Privacy Act Review Issues Paper

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

18 December 2020

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

PO Box 639, Broadway NSW 2007
Tel: (02) 9288 4000 | Fax: (02) 9288 4019 | 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.

PO Box 639,
Broadway NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
Contact us through the National Relay Service

Contents

Executive Summary

ACCAN welcomes this review of the *Privacy Act 1989* to ensure the objectives of the Act and the OAIC's core purpose — to promote and uphold privacy and information access rights — is suited to the modern global digital economy.

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]

ACCAN supports the proposals of the ACCC's Digital Platforms Inquiry report, which aim to redress this imbalance and increase transparency, choice and control in consumer's data collection and processing practices including:

- Strengthened notice and consent requirements;
- Introduction of an enforceable privacy code for designated digital platforms; and
- Higher penalties for privacy infringements.

ACCAN also agrees with the OAIC's position that while an individual should have the ability to self-manage their privacy through enhanced notice and consent requirements, the entities entrusted with consumer data must be accountable for any handling – or mishandling – of this data.

ACCAN's submission to the *Privacy Act Review* contains proposals which are intended to provide greater protection or consumers:

- broadening the definition of 'Personal Information';
- increased penalties for privacy breaches;
- greater transparency and clarity in obtaining consumer consent to data collection;
- reform of the exemptions for small business with a turnover of less than $3 million;
- more stringent regulation of digital marketing practices;
- introduction of a direct right of action and statutory tort;
- introduction of rules to protect Australia's vulnerable groups such as children.

Developments in privacy regulation internationally are an important guideline for the evolution of Australia's data regime, and our responses frequently refer to the EU's General Data Protection Regulation (GDPR).

In addition, it is also important to consider reform of the *Privacy Act* cohesively with other regimes, including the *Consumer Data Right* and the *Telecommunications Act*.

[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/

List of recommendations

Recommendation 1: The definition of 'Personal Information' needs to be expanded to adequately regulate modern data collection practices and analytic capabilities.

Recommendation 2: The various exemptions in the Act need revision as a matter of priority.

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

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

Recommendation 5: Regulations should be introduced to mandate privacy by design in IoT devices to protect consumers.

Recommendation 6: Consent to the use of IoT devices used by more than one person should be 'unbundled' to facilitate genuine consent by each individual.

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

Recommendation 8: Access to a product or service should not be conditional on an individual's consent to their personal information being collected, used or disclosed by an entity.

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

Recommendation 10: A stronger enforcement framework and penalties, and a well-resourced regulatory body, are needed to ensure compliance with a strengthened privacy regime.

Recommendation 11: There is a need for a more affordable avenue of appeal for consumers disputing a decision by the Privacy Commissioner.

Recommendation 12: A direct right of action, via a straightforward, easy to access and cheap tribunal should be introduced to provide consumers with equitable access to justice.

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

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

The Australian Communications Consumer Action Network (ACCAN) thanks the Attorney-General's Department for the opportunity to contribute to its review of the *Privacy Act 1988* (Cth).

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 often have concerns about their privacy and the security of their personal information online, and telecommunications is a particularly sensitive area. Consumers can feel disempowered by the lack of transparency around their personal information, and indeed some consumers don't fully understand how their personal information is gathered, stored or used online. ACCAN firmly believes that privacy protections are essential for communications consumers in Australia, and that these protections must adequately protect consumer information.

In our below response we offer feedback on some of the key themes identified in the Issues Paper. We would welcome further opportunities for consultation based on any of the issues we raise in our response.

Objectives of the Privacy Act

Section 2A

Although Section 2A(a) identifies one of the objectives of the Privacy Act 1988 (Cth) (the Act) as "to promote the protection of the privacy of individuals", in practice the Act fails to achieve this goal. For example:

- Section 2A(b) aims to balance the "interests of entities in carrying out their functions or activities" with "the protection of the privacy of individuals". Despite this, the increasing volume of personal data collected and used by organisations for direct marketing purposes means that the interests of business are often prioritised over the protection of personal information.

- The objective of section 2A(d) in facilitating "responsible and transparent handling of information by entities" is not adequately fulfilled by the method of consumer notice and consent adopted by the majority of organisations.

