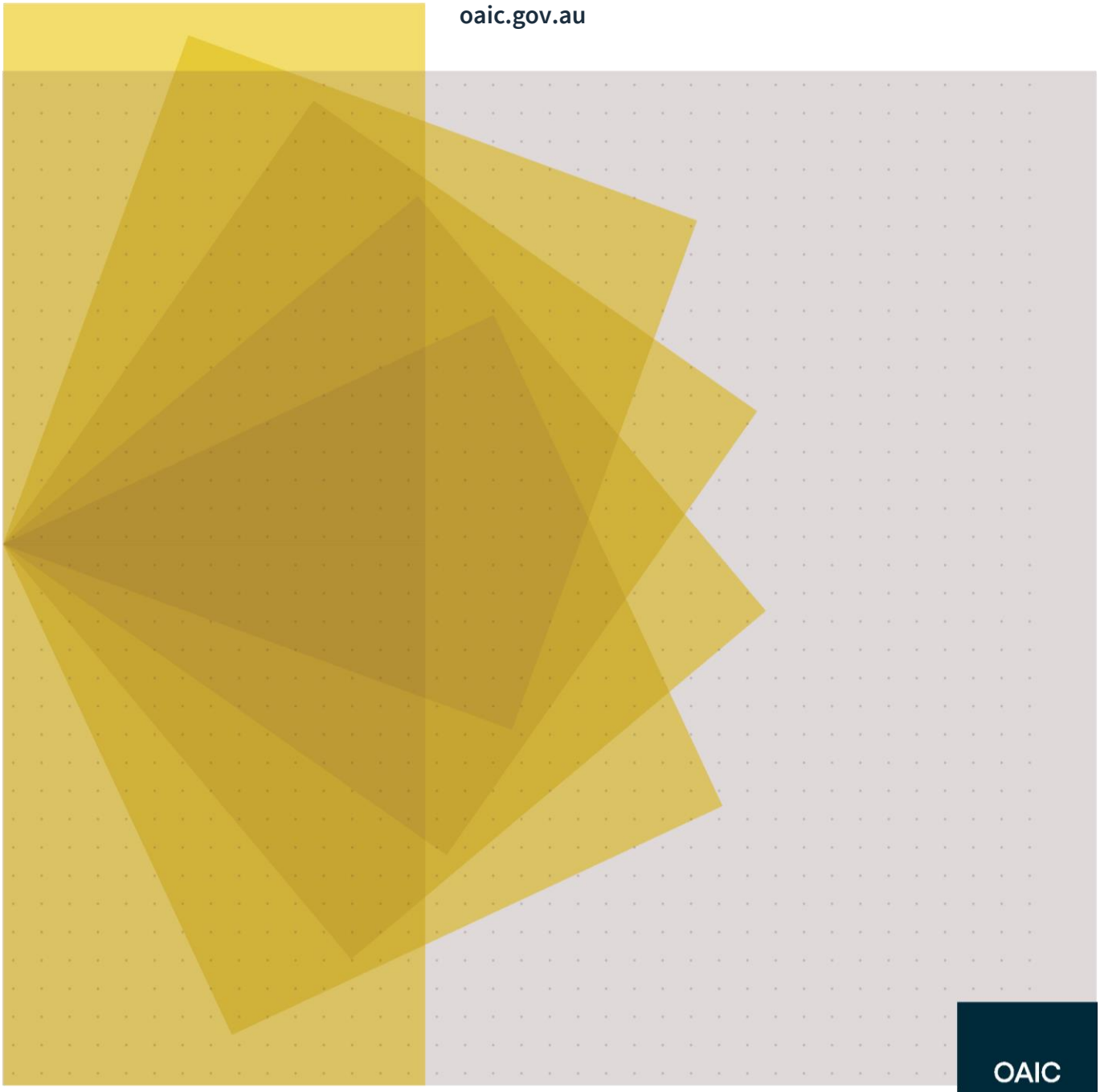
Australian Government

Office of the Australian Information Commissioner

Digital Platforms Inquiry

Submission of the Office of the Australian Information Commissioner on the preliminary report of the Australian Competition and Consumer Commission

oaic.gov.au



OAIC

Contents

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry Preliminary Report* (preliminary report).

