Privacy Act Review Issues Paper

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

21 January 2022

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation

PO Box A1158, Sydney South NSW 1235
Tel: (02) 9288 4000 | Contact us through the National Relay Service
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

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 review of the *Privacy Act 1988 Discussion Paper October 2021*. We are pleased to note that the proposals put forward in the discussion paper positively reflect many of the positions we submitted in the first stage of the Privacy Act review in late 2020.

Currently, the information and power asymmetries between consumers and digital platforms can make it challenging for individuals to make informed decisions about how our 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.

[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/

Responses to discussion paper proposals and questions

Part 1: Scope and application of the Act

1. Objects of the Act

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals *with regard to their personal information*, and
(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

ACCAN supports these amendments to the Act. In our 2020 submission 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] We hope this, and other proposed amendments, will help ameliorate this imbalance.

2. Definition of personal information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

ACCAN sees these proposals, 2.1 – 2.5, related to the definition of 'personal information' as positive amendments to the Act. ACCAN expects that these will provide greater clarity for the interpretation of the Act with regard to what is considered 'personal information'. However, ACCAN supports the

[2] https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

Salinger Privacy submission recommendations that aspects of these amendments be further elaborated on to ensure that any unanticipated gaps do not undermine the intent of the proposals.[3]

Furthermore, ACCAN does not support the re-introduction of the Privacy Amendment (Re-identification) Offence Bill 2016, proposal 2.6. Acknowledging the Privacy Commissioner's criticism of this Bill, ACCAN does not believe that the Bill will provide the necessary protections needed for public interest research. ACCAN supports the Salinger Privacy submission suggestion that Malicious re-identification attacks on public data could be better regulated by way of a statutory tort (Proposal 26).

3. Flexibility of the APPs

3.1. Amend the Act to allow the Information Commissioner (IC) to make an APP code on the direction or approval of the Attorney-General:

- **where it is in the public interest to do so without first having to seek an industry code developer, and**
- **where there is unlikely to be an appropriate industry representative to develop the code**

3.2 Amend the Act to allow the IC to issue a temporary APP code 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.

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- **entities, or classes of entity**
- **classes of personal information, and**
- **acts and practices, or types of acts and practices.**

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

ACCAN has previously made a separate submission to the Attorney-General's consultation on the Exposure Draft Online Privacy Bill addressing our position on the development of codes. We submit that the most effective codes are those that have been developed with community involvement from the beginning. As such, we can only support proposals 3.1 and 3.2 if there is a mandate to include community participation.

4. Small business exemption

Acknowledging the discussion paper provides a variety of possible options related to the treatment of small businesses under the Act, ACCAN's view has not changed since our earlier submission to the Privacy Act review, in which we recommended that the Small Business Exemption be removed.[4] Thus, ACCAN supports the adoption of the option to remove the small business exemption. We reiterate

[3] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation[4]

our concerns that should it be retained, the small business exemption in the Act will undermine the success of the CDR. Recent proposed legislative changes to allow non-accredited parties to obtain CDR data[5] under the CDR regime - including accountants, lawyers, tax agents, BAS (Business Activity Statement) agents, financial advisors, financial counsellors, and mortgage brokers - will leave consumers unprotected if these small businesses that are not CDR accredited continue to be exempted from the Act.

5. Employee records exemption

Similarly, the discussion paper outlines a number of potential options to address the question of the current appropriateness of the Employee Records Exemption in the Act. Again, ACCAN's position on this issue has not changed since our earlier submission to the Privacy Act review.[6] ACCAN, acknowledging the position of the ALRC, recommends that the employee records exemption should be removed to bring Australian privacy law in line with comparable overseas jurisdictions such as the United Kingdom and New Zealand.[7]

6. Political exemption

Having considered the discussion paper's evaluation of the question about the value of the current Political Exemption from the Privacy Act, ACCAN remains convinced that this exemption should be repealed. As outlined in the discussion paper the overwhelming majority of submissions to the 2019 Privacy Act review recommended the removal of this exemption. Removing this exemption will bring Australia in-line with other democratic nations which require political parties to abide with their respective privacy regulations.

