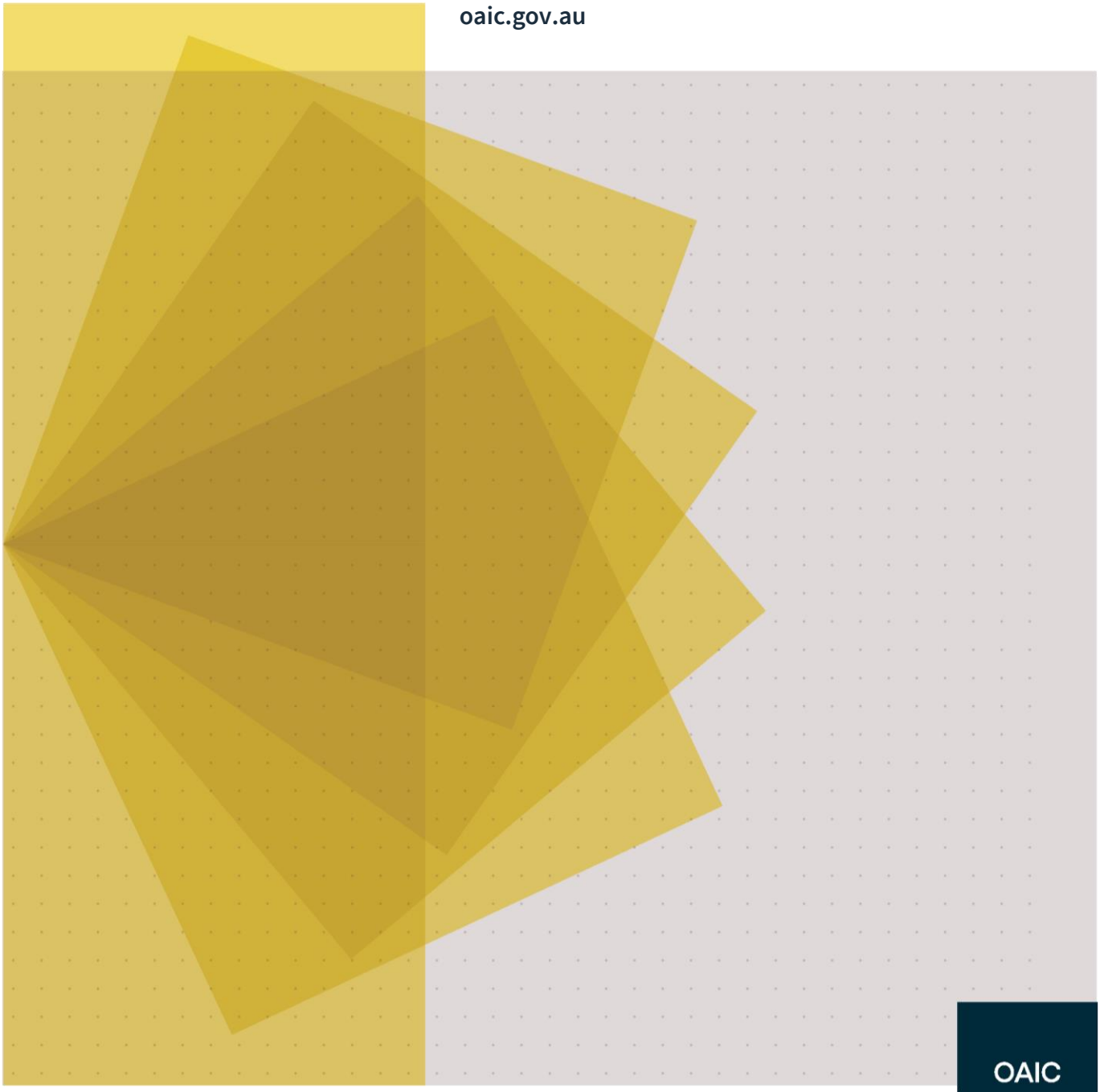
Australian Government

Office of the Australian Information Commissioner

Customer loyalty schemes review

Submission of the Office of the Australian Information Commissioner on the Australian Competition and Consumer Commission's draft report

