AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Privacy Act Review Report

ACCC submission

March 2023

1. Introduction

The Australian Competition and Consumer Commission (ACCC) welcomes the opportunity to provide feedback on the Privacy Act Review Report (the Report). The ACCC continues to strongly support the implementation of privacy measures to better empower consumers, protect their data and support the digital economy. The ACCC notes the importance of implementing such measures in a balanced and proportionate way that provides effective privacy protections without unduly reducing competition, productivity and innovation.

The ACCC is an independent Commonwealth statutory agency that promotes competition, fair trading and product safety for the benefit of consumers, businesses and the Australian community. The primary responsibilities of the ACCC are to enforce compliance with the competition, consumer protection, fair trading and product safety provisions of the *Competition and Consumer Act 2010* (Cth) (CCA), regulate national infrastructure and undertake market studies.

2. Intersection between privacy, competition and consumer protection

The effect of privacy laws on competition and consumer protection

The ACCC's views on the Report's proposals are informed by our competition and consumer protection work. This includes our role in implementing and enforcing the economy-wide data portability regime, the Consumer Data Right (CDR); our enforcement action against digital platforms for breaches of the Australian Consumer Law, including in respect of their data collection practices; and our extensive inquiries examining digital platform markets.[1]

For example, the final report of the ACCC's Digital Platforms Inquiry in 2019 (DPI Report) noted that robust data collection and privacy laws can enhance consumer protection by ensuring consumers receive accurate, intelligible information about entities' data practices. This, in turn, can increase the transparency of digital platforms' data practices, which can then help consumers make informed choices about which digital platform services to use, thus promoting effective competition on these issues.[2]

Such laws, as well as data portability schemes like the CDR, can also enhance competition in data-driven markets by enabling consumers to readily port their data between service providers, decreasing their switching costs and lowering barriers to entry or expansion for rival service providers.[3]

Developments since the DPI Report

The DPI Report was published in July 2019 and included several privacy-specific recommendations (Recommendations 16 to 19). The Privacy Act Review was initiated as part of the Government's response to these recommendations.[4]

It is worth noting some significant developments to the Australian privacy and digital landscape since the DPI Report was published and the Privacy Act Review commenced. These include:

- The ACCC's ongoing Digital Platform Services Inquiry (DPSI) has found consistently high concentration in a range of digital platform markets in Australia, including the

[1] These inquiries include the completed Digital Platforms Inquiry and Digital Advertising Services Inquiry, as well as the ongoing Digital Platform Services Inquiry.

[2] ACCC, Digital Platforms Inquiry – final report, July 2019, pp 434-435.

[3] ACCC, Digital Platforms Inquiry – final report, July 2019, p 435.

[4] Australian Government, Regulating in the digital age – Government Response and Implementation Roadmap for the Digital Platforms Inquiry, December 2019, p 6.

markets for general search engine, mobile operating system, web browser, social media, online private messaging, ad tech and digital advertising services.[5]

- The November 2022 interim report of the DPSI (the Regulatory Reform report) observed significant competitive advantages for digital platforms that have access to large amounts of consumer data. These advantages can increase barriers to entry and expansion for smaller rivals, leading to a lack of competition. Consumers may also experience reduced privacy and autonomy from excessive data collection and use.[6]
- Recent high-profile data breaches, combined with a surge in scam-related losses to over $2 billion in 2021,[7] highlight the need for strong privacy protections to help keep consumers safe.
- As part of the October 2022 Budget, the Government announced seed funding for the ACCC to work with other government agencies, law enforcement and the private sector to advise on the establishment of a National Anti-Scam Centre.[8] The Government is currently consulting with stakeholders, seeking input on the function and role of the National Anti-Scam Centre.
- The formation of the Digital Platform Regulators Forum (DP-REG) in March 2022 has deepened the strong existing relationship between the ACCC and the Office of the Australian Information Commissioner (OAIC) on privacy issues in the digital space.[9]
- The CDR scheme has successfully launched and begun progressively rolling out across the economy, with live sharing of banking data commencing on 1 July 2020. This program is now being rolled out to the energy sector, with additional sectors to follow.
- On 1 April 2022, the *Data Availability and Transparency Act 2022* (Cth) entered into force. This Act establishes the Office of the National Data Commissioner to administer a new, best practice scheme for sharing Australian Government data.[10]
- On 13 December 2022, the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) entered into force. Among other changes, this Act addresses Recommendation 16(f) in the DPI Report, by increasing the maximum penalty for a breach of s13G of the *Privacy Act 1988* (Cth) (Privacy Act) to match the quantum of penalties in the CCA.[11]