- The objective of section 2A(c), to "provide the basis for nationally consistent regulation of privacy and the handling of personal information", is not achieved by the Act. The complex system of privacy laws between levels of government, states and territories and the numerous exclusions means "there are instances where

entities are exempt from the Act but are not bound by State or Territory privacy laws, in effect making them completely unregulated for certain practices."[2]

In revising the objectives of the Act, it is essential that these objectives are adequately buttressed by provisions which enable these objectives to be met. The privacy framework for the Consumer Data Right (CDR) in its current form (not including the draft changes to the *Competition and Consumer (Consumer Data Right) Rules 2020*)[3] provides the standard of consumer protection ACCAN would like to see as a benchmark for privacy protection.[4]

Personal information

Definition of 'Personal Information'

The definition of 'personal information' in the Act should be amended to include:

- Inferred personal information;
- De-identified information;
- Technical information;
- Pseudonymised information; and
- Anonymous information

Inferred personal information

Data analytics activities can collate data from a wide variety of different sources, including from third parties, to generate new information about an individual's information through 'collection via creation'. These new data insights can be used for a range of different purposes, including new purposes that may not have been anticipated.[5]

For consumers to be adequately protected by the Act, such inferred data needs to be included in the definition of 'personal information' and 'sensitive information'. The definition of data 'collection' must also be amended to include the creation of new data, including sensitive data, by generating new inferences about an individual from existing data.

De-identified information

Under the Act, information that has "undergone an appropriate and robust de-identification process" is not personal information and is not protected.[6] ACCAN believes that de-identified data must also be protected under the Act. The Australian Competition and Consumer

[2] Salinger Privacy, Submission to the Privacy Act Review

[3] www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-cdr-rules

[4] https://treasury.gov.au/consumer-data-right

[5] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/

[6] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

Commission (ACCC) has identified problems with current de-identification practices, citing that many businesses aim to distinguish, profile and interact with individual consumers by using "de-identified" data using "unique identifiers."[7]

Technical information

Because de-identification of data can be reversed using unique identifiers, the definition of 'personal information' must be expanded to include technical data such as IP addresses, location data, device identifiers and any other online identifiers. As the Issues Paper has noted, the current definition of personal information does not adequately capture technical information and should be revised to reflect the General Data Protection Regulation (GDPR) definition.

Pseudonymised information

Pseudonymised information must be explicitly protected under the Act, in line with Recital 26 of the GDPR. Pseudonymisation is a reversible process, that de-identifies data but allows reidentification if necessary.[8] Because the de-identification process is reversible, pseudonymised information must be included in the definition of 'personal information'.

Anonymous information

Despite that fact that the GDPR excludes 'anonymous information' from the principles of data protection (Recital 26), ACCAN submits that anonymous information must be included in the definition of 'personal information'. This is because Recital 26 of the GDPR is based on the assumption that it is impossible to re-identify anonymous information.[9]

However, research suggests that information is rarely irreversibly anonymised. Researchers from two universities in Europe have published a method they say is able to correctly re-identify 99.98% of individuals in anonymised data sets with just 15 demographic attributes.[10]

Recommendation 1: The definition of 'Personal Information' needs to be expanded to adequately regulate modern data collection practices and analytic capabilities.

[7] Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* - accessed at https://www.accc.gov.au/system/files/Dr%20Katharine%20Kemp%20%2826%20April%202020%29.pdf

[8] https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/

[9] www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and

[10] https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

Exemptions

The extensive exemptions or restrictions in favour of organisations and ambiguity regarding organisational responsibilities water down the protections offered to consumers. Overall, Australia's privacy laws are generally more concerned with organisational interests than with individual interests and, arguably, privacy laws have become vehicles for the legitimisation of organisational data processing practices.[11]

Small business exemption

The small business exemption in its current form fails to strike the right balance between protecting the privacy rights of individuals and avoiding the imposition of unnecessary compliance costs on small business. The Act was drafted when the amount of data that could be collected by small businesses was far more limited. In the current technological marketplace small businesses are capable of managing vast amounts of personal information and this poses significant threats to the privacy of individuals.

As an example, the Australian Law Reform Commission (ALRC) has noted that the telecommunications industry is increasingly handling large amounts of personal information and that it is appropriate that the handling of personal information by these organisations is regulated by the Act. Accordingly, ACCAN supports the ALRC's recommendation that the small business exemption should be removed to ensure even small telecommunications businesses are subject to privacy rules.[12]

If 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[13] 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 and continue to be exempted from the Act.