oaic.gov.au



OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Australian Competition and Consumer Commission (ACCC) on its draft report on customer loyalty schemes (draft report).
2. The draft report examines consumer and competition issues associated with customer loyalty schemes in Australia and includes a detailed examination of the way in which personal information is collected, used and disclosed by operators of customer loyalty schemes.
3. The data practices identified by the ACCC, and the corresponding draft recommendations relate to the application of the *Privacy Act 1988* (Privacy Act) and reflect many of the findings and recommendations of the ACCC's Digital Platforms Inquiry (DPI) final report.[1]
4. The OAIC has responded to the DPI final report with broad support for the recommendations subject to some suggestions aimed at ensuring the interoperability of Australia's data protection laws globally, as well as striking the right balance between an individual's ability to self-manage their privacy, and the accountability of those entrusted with the personal information of Australians.[2] Implementation of the DPI recommendations are likely to address some of the concerns outlined by the ACCC in this draft report.
5. The OAIC provides the comments below in relation to the draft report.

Data practices of loyalty schemes identified in the draft report

6. As the draft report outlines, loyalty schemes derive significant value from consumers by collecting data, including personal information, from members, and use this information to profile consumers and generate revenue by producing insights about consumer's purchasing behaviour.
7. The ACCC has outlined concerns about the business and data practices of loyalty schemes, including:

- presenting privacy policies in a way that consumers cannot readily understand
- seeking broad consents from consumers and making vague disclosures to consumers about the collection, use and disclosure of their data
- providing consumers with limited insight and control over the sharing of their data with third parties
- providing a limited ability for consumers to opt out of targeted advertising delivered by third parties on behalf of loyalty schemes.

8. Entities regulated by the Privacy Act (APP entities) – including those operating loyalty schemes – are required to manage personal information in an open and transparent way in accordance with the Australian Privacy Principles (APPs), including by having a clearly expressed and up to date privacy policy about the management of personal information by the entity.[3] There are specific obligations regarding the collection, use and disclosure of personal information (APP 3 and APP 6), as well as in relation to direct marketing practices (APP 7). APP entities are also

[1] ACCC, Digital Platforms Inquiry, Final Report, 26 July 2019, https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry

[2] The OAIC's submission to Treasury regarding the DPI final report will become available online in due course.

[3] Australian Privacy Principle (APP) 1.

required under APP 5 to take reasonable steps to notify individuals about important matters relating to the collection, use and disclosure of the individual's personal information, including the purposes for which personal information is collected and disclosures to third parties.

9. The OAIC recognises the popularity of loyalty schemes amongst Australian consumers and the large amounts of data collected, used and disclosed via these loyalty schemes. This includes information that is collected passively (such as tracking through apps, transactions and social media activity) and information that is able to be inferred through data matching and analytics.

10. The OAIC has previously conducted limited scope assessments[4] of some of Australia's loyalty schemes[5]. The OAIC's assessments included suggestions relating to the navigability and readability of privacy policies and collection notices, and the handling and use of personal information collected by loyalty schemes.

11. The ACCC's digital platforms inquiry has provided an in-depth analysis of data handling practices of digital platforms, and the draft report provides comprehensive research into loyalty schemes which indicates that data collection practices of loyalty schemes are increasing in scale and complexity. The OAIC's assessments of some of Australia's loyalty schemes noted that privacy policies and collection notices should be regularly reviewed to ensure they adequately explain the use of a member's personal information, especially if the nature and scale of marketing and data analytics activities changes.[6]

12. The OAIC supports recommended reforms to the Privacy Act made by the DPI, designed to increase transparency, choice and control over the handling of personal information and ensure that Australia's regulatory framework remains fit for purpose in the digital age.

ACCC's draft recommendations

13. The ACCC makes four recommendations in the draft report. Recommendations 1 and 2 relate to competition and consumer law, while recommendations 3 and 4 relate to the Privacy Act and privacy regulatory framework.

14. The OAIC supports recommendations to enhance the ways in which personal information is collected, used and disclosed by APP entities to provide consumers with greater choice, transparency and control over how their personal information is used by loyalty schemes.

Draft recommendation 3: improve the data practices of loyalty schemes

15. The ACCC suggests that loyalty schemes should take the following steps to improve their data practices:

---

[4] Section 33C of the Privacy Act establishes that the Commissioner may conduct an assessment relating to the Australian Privacy Principles, amongst other things (s 33C(1)(a)(i)). Assessments are a snapshot of personal information handling practices relating to an APP entity at a certain time and in a particular location.