3. Observations on the Report

The comments below focus on the proposals of the Report most relevant to the role of the ACCC as Australia's competition and consumer regulator. They are broken down into the following three parts, which broadly align with the three parts of the Report:

1. Scope and application of the Privacy Act
2. Consumer rights and protections
3. Regulatory and enforcement considerations.

---

[5] ACCC, Digital platform services inquiry - September 2022 interim report - Regulatory reform, September 2022, pp 198-206.

[6] ACCC, Digital platform services inquiry - September 2022 interim report - Regulatory reform, September 2022, pp 31-35 and 40-43.

[7] ACCC, Targeting scams: report of the ACCC on scams activity 2021, July 2022, p 10.

[8] ACCC, ACCC receives additional responsibilities in budget, 26 October 2022.

[9] ACCC, Agencies form Digital Platform Regulators Forum, 11 March 2022. DP-REG is a joint initiative of the ACCC, the OAIC, the Australian Communications and Media Authority and the Office of the eSafety Commissioner to discuss and collaborate on digital platforms issues where their respective regulatory remits intersect.

[10] Office of the National Data Commissioner, The DATA Scheme is now open for business, accessed 23 March 2023.

[11] *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth), s14.

Part 1: Scope and application of the Privacy Act

The ACCC remains strongly supportive of privacy proposals that provide clarity to the scope and application of the Privacy Act, particularly those that clarify the definition of important words and phrases. We also support proposals that would result in the Privacy Act better aligning with the CDR Privacy Safeguards, on the basis that this will deliver a more consistent privacy regime for consumers.

Personal information, de-identification and sensitive information (Chapter 4)

As the ACCC noted in its submission to the Discussion Paper of this review, there is considerable uncertainty as to whether technical information in relation to an individual (such as IP addresses and other online identifiers) constitutes 'personal information' for the purposes of the Privacy Act.[12] In addition, the ACCC recommended in the DPI Report that the definition of 'personal information' in the Privacy Act should be updated to clarify that it includes these types of technical data, as well as location data and other identifiers that may be used to identify an individual.[13]

We note that Proposal 4.1 is not intended to significantly change the existing definition but is intended to make clear that technical and inferred information (such as IP addresses and other online identifiers) can be personal information. We note the requirement that a person be identifiable or reasonably identifiable from the information would remain.

We support the proposal to make clear that 'personal information' includes these types of technical data that may be used to identify an individual. In line with Proposals 4.1 and 4.2, this could be done through drafting and including relevant examples in the Privacy Act itself, explanatory materials and OAIC guidance. Of these options, the ACCC believes including examples in the Act or explanatory materials is likely to provide the most clarity and certainty.

We also note the proposal to change the word 'about' to 'relates to' in the definition of personal information (Proposal 4.1) would further align the Privacy Act with the terminology used in the CDR legislation. Section 56AI(3) of the CCA states that a person is a CDR consumer for CDR data if the data relates to them as a result of the supply of a good or service to them, the CDR data is held by a CDR participant and the person is reasonably identifiable from the data.

Small business exemption (Chapter 6)

The ACCC supports the proposal to repeal the small business exemption. While the ACCC appreciates the compliance costs that this may impose on small businesses, we note the Report's findings that Australian consumers expect their privacy to be protected regardless of the entity collecting their information, and the submissions to the Discussion Paper which noted the exemption is no longer acceptable in light of the fact that advances in technology have increased the privacy risks small businesses can pose to consumers.[14] The ACCC understands the need for additional consultation to establish how to implement this change appropriately and proportionately.