Employee records exemption

As the Issues Paper has identified, a substantial amount of information, including sensitive information, falls within the employee records exemption, so that sensitive information relating to employees often does not need to be handled in accordance with the Act.[14] Clearly, the fact that the handling of personal information contained within an employee record is

---

[11] Lloyd, Halani, 'Are privacy laws more concerned with legitimising the data processing practices of organisations than with safeguarding the privacy of individuals? (2002) 9(5) *Privacy Law and Policy Reporter* 81 - retrieved at http://www5.austlii.edu.au/au/journals/PrivLawPRpr/2002/39.html

[12] www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/71-telecommunications-act/small-business-exemption-2/

[13] 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

[14] www.allens.com.au/insights-news/insights/2020/11/privacy-act-review-what-you-need-to-know/

exempt in most circumstances from the operation of the Act undermines consumer protection.

As the ALRC has noted, there is a real potential for individuals to be harmed if employees' personal information is used or disclosed inappropriately. The power imbalance between employers and employees means employees may be under economic pressure to provide personal information to their employers, undermining genuine consent.[15]

ACCAN submits that the employee records exemption is contrary to public expectations that sensitive employee records should be subject to privacy protections, and supports the ALRC's recommendation 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.[16]

Political parties' exemption

The Act was drafted when the amount of data that could be collected and used to profile and target individuals for campaigning purposes was much smaller. In light of recent revelations about the role of Cambridge Analytica in influencing the outcome of elections, there is no justifiable reason why political parties should not have to be accountable for their management of personal information about constituents and voters, as is already the case in other jurisdictions. Accordingly, the political parties' exemption is now inappropriate and must be removed from the Act.

> **Recommendation 2:** The various exemptions in the Privacy Act need revision as a matter of priority.

Notice and consent

Notice of collection

There are two major impediments to the effectiveness of notice of collection of personal information:

- 'Consent fatigue' discouraging consumers from reading privacy notices before accepting them;[17] and

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

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

[17] Utz. C. et al, ' (Un)informed Consent: Studying GDPR Consent Notices in the Field', 22 October 2019 – accessed at https://dl.acm.org/doi/10.1145/3319535.3354212

- The opacity of privacy notices which are so long, complicated and difficult to understand that they prevent consumers from genuinely exercising consent or control over how their personal information is disclosed.[18]

Results from a soon to be published survey report by one of ACCAN's grantees, Deakin University, highlights the inadequacy of notices of collection of personal information as an effective method of obtaining informed consent from consumers. From a sample of 1000 respondents, 30% find privacy notices too difficult to read, 26% don't have time to read them and 2.41% don't even know where to find the privacy notice.

In addition, the majority of respondents had either an 'average understanding' (39%) or 'some understanding' (28%) of privacy notices, while a meagre 4.5% of respondents had a complete understanding and almost 10% had no understanding of the privacy notice at all.[19]

ACCAN agrees with the Office of the Australian Information Commissioner (OAIC) that the onus of providing consent for use of data should be shifted away from the consumer. We also agree with the OAIC that the responsibility for protecting consumers' personal information should be assumed by privacy regulators, government legislators, and the digital platforms and organisations collecting it via "appropriate accountability obligations for entities, as well as other regulatory checks and balances".[20]

This could be achieved in a variety of ways, including for example:

- Imposing mandatory privacy and security standards in the design of data collection and handling processes by digital platforms and organisations; and
- Amending APP5 to meet the current standard of privacy protection in the CDR, so that a participant "must take steps" to notify consumers of privacy collection practices rather than being required to "take reasonable steps."

Limiting information burden

ACCAN supports the principle of 'limiting information burden' on consumers through the use of a standardised framework of notice, such as standard words or icons. This was recommended by the OAIC in order to create "a common language in relation to privacy and personal information" and enable consumers to understand data collection practices and exercise informed choice.[21]

However, the initial survey results of Deakin University's grant research suggests that although respondents think 'star ratings' and icons may be useful in helping consumers gain more meaningful understanding of the use of their data, limited understanding of the meaning of the icons and the privacy regulatory framework underpinning them may undermine their effectiveness.[22] A comprehensive consumer education campaign would

[18] See www.oaic.gov.au/assets/updates/news-and-media/facebook-federal-court-concise-statement.pdf

[19] Deakin University, 'Enhancing Consumer Awareness of Privacy and the Internet of Things', unpublished