[5] See for example: Loyalty program assessment: Woolworths Rewards (field work conducted in February 2016) <https://www.oaic.gov.au/privacy/privacy-assessments/loyalty-program-assessment-woolworths-rewards-woolworths-limited/>, flybuys (field work conducted in November 2015): <https://www.oaic.gov.au/privacy/privacy-assessments/loyalty-program-assessment-flybuys-coles-supermarkets-australia-pty-ltd/>, Qantas Frequent Flyer (fieldwork conducted in May-June 2017): <https://www.oaic.gov.au/privacy/privacy-assessments/management-of-personal-information-qantas-frequent-flyer/., Velocity Frequent Flyer (fieldwork conducted July 2017): <https://www.oaic.gov.au/privacy/privacy-assessments/management-of-personal-information-velocity-frequent-flyer/>.

[6] See Qantas Frequent Flyer assessment report at paragraphs 4.86 and Velocity Frequent Flyer assessment report at paragraphs 4.86.

Reviewing their clickwrap agreements for unfair contract terms, including by assessing the potential consumer detriment of unilateral variation terms

16. Through the use of clickwrap agreements, organisations may bundle together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.[7] A request for consent to handle personal information tied to the provision of a contract or service also impacts privacy where the handling of that personal information is not necessary for the performance of the contract or service.[8]

17. The OAIC supports the ACCC's recommendation 16(c) in the DPI that consent should require a clear affirmative act that is freely given, specific, unambiguous and informed. The OAIC also suggests that consideration is given to other mechanisms to enhance the specificity of consent such as:

    a. the use of graduated consent – where an individual can give consent to different uses of their data throughout their relationship with a service provider[9]

    b. the use of tiered consent – where an individual may consent to disclosing increasing amounts of personal information in exchange for different products or levels of services.

Improving the clarity, accessibility, navigability and readability of privacy policies, including by using definitions consistent with those in the Privacy Act

18. APP 1.3 requires APP entities to have a clearly expressed and up to date privacy policy (APP privacy policy) explaining how personal information will be managed by the entity. An APP privacy policy should be easy to understand, easy to navigate and only include information that is relevant to the management of personal information by the entity.[10] The OAIC made suggestions in its assessments of loyalty schemes regarding these matters.[11]

19. The OAIC agrees that organisations –including those operating loyalty schemes – should adopt the definition of 'personal information,' as it is defined in Privacy Act, consistently across their policies. The OAIC has previously made similar suggestions in relation to the use of consistent definitions during targeted assessments of agencies and organisations.[12] This will ensure that

---

[7] See the OAIC's APP Guidelines, Chapter B for guidance on bundled consent <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/>

[8] The European Data Protection Board's interpretation of article 7(4) of the GDPR is that consent will not be presumed to be freely given where the consent is tied to the provision of a contract or service, and the processing of personal data is not necessary for the performance of the contract or service. This is to ensure that consent for the processing of personal data cannot directly or indirectly become the counter-performance of a contract. For more information, see the Article 29 Working Party (endorsed by the European Data Protection Board), Guidelines on consent under Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030> section 3.1.2

[9] See discussion in the UK Information Commissioner's Office (UK ICO) report: *Big Data, AI, Machine Learning and Data Protection*, 2017, page 30 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-dataprotection.pdf

[10] See the OAIC's APP Guidelines, Chapter 1 for guidance in relation to developing an APP privacy policy <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information/>

[11] See Qantas Frequent Flyer assessment report at paragraphs 4.96-4.98 and Velocity Frequent Flyer assessment report at paragraphs 4.95-4.96.

[12] See, for example, OAIC Audit report: National Repositories Service – eHealth record System Operator, 1 November 2014 <https://www.oaic.gov.au/privacy/privacy-assessments/national-repositories-service-ehealth-record-system-operator-audit-report/> and Velocity Frequent Flyer assessment report at paragraph 4.22 .

organisations comply with their legal obligations under APP 1, including setting out the kinds of personal information collected, how and why it is collected, used and disclosed.[13]

20. The OAIC has published a guide to developing an APP privacy policy which organisations may find useful in reviewing their approaches to informing consumers about how they handle personal information.[14]

Minimising information overload for consumers by prominently presenting relevant aspects of their terms, conditions and privacy policies to consumers during key interactions

21. The OAIC supports measures to minimise information overload for consumers as this will ensure consumers can provide meaningful consent and exercise choice and control over how their personal information is collected, used and disclosed. Organisations should note that the timing of privacy notices can occur dynamically to ensure that information is provided to individuals at the right time (such as during key interactions) and in a way that is easy to read and understand in context.[15]

22. In particular, the OAIC supports measures to create a common language in relation to privacy and personal information, which could include the use of standardised icons or phrases, to help consumers understand important aspects of privacy policies, privacy notices and data practices.