The ACCC also supports the short-term proposals to remove the exemption for small businesses that trade in personal information with consent, and to prohibit the collection of biometric information for use in facial recognition technology by small businesses. These proposals are appropriate intermediate steps to quickly provide necessary protections for Australian consumers in advance of the full-scale repeal of the small business exemption.

---

[12] ACCC, Privacy Act Review Discussion Paper – ACCC submission, December 2021, pp 2-3.

[13] ACCC, Digital Platforms Inquiry – final report, July 2019, p 34.

[14] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, p 52. See also OAIC, Privacy Act Review – Discussion Paper – Submission by the Office of the Australian Information Commissioner, December 2021, pp 48-49.

The ACCC notes that repealing the small business exemption would help ensure that consumers' personal information would remain protected when it leaves the CDR system. This could include where trusted advisers such as mortgage brokers, lawyers or accountants receive CDR data (which they can receive without being accredited where a consumer provides consent). If a trusted adviser is a small business, they are not currently subject to CDR Privacy Safeguards or the Privacy Act. Removing the small business exemption would ensure that CDR data would be subject to protection under the Privacy Act once it is received by a small business trusted adviser.

Part 2: Consumer rights and protections

The ACCC strongly supports privacy proposals that would provide consumers with additional safeguards and rights in relation to their personal information.

The 'fair and reasonable' test (Chapter 12)

The ACCC supports the introduction of a 'fair and reasonable' test for the collection, use and disclosure of personal information, as an additional privacy safeguard for consumers alongside other relevant proposals in the Report (such as proposals to strengthen notification and consent requirements in Chapters 10 and 11).

However, given that a test of this nature is open to multiple possible interpretations, including in the course of potential litigation and enforcement, the ACCC would stress the importance of carefully drafting the relevant amendments to the Privacy Act, to ensure the 'fair and reasonable' test achieves its intended objectives.

Overseas experience highlights that definitions and guidance are particularly important in relation to the meaning and application of terms that intersect with and/or require a shift in common business practices. For example, differing views on the interpretation of 'legitimate interests' under the EU's General Data Protection Regulation (GDPR) has led to ongoing litigation, placing significant resource burdens on businesses and regulators and giving rise to uncertainty around businesses' obligations.[15]

The ACCC therefore recommends that this test should be supported by clear and definitive guidance (such as through statutory criteria in the Privacy Act itself) to ensure consumers' privacy interests are prioritised, and that the test is not open to be interpreted in a way that gives undue weight to the commercial needs of companies that earn revenue by commercialising consumer information and data.

To this end, the ACCC considers that it will be important to make clear that the framing of this test has reference to what is fair and reasonable in relation to the average consumer, noting that most consumers do not read long and complex privacy policies,[16] and may only have a limited understanding of how their data is used within businesses or shared with other businesses.[17]

This is particularly important given that the length, complexity, ambiguity and inaccessibility of many privacy policies can make them highly challenging for consumers to read and understand. For example, an ACCC review of several large digital platforms' privacy policies

---

[15] For discussion of the concerns about the meaning of 'legitimate interests' in the GDPR, see: SS Rana & Co, Loopholes in the General Data Protection Regulation, 4 June 2018; D Kelleher, What does legitimate interest mean? The CJEU gives its answer in Rīgas, IAPP, 4 May 2017, accessed 16 March 2023.

[16] The 2020 Australian Community Attitudes to Privacy Survey found that only 31% of Australians read online privacy policies, with length of these policies cited as one of the main reasons for this: OAIC, 2020 Australian Community Attitudes to Privacy Survey, September 2020, p 69. See also ACCC, Digital Platforms Inquiry – final report, July 2019, pp 26, 394-397 and 498.

[17] The Consumer Policy and Research Centre (CPRC) found that only 12% of Australian consumers feel they have a good understanding of how their information is collected and shared online. See CPRC, 2020 Data and Technology Survey, p 14.

found they were between 2,500 and 4,500 words long, and many used complex language that would require at least a university education to comprehend.[18]

Rights of the individual (Chapter 18)

New and expanded rights of the individual (Proposals 18.1 to 18.5)

The ACCC supports the proposals to create new consumer rights to objection, erasure and de-indexing, as well as the proposals to enhance the existing rights to access and correction in the Privacy Act.

