper consultation,* https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation
[16] Ibid.

(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.

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.
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.

ACCAN supports the proposal put forward in the Discussion Paper (proposal 28.1).

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.
Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.
Proposal 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

ACCAN supports this Proposal. In our earlier submission to the Privacy Act review, ACCAN highlighted the multiple legislative instruments which have overlapping privacy frameworks. Specifically in the context of communications, we submitted that both the Telecommunications Act and the Privacy Act should be included in the review of the various privacy protections in telecommunications, including provisions for privacy protections, and the transparency and accountability for those protections. There may be contradictions, overlaps and duplication of regulation which could be resolved for the benefit of all stakeholders. Our recommendation was:

> Recommendation 14: The Telecommunications Act and the Privacy Act should both be reviewed to ensure contradictions, overlaps and duplication are resolved.

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.

ACCAN supports the proposal put forward in the Discussion Paper (proposal 30.1).