23. Economy-wide enforceable rules, standards, binding guidance or a code could be developed to operationalise a common language more broadly across the economy. Legislative amendment to the Privacy Act could be considered to enable the Australian Information Commissioner to make such rules, standards or an economy-wide code over time. This would assist in consumer understanding and reduce regulatory fragmentation.

Ending the practice of automatically linking customers' payment cards to their profile to track their purchasing behaviour and transaction activities when they do not scan their loyalty card

24. The ACCC recommends that loyalty schemes cease the practice of automatically linking customers' payment cards to their profile to enable tracking of purchasing behaviour and transaction activities even where they do not scan their loyalty card.

25. Personal information may only be collected where it is reasonably necessary for, or directly related to, loyalty s' functions or activities.[16] The OAIC notes that the draft report provides that loyalty schemes are not compensating their members with points as a result of this tracking. Furthermore, we note that a higher threshold applies to the collection of information that is sensitive information.[17]

26. In addition, consumers may not appreciate that their purchasing behaviour and transaction activities may continue to be tracked even after they decide to stop using their loyalty card. This impacts consumers' ability to make meaningful decisions in relation to the collection, use and

[13] See APP 1.4.

[14] OAIC, Guide to developing an APP privacy policy <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/#top>

[15] See the OAIC's Guide to data analytics and the Australian Privacy Principles for a best practice approach to privacy notices <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/>.

[16] See APP 3.

[17] See APP 3.3.

disclosure of their personal information by loyalty schemes and raises whether collection is by fair means.

27. The Privacy Act provides privacy complaint mechanisms for individuals which contemplate that in general an individual will raise a privacy issue with a regulated entity in the first instance and if unresolved, may lodge a complaint with the OAIC.[18]

Outlining with which entities consumer data is being shared and for what purposes, and drawing to consumer's attention how their data is being handled (including, for example, by providing a prominent notice during relevant interactions with customers)

28. The OAIC supports point in time notification specific to interactions with customers. The OAIC's guidelines provide notification should occur at or before the time an APP entity collects an individual's personal information. This is in order to assist the individual to make an informed choice about whether to provide the personal information to the APP entity. If that is not practicable, notification may occur as soon as practicable after collection occurs. It is the responsibility of the APP entity to be able to justify that it is not practicable to give notification or ensure awareness before or at the time of collection.[19]

29. The APPs contain several important requirements in relation to the disclosure of personal information to other entities, including:

- An APP privacy policy must contain information on whether the entity is likely to disclose personal information to overseas recipients[20], and the countries in which such recipients are likely to be located.[21]
- An APP entity must notify the individual of any other entity, body or person to which the APP entity usually discloses personal information that is collected[22] including whether the APP entity is likely to disclose personal information to overseas recipients,[23] and provide the countries in which such recipients are likely to be located.[24]
- If an APP entity holds personal information about an individual that was collected for a particular (the primary) purpose, it must not use or disclose the information for a secondary purpose unless the individual has consented, or an exception applies.[25]
- An entity must take reasonable steps to ensure that an overseas recipient of personal information does not breach the APPs prior to disclosing personal information overseas.[26]

30. Loyalty schemes must comply with these obligations and periodically review their practices to ensure best privacy practice in this regard. A Privacy Impact Assessment (PIA) would assist loyalty schemes to map customer data flows and privacy risks which may emerge at various stages of collection, use and disclosure of personal information. For example, the data flows set

[18] See the OAIC's website on how to lodge a privacy complaint: <https://www.oaic.gov.au/privacy/privacy-complaints/>

[19] See the OAIC's APP Guidelines, Chapter 5 for more information on the notification of the collection of personal information < https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information/>

[20] APP 1.4(f).