In particular, the ACCC supports:

- introducing a right for consumers to object to the collection, use or disclosure of their personal information (Proposal 18.2). Given that the Report suggests a likely ground of objection would be that a particular collection is not reasonably necessary and/or not fair and reasonable,[19] this reinforces the need for the drafting and definition of 'fair and reasonable' in legislative amendments to be supported by clear and definitive guidance.
- introducing a right to erasure, whereby an individual may seek to exercise the right to request their personal information be deleted (Proposal 18.3), which would be consistent with Recommendation 16(d) of the DPI Report. As the Report notes, this would also mirror the ability of a consumer to elect to have their redundant data deleted under the CDR.[20]
- introducing a right for consumers to request the de-indexation of online search results containing their personal information, which would be consistent with Recommendation 16(d) of the DPI Report.

The ACCC also supports the proposal not to introduce an additional right to portability in the Privacy Act, but to instead develop this right in the CDR (see section 18.1 of the Report).[21]

This would ensure that a single data portability scheme provides consumers with consistent rights, protections and experiences.

The ACCC recognises that there are important policy questions associated with the introduction of individual data portability rights through the CDR, including the mechanism by which data portability should occur and ensuring strong consumer protections are in place. We support the development of an individual data portability right, following further consideration and the resolution of these issues.

Exceptions (Proposal 18.6)

The ACCC acknowledges the importance of exceptions to the proposed new and expanded rights of the individual, including the need to discourage unreasonable, frivolous or vexatious requests.

The Report proposes to exempt 'relationships with a legal character', such as contracts, from these rights of the individual.[22] Noting the Report's discussion of 'data practices which are terms of service'[23], it will be important to draft this proposed exception carefully, to ensure it is not open to exploitation based on ambiguity in wording. For example, many digital

---

[18] ACCC, Digital Platforms Inquiry – final report, July 2019, pp 405 and 597-598.

[19] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, pp 172-3.

[20] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), sub-div 4.3.4.

[21] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, p 166.

[22] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, pp 181-182.

[23] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, p 173.

platforms frame their terms of service or user agreements as contracts which users accept by using the platform's services or signing up for an account.[24] This could lead to a digital platform or another entity with a similar business model refusing a consumer's otherwise reasonable request for erasure or de-indexation on the grounds of an ongoing contract with the consumer, based only on the fact the consumer continues to use their services. In turn, it could leave a consumer unable to exercise certain rights of the individual for as long as they continue to use any of the entity's services.

Accordingly, when drafting the 'relationships with a legal character' exception for implementation in the Privacy Act, consideration could be given to limiting the exception to cases where the personal information itself is necessary for the entity's performance of a contract to which the consumer is a party, and not circumstances where complying with the consumer's request would merely be unnecessary based on the entity's terms of service.

Direct marketing, targeting and trading (Chapter 20)

Debate on Proposals 20.2 and 20.3

The ACCC supports the Report's proposals to clearly define these terms under the Privacy Act (Proposal 20.1) and to give consumers more rights and protections in relation to these practices (Proposals 20.2 to 20.8).

The ACCC notes there has been considerable debate on several of the proposals in this chapter. In particular, we have observed strong arguments on both sides of the issue of whether Proposals 20.2 (the right to opt out of personal information being used or disclosed for direct marketing purposes) and 20.3 (the right to opt out of receiving targeted advertising) should be changed to 'opt-in', which would mean a consumer would need to provide an entity with consent if they wished to receive targeted advertising or let their data be used for direct marketing purposes.

The ACCC acknowledges that several submissions to the Privacy Act Review Discussion Paper were supportive of these proposals being 'opt out', in the interests of minimising 'consent fatigue' and limiting technological challenges for businesses.[25]

On the other hand, as noted in the Report, the ACCC has previously expressed concerns about the ability of digital platforms and other entities which collect personal information online to use 'dark patterns' – a form of choice architecture[26] which involves intentionally designing user interfaces to confuse users, make it difficult for them to express their actual preferences, or manipulate them into taking certain actions.[27]

The ACCC raised specific concerns that some digital platforms may employ dark patterns to manipulate consumers into selecting more intrusive privacy controls and settings than they otherwise would.[28] There is a risk that consumers' awareness of and ability to exercise their rights to opt out under Proposals 20.2 and 20.3 may be somewhat limited in practice.