[20] www.accc.gov.au/system/files/OfficeoftheAustralianInformationCommissioner-October2019.pdf; www.accc.gov.au/system/files/OfficeoftheAustralianInformationCommissioner%28May2019%29.pdf

[21] www.oaic.gov.au/engage-with-us/submissions/customer-loyalty-schemes-review-submission-to-the-accc/

[22] 'Deakin University, 'Enhancing Consumer Awareness of Privacy and the Internet of Things', unpublished

therefore be needed to ensure any such labelling scheme was successful in enabling consumers to make informed decisions and provide genuinely informed consent to data collection. Such a consumer education campaign must be provided in plain English and be accompanied by informative and accessible images, graphics or videos. Information about the icons must be clear, user friendly and easy to read and understand.

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

Pro-consumer defaults

ACCAN submits that there must always be pro-privacy defaults in the collection, use and disclosure of personal information. 'Sensitive' personal information – for example, geolocation data which is highly granular and can be used to uniquely identify 95% of the population[23] – merits a particularly high level of protection. Recent amendments to Californian privacy law, which now classifies geolocation data as sensitive information requiring more stringent protective measures, provides a benchmark for Australian privacy law reform.[24]

In addition, ACCAN supports 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".[25]

Obtaining consent from children

ACCAN's strongly believes that specific requirements are needed in relation to how entities seek consent from children. Article 16 of the United Nations Convention on the Rights of the Child states that:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.[26]

---

[23] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, 'Unique in the Crowd: The privacy bounds of human mobility', Scientific reports, March 2013, available at: https://www.nature.com/articles/srep01376?ial=1

[24] The California Privacy Rights Act 2020 expands the definition of 'sensitive personal information' (which is afforded superior protection) to include "a consumer's precise geolocation", which is defined as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet"; see https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf

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

[26] https://www.unicef.org.au/Upload/UNICEF/Media/Our%20work/childfriendlycrc.pdf

Article 8 of the European General Data Protection Regulation (GDP) applies where an information society service (ISS) is being offered directly to a child and regulates the circumstances under which a child can consent to the "processing" of their personal data. 'Processing' includes both the automated and non-automated collection, use, disclosure, erasure or destruction of personal data.[27]

Article 8 states that the processing of personal data of a child under 16 years old is only allowed if "consent is given or authorised by the holder of parental responsibility over the child." It is the responsibility of the 'controller'[28] to "make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child."[29] ACCAN endorses the GDPR's approach because:

- The responsibility for safe data collection practices is shifted away from children, and the obligation to provide adequate privacy protections for children falls to responsible adults including regulators, entities and organisations.
- A child under 16 years old is regarded as not having the capacity to understand that entities are collecting their personal information and using it for marketing and other purposes.

The strict 16-year age limit offers greater protection to children than Australian law. In Australia, the Act doesn't specify an age after which an individual can make their own privacy decision, and only requires "capacity" – as assessed on a case by case basis - for consent to be valid. An organisation or agency handling the personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis.[30]

As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what's being proposed. Where it isn't practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, they may assume an individual over the age of 15 has capacity.[31] The subjectivity of this assessment is problematic both for children and for those with a disability.

As a result, different standards are applied in different contexts and across different jurisdictions, with minors able to apply for their own Medicare card or TFN or make decisions about health care at different ages.[32] ACCAN submits that the Act should specify that children

---

[27] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

[28] Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing. A controller can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual (such as a sole trader, partner in an unincorporated partnership, or self-employed professional). An individual processing personal data for the purposes of a purely personal or household activity is not subject to the GDPR – see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/

[29] https://www.privacy-regulation.eu/en/article-8-conditions-applicable-to-child%27s-consent-in-relation-to-information-society-services-GDPR.htm

[30] https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/#CapacityToConsent

[31] https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people/

[32] Digital Identity Legislation Consultation Paper, p28

under 16 should not be subject to collection and processing of personal information by organisations and entities without the express authorisation of a responsible adult, as per Article 8 of the GDPR.

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

IoT devices and emerging technologies

The use of Internet of Things (IoT) enabled devices is accelerating in Australia, and yet there are limited market-based incentives for Australian IoT device manufacturers to provide consumer protection measures or regulations to ensure consumers are properly informed that their data is being collected.