7. Journalism exemption

While ACCAN has not previously held a position on this exemption, our review and consideration of the discussion paper's evaluation of previous submissions and related questions has informed our current thinking on the value of the current Journalism Exemption. Acknowledging the importance of public interest journalism, ACCAN supports the calls for a tightening of the current exemption, to include a public interest test.

Additionally, ACCAN supports the Salinger Privacy submission which recommends that a more limited exemption apply to media organisations for collection, use and disclosure for activities necessary to the conduct of investigative and public interest journalism.[8]

---

[5] CDR rules expansion amendments Consultation Paper September 2020 – accessed at www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf

[6] https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

[7] www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/40-employee-records-exemption/alrcs-view-3/

[8] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

Part 2: Protections

8. Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

8.2 APP 5 notices limited to the following matters under APP 5.2:

- **the identity and contact details of the entity collecting the personal information**
- **the types of personal information collected**
- **the purpose(s) for which the entity is collecting and may use or disclose the personal information**
- **the types of third parties to whom the entity may disclose the personal information**
- **if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection**
- **the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and**
- **the location of the entity's privacy policy which sets out further information.**

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the Online Privacy (OP) code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- **the individual has already been made aware of the APP 5 matters; or**
- **notification would be *impossible* or would involve *disproportionate effort*.**

ACCAN in general supports these proposed amendments. As outlined in the discussion paper, consumer understanding and consumer notice fatigue are significant factors that need to be considered when endeavouring to provide appropriate information to consumers in order that they can make informed decisions about the collection of their data. ACCAN believes that the adoption of these amendments will provide greater consumer confidence and provide greater privacy protections.

9. Consent to the collection, use and disclosure of personal information

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

Similarly, ACCAN supports these amendments. 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 believes these amendments in proposals 8 and 9 reflect this recommendation.

10. Additional protections for collection, use and disclosure of personal information

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- **Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances**
- **The sensitivity and amount of personal information being collected, used or disclosed**
- **Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information**
- **Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity**
- **Whether the individual's loss of privacy is proportionate to the benefits**
- **The transparency of the collection, use or disclosure of the personal information, and**
- **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.**

10.3 Include an additional requirement in APP 3.6 to the effect that 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.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

[9] https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

10.4 Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

ACCAN is pleased to see these proposed amendments in the discussion paper. We have significant concerns about the current practices of some entities in their collection and use of consumer data. Having read and considered the discussion of 'fairness' in the discussion paper, ACCAN continues to support the OAIC's proposal of introducing a "general fairness requirement for the use and disclosure of personal information" as a way of addressing "the overarching issue of power imbalances between entities and consumers" and "protecting the privacy of vulnerable Australians including children".[10]

11. Restricted and prohibited acts and practices

11.1 Option 1: APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- **Direct marketing, including online targeted advertising on a large scale**
- **The collection, use or disclosure of sensitive information on a large scale**
- **The collection, use or disclosure of children's personal information on a large scale**
- **The collection, use or disclosure of location data on a large scale**
- **The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software**
- **The sale of personal information on a large scale**
- **The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale**
- **The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or**
- **Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.**

Option 2: In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

ACCAN recommends the adoption of Option 1. This option provides considerable privacy protections from entities that participate in a number of the listed restrictive practices.

ACCAN does however support the recommendation in the Salinger Privacy submission that refinements will be necessary in relation to the list of 'restricted practices.[11]

[10] https://www.accc.gov.au/system/files/OfficeoftheAustralianInformationCommissioner%28May2019%29.pdf

[11] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

12. Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

- **Option 1 – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.**
- **Option 2 – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.**

ACCAN recommends the adoption of Option 1. After considering the discussion paper's evaluation of various positions on this question, ACCAN retains our position that services and devices must have the most privacy protective settings by design. This is of particular importance for those people for which navigating settings and control options is difficult. For example, people with limited digital capacity and some people with disability.