[21] APP 1.4(g).

[22] APP 5.2.(f).

[23] APP 5.2(i).

[24] APP 5.2(j)

[25] See APP 6.

[26] APP 8.

out on page 36 of the draft report indicate movement of personal information that is collected actively and voluntarily, passively, and inferred from other sources.

31. The OAIC has also published guidance in relation to conducting PIAs,[27] as well as a guide to data analytics and the Australian Privacy Principles[28] which may assist loyalty schemes in the responsible handling of personal information.

Disclosing to consumers the sources of third party advertising, the sources of the consumer data used to inform that advertising, and the channels through which they may receive targeted advertising and how their consumer data may be used to generate leads (including, for example, via a regularly updated online notice)

32. The ACCC expresses concern in relation to certain targeted advertising practices, including opacity in relation to the extent of which customers are tracked online and the source of the targeted advertising that is being delivered to the consumer. The lack of specificity and detail around targeted advertising is noted as imposing a significant barrier to consumers' understanding of how their personal information is used, and the implications of this use. This is problematic as it impacts on consumers' ability to provide meaningful consent and reduces organisational accountability for the open and transparent management of personal information.

33. The OAIC has acknowledged similar concerns around a lack of transparency raised during the DPI and has expressed support for greater transparency around the use of consumer data, including personal information, for targeted advertising processes.

34. Where personal information is used to communicate directly with an individual to promote goods and services – otherwise known as direct marketing – APP 7 may apply.[29] Importantly, organisations engaging in direct marketing must provide a simple means by which the individual may request not to receive direct marketing communications from the organisation. If an individual makes such a request to stop receiving direct marketing communications or a request to an organisation to provide its source of personal information, the organisations must give effect to this request within a reasonable period.[30]

35. The ACCC makes several recommendations in the DPI final report in relation to targeted advertising, including that default settings which enable data processing for purposes other than performance of a contract – such as in order to conduct targeted advertising – be pre-selected to 'off'. The OAIC is generally supportive of the default setting aspect of this recommendation as a privacy-enhancing mechanism which reflects consumer preferences and expectations.

Providing consumers of loyalty schemes with more meaningful controls over the collection, use and disclosure of their data to respond to consumer demands to align the data practices of loyalty schemes with the data preferences of consumers

36. The ACCC notes that consumers who are concerned about the data practices of loyalty schemes but wish to continue to participate may benefit from being given the choice to meaningfully opt

---

[27] OAIC, Guide to undertaking privacy impact assessments < https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>

[28] OAIC, Guide to data analytics and the Australian Privacy Principles <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/>

[29] APP 7 does not apply to the extent that the *Do Not Call Register Act 2006* (Cth), the *Spam Act 2003* (Cth) or any other legislation prescribed in the *Privacy Regulation 2013* (Cth) applies.

[30] See APP 7.6 and 7.7.

out of certain data practices in a way that suits their own privacy preferences. The concerns and consumer preferences outlined in the draft report reiterate the need for greater choice and control over personal information handling practices.

37. The OAIC considers that a right for individuals to object to the handling of personal information for specific purposes would be beneficial, particularly to those who wish to continue using a service but do not agree to certain data practices.[31] Such a right would complement the right to erasure as recommended in the DPI final report, which would require APP entities to comply with an individual's request to erase personal information (subject to certain exceptions).

Draft recommendation 4: strengthen protections in the Privacy Act and broader reform of Australian privacy law

38. The ACCC notes that the concerns it has identified in the draft report have direct parallels with those in the ACCC's DPI final report. The ACCC is of the view that the findings in the draft report reinforce the recommendations made in the DPI final report and further support the recommendations for economy-wide changes in relation to privacy law.

39. The OAIC generally agrees with the ACCC's position in this regard and is broadly supportive of the DPI final report recommendations, subject to some targeted suggestions to ensure that the right balance is struck between privacy self-management and organisational accountability.

40. We note that the DPI final report recommended additional protections for vulnerable groups such as children in the context of digital platforms, given the substantial power imbalances and information asymmetries which exist between those groups and digital platforms. Although the draft report does not explore the extent to which children are engaged with loyalty schemes, we suggest that some consideration could be given to whether any additional protections are required for vulnerable groups in this context, noting the increasing prevalence of loyalty schemes across the retail and entertainment sector.