Currently, IoT devices present a number of challenges in terms of consent:

- An enforceable data privacy regulatory framework is needed to ensure consumers provide genuinely informed consent to use IoT products and services in full knowledge of the risks involved.
- Regulations should be introduced to mandate privacy by design in IoT devices to protect consumers.
- Consent for the use of IoT devices intended for use by an entire household such (e.g. Google Nest, Alexa) must be 'unbundled' to be meaningful.[33]

> **Recommendation 5:** Regulations should be introduced to mandate privacy by design in IoT devices to protect consumers.
>
> **Recommendation 6:** Consent to the use of IoT devices used by more than one person should be 'unbundled' to facilitate genuine consent by each individual.

Direct marketing

APP 7 is inadequate to regulate the collection and use of personal information for direct marketing purposes.[34]

---

[33] The practice of bundled consent by APP entities poses a significant problem in the context of real and free consent. Bundled consent occurs when an APP entity "bundles" together multiple request for an individual's consent for a range of various collection, uses and disclosure purposes of their personal information. The inherent problem with such a practice is that the individual may be unaware as to the wide range of purposes they have given their consent on. The individual is given no choice to choose which collections, uses and disclosures they agree to and which they do not. Bundling will lead to disputes with the regulator as to the nature of the consent that was actually given. – see https://www.cbp.com.au/insights/insights/2019/november/what-is-real-consent-to-data-collection

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

First, the extensive exemptions to APP 7 include all businesses and not-for-profit organisations with an annual turnover of less than $3 million, some small businesses and businesses not categorised as 'organisations' under the Act. As discussed above, businesses of all sizes are now able to collect and use online personal information for direct marketing purposes, which makes these exemptions outdated and undermines the consumer protection that the *Privacy Act* was intended to enable.

Second, the limited definition of 'personal information' in the Act means there are many forms of information that analytics can manipulate for the purposes of personalised marketing communications which are not protected under APP 7. The APP fails to include online identifiers and other individuation techniques which can be used for direct marketing - to curate targeted advertising, personalise content and individualise political messaging - based on automatically generated user profiles.

Third, as discussed above, there are limitations in consumers providing genuinely informed consent when agreeing to have their personal data collected and disclosed by collecting organisations and third parties.

ACCAN considers that more stringent regulation is required for:

- the secondary use of personal data in direct marketing;
- sale of personal data in any form for direct marketing purposes;
- for-profit trade in personal data through data brokers;
- the use of second-party or third-party customer data for online behavioural advertising;
- the illegal gathering of children's personal data on YouTube without parental consent;[35] and
- the use of dark patterns in digital design to mislead consumers.[36]

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

Withdrawal of consent

Australia needs a privacy regime which prohibits any uses or disclosures of data that are contrary to a consumer's interests. As per the GDPR, meaningful consent must be time limited

[35] O'Flynn, S. 'We street-proof our kids. Why aren't we data-proofing them?', 29 September 2019, *The Conversation* – accessed at https://theconversation.com/we-street-proof-our-kids-why-arent-we-data-proofing-them-123415

[36] Lacey, C. and Beattie, A. 'We need a code to protect our online privacy and wipe out dark patters in digital design', 16 September 2020, *The Conversation* – accessed at https://theconversation.com/we-need-a-code-to-protect-our-online-privacy-and-wipe-out-dark-patterns-in-digital-design-145622

and easily withdrawn, and consumers must be given the option to refresh consent on a regular basis.[37]

Currently under Australian privacy law a consumer can withdraw their consent at any time, and organisations or agencies must disclose the possible consequences of withdrawing consent - for example, losing access to a service.

However, ACCAN submits that even if an individual does refuse to consent to their personal information being collected, used or disclosed by an entity, they should still be able to access the product or service. Withdrawal of consent, or refusal to provide consent initially, should not exclude consumers from accessing a product or service.[38]

> **Recommendation 8:** Access to a product or service should not be conditional on an individual's consent to their personal information being collected, used or disclosed by an entity.

Right to erasure

A 'right to erasure' or 'right to be forgotten' must be introduced into the Act to more adequately protect consumer data. ACCAN submits that, to align Australian privacy law with Article 17 of the GDPR, individuals must have the right to have personal data erased if:

- A consumer's personal data has been collected without their consent;
- A consumer's personal data is no longer necessary for the original purpose of its collection or use;
- A consumer has withdrawn consent to retain the data;
- A consumer has objected to the processing of their personal data and there is no legitimate interest to override the objection;
- A consumer has objected to their personal data being used for direct marketing purposes;
- An organisation has processed a consumer's personal data unlawfully; and
- A child's personal data has been collected and processed. [39]

---

[37] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what6

[38] www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/

[39] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

The GDPR's exceptions to the right to erasure are driven by public interest imperatives, and it would be appropriate for Australian privacy law to emulate these exceptions.