It is possible that some of these risks may be partially mitigated by the effective implementation of the proposed 'fair and reasonable' test, as this would require all personal

---

[24] For example, see Google, Google Terms of Service – Country version: Australia, 5 January 2022, accessed 16 March 2023. In these Terms of Service, Google states that 'by using our services, you're agreeing to these terms', and tells consumers they are 'contracting with' Google by using its services and thus accepting these terms.

[25] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, pp 212-213.

[26] 'Choice architecture' is defined as the way that choices are presented to users. User interface design is a form of choice architecture and can influence consumer choices by appealing to certain psychological or behavioural biases. See ACCC, Digital platform services inquiry - September 2022 interim report - Regulatory reform, September 2022, pp 19, 44 and 65-69.

[27] ACCC, Digital platform services inquiry - September 2022 interim report - Regulatory reform, September 2022, p 9.

[28] ACCC, Digital platform services inquiry - September 2022 interim report - Regulatory reform, September 2022, p 68; see also Cyber Security Cooperative Research Centre, Submission to the ACCC Digital Platform Services Inquiry Fifth Report, May 2022, p 3.

information collection to be fair and reasonable in the circumstances, even if a consumer has given consent.

However, to ensure the effectiveness of these measures, the ACCC recommends that entities which collect personal information for direct marketing, or which show targeted advertising should be required to clearly disclose this to consumers, alongside clearly telling consumers how and where they can easily opt out of these practices.

Implementation of Proposal 20.4

The ACCC supports a new requirement for an individual's consent to be obtained to trade their personal information (Proposal 20.4). We also agree on the need to consider such consent requirements in developing obligations for particular designated digital platforms to share certain data (for example, as part of new competition measures proposed in the ACCC's Regulatory Reform report).

The Report correctly points out that some businesses may attempt to circumvent this requirement by making consent to trade personal information a condition of accessing goods and services. We support the Report's suggestion that Australian Privacy Principle (APP) entities relying on such consent be required to demonstrate that trading in personal information is reasonably necessary for their functions or activities.

Consideration could also be given to requiring a more direct connection between the provision of goods or services accessed by a consumer and the need for an entity to trade personal information, to ensure 'bundled consents' are not exploited to allow trading of personal information not related to the actual purpose of providing a good or service to the consumer.

Clarification of the term 'socially beneficial'

Proposal 20.8 recommends prohibiting targeting of individuals based on sensitive information, with an exception for 'socially beneficial' content. To avoid potential ambiguity, the Government could consider clearly and explicitly defining the term 'socially beneficial' in the Privacy Act. This definition could be supplemented with some examples in an explanatory memorandum, noting that our understanding is that the intent of this exception is to allow targeting by public health campaigns and similar activities that are in the public interest.

The ACCC considers that this clarification could help avoid doubt over whether the typical business activities of a digital platform or other data collector are considered 'socially beneficial' based on mission statements and other publicly stated objectives. For example, Meta states on its website that its mission 'is to give people the power to build community and bring the world closer together' and that its products 'empower more than 3 billion people around the world to share ideas, offer support and make a difference.'[29]

Privacy policies and collection notices (Chapter 10)

The ACCC supports the proposals to improve notification requirements for the collection of personal information (Proposals 10.1 to 10.3).

In conjunction with an appropriately calibrated 'fair and reasonable' test, discussed earlier in this submission, the ACCC considers that these proposals could broadly achieve the intended objectives of Recommendation 16(b) in the DPI Report.

Consent and privacy default settings (Chapter 11)

[29] Meta, Meta Investor Relations – FAQs, accessed 16 March 2023.