13. Children and vulnerable individuals

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1 - Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.**
- **Option 2 - In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.**

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

13.2 Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

ACCAN recommends the adoption of 13.1 Option 1. In our earlier submission to the Privacy Act review, ACCAN made the following recommendation.

> **Recommendation 4:** Children under the age of 16 may only have their personal information processed with the express consent of a responsible adult.

Additionally, ACCAN supports the adoption of Proposal 13.2.

14. Right to object and portability

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

ACCAN supports the adoption of Proposal 14.1.

15. Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- **the personal information must be destroyed or de-identified under APP 11.2**
- **the personal information is sensitive information**
- **an individual has successfully objected to personal information handling through the right to object (see Chapter 14)**
- **the personal information has been collected, used or disclosed unlawfully**
- **the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and**
- **the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.**

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either *all or some* of the personal information held by an APP entity.

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

ACCAN supports this Proposal. Implementing these proposals will bring the Act closer in line with Article 17 of the GDPR, The GDPR's exceptions to the right to erasure are driven by public interest imperatives. In our earlier submission to the Privacy Act review, ACCAN made the following recommendation.

> **Recommendation 9:** Individuals must have the right to have their data erased under certain circumstances.

16. Direct marketing, targeted advertising and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.
On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

16.2 The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

16.3 APP entities would be required to include the following additional information in their privacy policy:

- **whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and**
- **whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.**

16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

ACCAN, in principle, supports this proposal. In our earlier submission to the Privacy Act review, we asserted that APP 7 is inadequate to regulate the collection and use of personal information for direct marketing purposes and we made the following recommendation.[12]

> **Recommendation 7:** The Act should impose more stringent regulation on the use of personal information for digital marketing purposes.

ACCAN considers that these proposals will provide greater clarity to consumers regarding the use of their data for the purposes of Direct Marketing.

Having said this however, ACCAN supports the Salinger Privacy position regarding the clarification of the various levels of harm covered under the umbrella term Direct Marketing.[13] ACCAN believes that there needs to be consideration of these issues before these proposals are implemented.

[12] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing/

[13] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

17. Automated decision-making

17.1 Require privacy policies to include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on people's rights.

ACCAN has participated in a number of recent inquiries into the ethical use of AI in Australia, including the AHRC Human Rights and Technology project. We support the recommendations included in the AHRC Human Rights and Technology report relating to the use of personal data in AI and ADM processes.

While we do not oppose Proposal 17.1, ACCAN considers that the following recommendations for additional amendments to the Act made in the Salinger Privacy submission may indeed provide greater privacy protections:

- a right to human review of automated decision-making, and
- a right to algorithmic transparency, including explain ability and auditability.

18. Accessing and correcting personal information

18.1 An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

18.2 Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- **the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.**

18.3 Clarify the existing access request process in APP 12 to the effect that:

- **an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature; and**
- **where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.**

In principle, ACCAN supports this Proposal. We do however submit that the term 'dispropropinate effort'in 18.1 leaves too much discretion in the hands of entities and needs to be further clarified to eliminate any potential loop holes.

19. Security and destruction of personal information

19.1 Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.

19.2 Include a list of factors that indicate what reasonable steps may be required.

19.3 Amend APP 11.2 to require APP entities to take *all* reasonable steps to destroy the information or ensure that the information is *anonymised* where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

ACCAN supports this Proposal. ACCAN has made a submission to the Dept of Home Affairs, Strengthening Australian Cyber Security Regulations and Incentives consultation. In our submission 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.[14]

20. Organisational accountability

20.1 Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:

- **Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.**

ACCAN supports this Proposal. We have advocated for the adoption of Privacy by Design and Privacy by Default principles to ensure greater levels of privacy protection. We also assert that adopting this Proposal will bring Australian privacy protections in-line with comparable countries.