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

Enforcement powers under the Privacy Act and role of the OAIC

ACCAN supports the introduction of a privacy regulatory framework equivalent to the CDR scheme in its current form. The Act should replicate the much higher penalties imposed by the CDR scheme to remedy a breach of a Privacy Safeguard – i.e. whichever is highest out of $10M, 10% of domestic turnover pa, or three times the value of benefits obtained from the breach. The civil penalties under the Privacy Act, to be levied by the OAIC, should be increased to mirror the CDR scheme.

In terms of the OAIC's potential role as the enforcer of compliance with a strengthened privacy regulatory framework, ACCAN notes that the OAIC is already experiencing slow resolution times for complaints. If an existing regulatory body such as the OAIC were to perform this function, it would need to be adequately resourced to efficiently manage this additional role and be able to respond swiftly in response to breaches of privacy.

There is also a need for more affordable avenues of appeal for consumers. As noted by the Issues Paper, there is no ability for an individual to appeal from a decision by the Privacy Commissioner to dismiss a complaint, and average consumers do not have the deep pockets required to appeal against any formal determination by the OAIC in the Federal Court.

> **Recommendation 10:** A stronger enforcement framework and penalties, and a well-resourced regulatory body, are needed to ensure compliance with a strengthened privacy regime.
>
> **Recommendation 11:** There is a need for a more affordable avenue of appeal for consumers disputing a decision by the Privacy Commissioner.

Direct right of action

ACCAN is in favour of the introduction of a direct right of action to more sufficiently provide consumers with access to justice. The penalties and procedures in Australia's privacy regulatory regime need to be genuinely prohibitive to deter organisations who breach privacy laws. A direct right of action, via a straightforward, easy to access and cheap tribunal, is essential to deliver meaningful privacy protections to everyday Australians.

The CDR scheme has established a statutory right to sue for damages for any breach of a Privacy Safeguard in relation to CDR data. It also makes broad enforcement powers available to the ACCC and the OAIC to ensure compliance with the CDR regulatory framework. ACCAN believes that the CDR scheme sets a benchmark for the introduction of a direct right of action for breach of privacy as part of Australian privacy law.

Recommendation 12: A direct right of action, via a straightforward, easy to access and cheap tribunal should be introduced to provide consumers with access to justice.

Statutory tort

ACCAN agrees with the ACCC that, although "there is overlap" between the introduction of a direct right of action and a statutory tort for invasion of privacy, a Federal statutory tort would address gaps in the existing privacy framework which is comprised of both Federal and State and Territory legislation.[40] ACCAN is in favour of the introduction of the recommended statutory tort to allow individuals to bring actions for serious invasions of their privacy.

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

Interaction between the Act and other regulatory schemes

Consumer Data Right

ACCAN submits that the Privacy Act and the CDR need to work together to reinforce the protection of consumer data. ACCAN views the strengthened consumer protections under the CDR regime as a benchmark to be emulated in the development of a more robust and enforceable privacy regulatory framework in Australia. If the proposed legislative changes to the CDR scheme are passed, allowing consumer data to be passed from accredited entities to non-accredited entities, the introduction of stronger privacy protections and standards in the handling of consumer data will be imperative.[41]

Telecommunications Act

Privacy protections in telecommunications is spread across a range of legislation, licence conditions and codes:

- Telecommunications Act 1997, Part 13;
- Privacy Act 1998;
- Do Not Call Register Act 2006;
- Spam Act 2003;

[40] Dawson, S., Parsons, J. and Galli, M. *Digital Platforms and proposed amendments to privacy laws*, 12 August 2019 – accessed at https://www.twobirds.com/en/news/articles/2019/global/digital-platforms-and-proposed-amendments-to-privacy-laws

[41] For further outlining of our concerns with respect to the provision of CDR data to non-accredited parties see Financial Rights' Submission to ACCC re: CDR rules expansion amendments, Consultation Paper. https://financialrights.org.au/wpontent/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf

- Integrated Public Number Database (IPND); and
- OAIC complaints handling.

ACCAN submits that both the Telecommunications Act and the Privacy Act should be included in the review of all 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.

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