The ACCC supports revising the definition of consent under the Privacy Act to make clear that consent must be voluntary, informed, current, specific and unambiguous (Proposal 11.1); requiring that withdrawal of consent be as easy as giving consent (Proposal 11.3); and requiring online service providers to reflect the 'privacy by default' framework of the Privacy Act through their online privacy settings and by being clear and transparent with users about privacy settings (Proposal 11.4).

These features of consent reflect those found in the CDR Rules, and they broadly align with the intended objectives of Recommendation 16(c) of the DPI Report. This DPI Report recommendation originally proposed that consent be required for any collection, use or disclosure of personal information with limited exceptions. However, we note the Report's concern around 'consent fatigue' generated by a broader consent regime, and the additional proposed safeguard of the 'fair and reasonable test'.

Likewise, the ACCC supports proposals that would result in the Privacy Act better aligning with the CDR Privacy Safeguards, and we support using the standardised consent taxonomies developed for the CDR as the basis for developing future OAIC guidance or standards for consent requests, in the context of the Privacy Act (Proposal 11.2). This would assist entities to understand how the elements of valid consent should be interpreted in the online context, reduce confusion for consumers and promote a more consistent privacy regime.

The ACCC considers that there is merit in considering whether even greater alignment between the CDR and the Privacy Act could remove or reduce the need for a dual privacy regime, if the protections in the Privacy Act were as strong as the CDR Privacy Safeguards.

The ACCC notes that participants in the CDR have provided feedback that having two sets of privacy protections across the Privacy Act and the CDR for what can be the same data (but in different contexts) is a barrier to adoption, due to the complexity, regulatory requirements and cost of dual regimes. This may undermine the objective of the CDR as a competition reform. A single, strong privacy regime, to the standard of the CDR Privacy Safeguards, would simplify regulatory requirements, level the playing field for providers and allow greater certainty for consumers and businesses.

Additional protections (Chapter 13)

The ACCC supports the proposal to require APP entities to conduct a privacy impact assessment (PIA) for all activities with high privacy risks, and that the Privacy Act should include a clear definition of a 'high privacy risk activity' (Proposal 13.1).

The ACCC also agrees with the proposal that this definition should be supplemented with lists of risk factors and examples in explanatory materials or OAIC guidance, and that specific high-risk practices should be set out in the Privacy Act (also Proposal 13.1). This list of examples should be clearly qualified as being non-exhaustive, given the rapidly evolving variety of ways in which data may be collected from consumers.

For the sake of clarity, the ACCC suggests that the definition and/or list of examples of a 'high privacy risk activity' should articulate whether an additional PIA is required in the case of a merger between two companies, in cases where at least one of the entities involved engages in activities that may carry a high privacy risk.

We note that the Report's suggested list of 'high privacy risk activities' appropriately includes 'the use of biometric templates or biometric information … when collected in publicly accessible spaces',[30] and note that this should explicitly apply to the combination of scraped personal information and use of biometric facial recognition employed by organisations such

[30] Attorney-General's Department, Privacy Act Review Report 2022, February 2023, p 124.

as Clearview AI. We also support broader consideration of how facial recognition technology and other biometric information may be addressed by this new PIA proposal (Proposal 13.2).

Research (Chapter 14)

The ACCC supports the proposed legislative provision permitting 'broad' consent to the use of personal information for the purposes of research, as well as the proposed expansions to the existing research exceptions under the Privacy Act.

The ACCC considers that these changes should help achieve greater transparency and improved research outcomes, provided that these 'broad' consent provisions are limited to the research purposes detailed in the Report.

Security, retention and destruction (Chapter 21)

The ACCC supports the Report's proposals to provide greater clarity around the security, retention and destruction provisions in the Privacy Act and APPs (Proposals 21.1 to 21.8).

Allowing entities to set their own minimum and maximum retention periods has a number of advantages, as outlined in the Report. However, some digital platforms, data brokers and other entities whose business models rely on monetising consumer data may argue they have a commercial need to retain this information indefinitely.

To address this risk, it may be worth considering whether to prescribe defined maximum retention periods for certain types of personal information (such as sensitive information), either as part of APP 11 or through the OAIC guidance recommended in Proposal 21.5 in relation to APP 11.2. These periods could vary based on the type and sensitivity of personal information being retained.