41. We provide the following comments, consistent with our submission in response to the DPI final report.

Updating the definition of personal information in line with current and likely future technological developments to capture any technical data relating to an identifiable individual

42. We support a revision of the definition of 'personal information' in the Privacy Act to specifically capture technical data such as IP addresses, device identifiers, location data and other online identifiers that may be used to identify an individual.

Strengthening notification requirements to ensure that the collection of consumers' personal information directly or by a third party is accompanied by a notice of the collection that is concise, intelligible and easily accessible, written in clear and plain language, provided free of charge and accompanied by appropriate measures to reduce the information burden on consumers

43. We support the strengthening of existing notice requirements under APP 5, subject to appropriate legal and public interest exceptions. Requirements for notices to be concise, transparent, intelligible, written in clear and plain language and provided free of charge provide important privacy protections that assist individuals to exercise choice and control over how their personal information is collected, used and disclosed.

[31] See Article 21 of the GDPR

44. We acknowledge that a balance must be struck between appropriate, strengthened notice requirements and the practical consequences of increased provision of notices to consumers, which could include increased notification fatigue.

Strengthening consent requirements to require that consents are freely given, specific, unambiguous and informed, and that any settings for additional data collection must be pre-selected to 'off'

45. The OAIC supports strengthened consent requirements, including that consent should require a clear, affirmative act that is freely given, specific, unambiguous and informed. This reform would align the definition of consent more closely with the European Union General Data Protection Regulation (EU GDPR).[32] The OAIC also suggests that consideration be given to other mechanisms to enhance the specificity of consent, including:

- the use of graduated consent – where an individual can give consent to different uses of their data throughout their relationship with a service provider[33]
- the use of tiered consent – where an individual may consent to disclosing increasing amounts of personal information in exchange for different products or levels of services.

46. The OAIC suggests that greater certainty about consent requirements could be achieved through economy-wide enforceable rules, standards, binding guidance or a code to create a common language to assist individuals in understanding privacy practices and providing meaningful consents to the collection, use and disclosure of personal information. This could include the use of standardised icons or phrases.

Ensuring consents are required whenever personal information is collected, used or disclosed by an entity subject to the Privacy Act, unless the personal information is necessary to perform a contract to which a consumer is a party, required under law or otherwise necessary in the public interest

47. The OAIC notes that while consent is an important part of Australia's privacy framework, it is not the only basis for permitting the handling of personal information under the Privacy Act.[34] Seeking freely given, specific, unambiguous and informed consent may, in some circumstances, be impractical or overly burdensome. Seeking consent for routine purposes may also undermine the quality of consents obtained and result in consent fatigue for consumers.

48. Overreliance on consent shifts the burden to individuals to critically analyse and decide whether they should disclose their personal information in return for a service or benefit. In the digital age, where data flows and technologies used to process personal information are increasingly complex and difficult to understand,[35] individuals are not always well placed to assess the risks and benefits of providing their personal information.[36]

---

[32] Article 4(11) of the GDPR defines 'consent' of the data subject as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[33] See discussion in the UK Information Commissioner's Office (UK ICO) report: *Big Data, AI, Machine Learning and Data Protection*, 2017, page 30 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[34] See, for example: APP 3, APP 6, APP 7 and APP 8.

[35] See discussion around the challenges of seeking consent in relation to the use of artificial intelligence technologies in the OAIC submission to Standards Australia, *Developing Standards for Artificial Intelligence: Hearing Australia's Voice – Submission to Standards Australia*, 26 August 2019 <https://www.oaic.gov.au/engage-with-us/submissions/developing-standards-for-artificial-intelligence-hearing-australias-voice-submission-to-standards-australia/>

[36] See the discussion of human behaviour in Office of the Privacy Commissioner of Canada's Discussion Paper - *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (2016) <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf>. Page 9 refers to

49. Accordingly, in addition to appropriately strengthened consents, we also support the introduction of organisational accountability measures that will redress the imbalance in knowledge and power between individuals and organisations – such as codifying the obligation on entities to use and disclose personal information 'fairly and lawfully', and adopting express requirements to conduct compulsory privacy impact assessments for the collection, use or disclosure of personal information involving high risks, and to implement privacy by design and default.