21. Controllers and processors of personal information

These concepts are found in many overseas data protection frameworks. Generally, a *data controller* is an entity which, alone or jointly with others, determines the purposes and means of the processing of personal information and a *data processor* is an entity which processes personal information on behalf of the controller.[15]

ACCAN has not previously had a position on this issue. However, having considered the discussion paper's informative discussion of this question, ACCAN supports the adoption of a descriptive clarification of each of these entities with assigned responsibilities for each. In doing this Australia will be more in-line with comparable countries' privacy frameworks.

[14] https://accan.org.au/accans-work/submissions/1916-cybersecurity-regulations-and-incentives

[15] GDPR (n 26) art 4(7), 4(8).

22. Overseas data flows

22.1 Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

22.3 Remove the informed consent exception in APP 8.2(b).

22.4 Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

22.5 Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

22.6 Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

ACCAN supports the response in the Salinger Privacy submission to the Privacy Act review on this Proposal.[16]

23. Cross Border Privacy Rules (CBPR) and domestic certification

23.1 Continue to progress implementation of the CBPR system.

23.2 Introduce a voluntary domestic privacy certification scheme that is based on and works alongside CBPR.

ACCAN has not previously held a position on this issue. Having considered the discussion paper's elaboration and questions, ACCAN considers these proposals as being beneficial to consumer privacy protections and therefore we do not oppose these proposals being adopted.

Part 3: Regulation and enforcement

24. Enforcement

24.1 Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:

- **A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.**

[16] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

- **A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.**

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

24.3 The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.

24.4 Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

24.5 Amend paragraph 52(1)(b)(ii) and 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.**

24.6 Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- **A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and**
- **A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.**

24.8 Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

24.9 Alternative regulatory models

- **Option 1 - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.**
- **Option 2 - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.**
- **Option 3 - Establish a Deputy Information Commissioner – Enforcement within the OAIC.**

ACCAN supports the adoption of proposals 24.1 – 24.8. We have made a submission to the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* in which we support the adoption of Part B: Enforcement and penalties for privacy breaches.

ACCAN has previously advocated for increased penalties for privacy breaches. The move to bring the privacy breach penalties in line with the Australian Consumer Law penalties is welcome. ACCAN recommended a similar increase in the maximum penalty for privacy breaches in our submission to the Privacy Act Review, recommending that the penalties for privacy breaches be increased to match those in the Consumer Data Right scheme.[17]

With regard to proposal 24.9 - **Alternative regulatory models**, ACCAN supports the adoption of Option 3. We believe that the most appropriate mechanism for review and enforcement activities for the Act are best housed within an appropriately resourced OAIC. However, ACCAN submits that , there is benefit in having both an expanded EDR and enforcement within this proposal. In the telecommunications sector complaints and enforcement are separated.

25. A direct right of action

25.1 Create a direct right of action with the following design elements:

- **The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.**
- **The action would be heard by the Federal Court or the Federal Circuit Court.**
- **The claimant would first need to make a complaint to the OAIC (or FPO)[1] and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.**
- **The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.**
- **The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.**

While ACCAN has previously called for a Direct Right of Action framework, we do not support this proposal in its current form. As is outlined in the Salinger Privacy submission, this proposal fails to meet the needs of individuals seeking redress for privacy breaches.[18] 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.

[17] See https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

[18] https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

26. A statutory tort of privacy

26.1 Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

26.2 Option 2: Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

26.3 Option 3: Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

26.4 Option 4: In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

ACCAN strongly supports Option 26.1 This was one of the recommendations that we made in our earlier submission to the Privacy Act review,

> **Recommendation 13:** A Federal statutory tort is needed to address the gaps in the existing framework of Federal, State and Territory privacy legislation.[19]

27. Notifiable Data Breaches scheme

27.1 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.

ACCAN strongly supports this Proposal.

28. Interactions with other schemes

28.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

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

28.3 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

[19] https://accan.org.au/our-work/submissions/1827-privacy-act-review-issues-paper-consultation

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.