Part 3: Regulatory and enforcement considerations

The ACCC continues to support the OAIC having the necessary enforcement and investigative tools to help ensure the effectiveness of reforms to the Privacy Act. We also note that several of the Report's proposals would build on recent relevant legislative amendments.[31]

New codes and code-making powers (Chapters 5 and 16)

The ACCC supports new code-making powers for the OAIC, as suggested in Proposals 5.1 and 5.2. However, we would suggest extending the second limb of Proposal 5.1 (currently requiring that 'there is unlikely to be an appropriate industry representative to develop the code') to also incorporate circumstances where an industry representative exists but has not satisfactorily developed such a code within an appropriate timeframe. Such timeframes could be defined in the Privacy Act or through OAIC guidance.

The ACCC also supports the proposed Children's Online Privacy Code (Proposal 16.5).

Organisational accountability (Chapter 15)

The ACCC supports requiring APP entities to record the purpose or purposes for which they collect personal information (Proposal 15.1). This proposal should help improve APP entities' transparency, compliance and accountability from a regulatory perspective.

Accountability requirements of this nature could also make it easier for consumers, regulators and other relevant parties to determine whether an APP entity's collection of personal information was fair and reasonable in the circumstances.

---

[31] Notably, the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth).

A direct right of action (Chapter 26)

The ACCC supports the proposal to introduce a direct right of action, which would permit individuals to apply to the courts for relief in relation to an alleged interference with their privacy under the Privacy Act (Proposal 26.1).

Specifically, in line with Recommendation 16(e) of the DPI Report, the ACCC continues to support a right of action that empowers consumers to seek compensatory, aggravated and exemplary damages (depending on the circumstances) for the financial and non-financial harm they suffer due to a breach of the Privacy Act or an APP.[32]

This right of action would give consumers greater control over their own personal information, by offering them an avenue of judicial redress which does not require them to rely on the OAIC alone to take representative action, thus likely delivering additional benefits such as reducing the enforcement burden on the OAIC[33] and providing additional incentives for APP entities to comply with their privacy obligations.[34]

The ACCC also considers that enacting a personal right of action for consumers is a critical step in ensuring the effectiveness of the proposed new consumer rights and safeguards discussed elsewhere in the Report, such as the 'fair and reasonable' test (Chapter 12) and the rights of the individual (Chapter 18).

A statutory tort for serious invasions of privacy (Chapter 27)

The ACCC supports the proposal for a new statutory tort for serious invasions of privacy that fall outside the scope of the Privacy Act. This proposal would align with Recommendation 19 of the DPI Report, as well as the 2014 Australian Law Reform Commission report which provided the model for this proposed tort.[35]

[32] ACCC, Digital Platforms Inquiry – final report, July 2019, pp 473-475.

[33] Dr Katharine Kemp and Dr Rob Nicholls, Submission to the ACCC Digital Platforms Inquiry, March 2019, p 7.

[34] OAIC, Privacy Act Review – Discussion Paper – Submission by the Office of the Australian Information Commissioner, December 2021, p 206.

[35] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report No 123, September 2014.

Appendix A – Privacy-related recommendations from the DPI Final Report

Recommendation 16: Strengthen protections in the Privacy Act

16(a) Update 'personal information' definition: Update the definition of 'personal information' in the Privacy Act to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.

16(b) Strengthen notification requirements: Require all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party), unless the consumer already has this information or there is an overriding legal or public interest reason.

The notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and must clearly set out how the APP entity will collect, use and disclose the consumer's personal information. Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user.

To provide consumers with a readily understood and meaningful overview of an APP entity's data practices and as a means of reducing their information burden, it may also be appropriate for these requirements to be implemented along with measures such as the use of multi-layered notifications or the use of standardised icons or phrases.

16(c) Strengthen consent requirements and pro-consumer defaults: Require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.

Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled. Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian.

It may also be appropriate for the consent requirements to be implemented along with measures to minimise consent fatigue, such as not requiring consent when personal information is processed in accordance with a contract to which the consumer is a party, or using standardised icons or phrases to refer to certain categories of consents to facilitate consumers' comprehension and decision-making.