50. It is also important to ensure that consent is used to support real choice and control. This may require consideration of the need to constrain certain data or business practices which are contrary to consumers' expectations in relation to privacy. The OAIC suggests that the development of 'no-go zones' be considered for suitability in Australia, due to the enhanced privacy protection they provide against certain data practices.[37]

Requiring entities subject to the Privacy Act to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, except in certain circumstances

51. The OAIC supports the recommendation to enable individuals to request the erasure of their personal information subject to various exceptions. Under this recommendation, APP entities will be required to comply with the request to erase personal information without undue delay, unless there is an overriding reason for the information to be retained.

52. In addition, the OAIC recommends that consumers be notified of their ability to request the erasure of their personal information. This could be modelled on similar requirements in Article 13 of the EU GDPR.

53. As discussed above, we recommend that the right to erasure be complemented by a right for individuals to object to the handling of their personal information for specific purposes. A right to object could be modelled on a similar protection contained in Article 21 of the EU GDPR.

54. The OAIC also suggests that consideration be given to an obligation on all APP entities – including loyalty schemes – to delete all user data on request. A comparative provision is found in subsection 17(3) of the *My Health Records Act 2012* (Cth), which requires the destruction of records containing health information in a My Health Record upon request by the individual. This provision was implemented in response to the Australian community's calls for stronger privacy and security protections within the My Health Record system and reflects consumer expectations about continuing access to data. A similar ability to request (and require) deletion of data is built into the legislative framework of the Consumer Data Right and supported by data standards.

Introducing direct rights for individuals to bring actions or class actions before the courts to seek compensation for an interference with their privacy under the Privacy Act

55. The OAIC supports the introduction of a direct right of action for individuals to seek compensation under the Privacy Act for an interference with their privacy. This

numerous studies that have shown that individuals will say they care about privacy yet at the same time disclose significant quantities of personal information online. This may be because individuals have limited time and energy to fully engage in privacy policies and find it difficult to quantify privacy risks compared to concrete rewards for disclosing personal information online.

[37] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3),* May 2018 <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/> Examples of 'no-go zones' include profiling or categorisation that leads to unfair, unethical or discriminatory treatment contrary to human rights law, and the collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual.

recommendation, if implemented, would bring the Australian privacy framework into line with other countries including the United Kingdom, New Zealand and those in the European Union.

56. We also recommend consideration of whether this direct right of action may be supplemented by legislative options for the OAIC to exercise[38]:

- a right to intervene in proceedings (or alternatively to seek the leave of the court to intervene)
- a right to seek the leave of the court to act in the role of amicus curiae in the proceedings.

Recommendations for broader reform of the Australian privacy regime

57. The OAIC supports the ACCC's recommendations in relation to reviewing the current objectives and scope of the Privacy Act to ensure that Australia's privacy regulatory framework remains fit for purpose in the digital age. The OAIC also supports the introduction of a statutory tort of privacy.

58. The OAIC is also supportive of the introduction of a requirement for APP entities to use and disclose information 'fairly and lawfully' and has suggested that the need for additional protections for inferred and de-identified information be considered as part of a broader review of the privacy regulatory framework. Additionally, the OAIC is supportive of measures to increase privacy awareness amongst Australians, noting that this is an important protective factor for individuals navigating online platforms and services.

59. The OAIC has also recognised that there is an increasing convergence of privacy and competition and consumer regulatory frameworks globally. Several of the recommendations in the DPI final report reflect the increasing intersection of these jurisdictions. The OAIC therefore recommends that consideration be given to facilitating greater collaboration between the ACCC and OAIC through an information-sharing power to allow for the exchange of information in appropriate circumstances – such as where a privacy issue arises in the context of a competition and consumer matter. This would avoid the time and costs to all parties in duplicating the collection of data from regulated entities.

Conclusion

60. The OAIC looks forward to reviewing the final report on customer loyalty schemes and is available to provide further information if requested.

[38] There are several examples of agencies having the power to exercise either an intervenor and amicus curiae role where appropriate (e.g. the Australian Securities and Investments Commission (ASIC) has a right to intervene in court proceedings that relate to matters including under the *Corporations Act 2001* (Cth) (Corporations Act) and the *National Consumer Credit Protection Act 2009* (National Credit Act), and can also appear as an amicus curiae in certain circumstances).