16(d) Enable the erasure of personal information: Require APP entities to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.

16(e) Introduce direct rights of action for individuals: Give individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the Privacy Act.

16(f) Higher penalties for breach of the Privacy Act: Increase the penalties for an interference with privacy under the Privacy Act to mirror the increased penalties for breaches of the Australian Consumer Law.

Recommendation 17: Broader reform of Australian privacy law

Broader reform of Australian privacy regime to ensure it continues to effectively protect consumers' personal information in light of the increasing volume and scope of data collection in the digital economy.

This reform should have regard to the following issues:

1. **Objectives**: whether the objectives of the Privacy Act should place greater emphasis on privacy protections for consumers including protection against misuse of data and empowering consumers to make informed choices.
2. **Scope**: whether the Privacy Act should apply to some of the entities which are currently exempt (for example small businesses, employers, registered political parties, etc.).
3. **Higher standard of protections**: whether the Privacy Act should set a higher standard of privacy protection, such as by requiring all use and disclosure of personal information to be by fair and lawful means.
4. **Inferred information**: whether the Privacy Act should offer protections for inferred information, particularly where inferred information includes sensitive information about an individual's health, religious beliefs, political affiliations.
5. **De-identified information**: whether there should be protections or standards for deidentification, anonymisation and pseudonymisation of personal information to address the growing risks of re-identification as datasets are combined and data analytics technologies become more advanced.
6. **Overseas data flows**: whether the Privacy Act should be revised such that it could be considered by the European Commission to offer 'an adequate level of data protection' to facilitate the flow of information to and from overseas jurisdictions such as the EU.
7. **Third-party certification**: whether an independent certification scheme should be introduced.

Recommendation 18: OAIC privacy code for digital platforms

An enforceable code of practice developed by the OAIC, in consultation with industry stakeholders, to enable proactive and targeted regulation of digital platforms' data practices (DP Privacy Code). The code should apply to all digital platforms supplying online search, social media, and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information.

The DP Privacy Code should be enforced by the OAIC and accompanied by the same penalties as are applicable to an interference with privacy under the Privacy Act. The ACCC should also be involved in developing the DP Privacy Code in its role as the competition and consumer regulator.

The DP Privacy Code should contain provisions targeting particular issues arising from data practices of digital platforms, such as:

1. **Information requirements:** requirements to provide and maintain multi-layered notices regarding key areas of concern and interest for consumers. The first layer of this notice should contain a concise overview followed by more detailed information in subsequent layers. The final layer of the notice should contain all relevant information that details how a consumer's data may be collected, used, disclosed and shared by the digital platform, as well as the name and contact details for each third party to whom personal information may be disclosed.

2. **Consent requirements**: requirements to provide consumers with specific, opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service and, where consents relate to the collection of children's personal information, additional requirements to verify that consent is given or authorised by the child's guardian.
3. **Opt-out controls**: requirements to give consumers the ability to select global optouts or opt-ins, such as collecting personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes.
4. **Children's data**: additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimise the collection, use and disclosure of children's personal information.
5. **Information security**: requirements to maintain adequate information security management systems in accordance with accepted international standards.
6. **Retention period**: requirements to establish a time period for the retention of any personal information collected or obtained that is not required for providing the core consumer-facing service.
7. **Complaints-handling**: requirements to establish effective and timely mechanisms to address consumer complaints.

The ACCC considers that this recommendation could align with the Government's March 2019 announcement to create a legislated code applying to social media and online platforms which trade in personal information.

Recommendation 19: Statutory tort for serious invasions of privacy

Introduce a statutory cause of action for serious invasions of privacy, as recommended by the Australian Law Reform Commission (ALRC). This cause of action provides protection for individuals against serious invasions of privacy that may not be captured within the scope of the Privacy Act. The cause of action should require privacy to be balanced against other public interests, such as freedom of expression and freedom of the media. This statutory cause of action will increase the accountability of businesses for their data practices and give consumers greater control over their personal information.