The OAIC commends the ACCC for its preliminary report. The report raises a number of critical issues impacting privacy, such as information asymmetries and power imbalances between consumers and digital platforms that challenge consumers' capacity to make informed decisions about their personal information. The preliminary recommendations set out in Chapter 5 (preliminary recommendations) will support improvements to existing transparency obligations in the *Privacy Act 1988* (the Privacy Act) and build on entities' existing data stewardship obligations.

The OAIC has appreciated the opportunity to confer with the ACCC throughout this Digital Platforms Inquiry (inquiry) to address areas of mutual concern to secure better data protection outcomes for all Australians. This strong engagement between privacy and consumer protection regulators is replicated globally,[1] associated, in part, with the increasing commoditisation of personal information and a central concept of fairness underpinning both oversight regimes.

The OAIC generally supports the preliminary recommendations, subject to the comments below. The implementation of these recommendations will assist in addressing the information asymmetries and power imbalances identified by the ACCC. The OAIC acknowledges the importance of consultation regarding the implementation of the recommendations to ensure an appropriate balance of competing public interests.

In this submission, the OAIC:

- recommends amendments to preliminary recommendations 8(a) - (e) and 9 (Part 1)
- proposes two additional recommendations to further address issues identified in the preliminary report:
    - a recommendation to ensure that Australia's privacy protection framework is fit for purpose in the digital economy, including amending the definition of 'personal information' to align with the European Union General Data Protection Regulation (EU GDPR) definition of 'personal data', evaluating the current Privacy Act exemptions and consideration of whether additional EU GDPR rights should be introduced in Australia
    - a recommendation that the existing requirement for entities to collect information fairly, be extended to the fair use and disclosure of personal information through a new, explicit provision in the Privacy Act.

Part 1: ACCC Chapter 5 Preliminary Recommendations

1.1 Preliminary Recommendation 8: Use and collection of personal information

The OAIC supports preliminary recommendations 8(a) – (g), subject to the comments and proposed amendments set out below.

[1] See for example, the 2017 resolution adopted by the International Conference of Data Protection and Privacy Commissioners, *Resolution on collaboration between data protection authorities and consumer protection authorities for better protection of citizens and consumers in the digital economy* (<https://icdppc.org/document-archive/adopted-resolutions/>).

The OAIC agrees that the economy-wide application of these amendments will improve privacy practices by reducing information asymmetries and providing consumers with stronger, mandated privacy controls. These recommendations build on the existing privacy standards in the Australian Privacy Principles (APPs) in Schedule 1 of the Privacy Act and OAIC guidance on matters such as consent and notice.[2]

Preliminary recommendation 8(a): stronger notification requirements

The OAIC suggests that this preliminary recommendation be subject to appropriate public interest exceptions.

Australian Privacy Principle 5 requires entities to take 'reasonable steps' to notify an individual about a range of prescribed matters when collecting their personal information. This 'reasonable steps' test provides flexibility for businesses to design notifications having regard to their relationship with clients and business practices. It also balances the requirement to notify with other public interests. For example, this 'reasonable steps' test can be applied to situations where:

- consumers would otherwise receive a notice every time they were to access a service, potentially resulting in notification fatigue and disengagement
- notification may jeopardise the purpose of collection or the integrity of the personal information collected in circumstances and there is a clear public interest in the collection; for example law enforcement agencies undertaking covert surveillance[3]
- notification would be inconsistent with another legal obligation, for example, breaching a statutory secrecy provision, a client's legal professional privilege or a legal obligation of confidence.[4]

The EU GDPR reflects a similar balance between a requirement for transparency about information handling practices and other public interest objectives. It sets out a range of instances where notification to an individual is not required, such as where:

- the individual has already been provided with the information[5]
- entities are subject to an obligation of professional secrecy regulated by law that covers the personal data[6]
- entities are required by law to obtain or disclose the personal data.[7]

In recognition that it may not always be in the public interest to receive a notification about each collection of personal information, the OAIC suggests that this recommendation be 'subject to appropriate public interest exceptions.' These could be identified as part of the implementation process, and informed by consultation.

[2] See for example, OAIC's APP Guidelines <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>.

[3] APP Guidelines, paragraph 5.7.

[4] APP Guidelines, paragraph 5.7.

[5] EU GDPR article 13.

[6] EU GDPR article 14.

[7] EU GDPR article 14.

Preliminary recommendation 8(b): independent third-party certification

The OAIC suggests that this preliminary recommendation be amended to:

1. provide that an independent body approves the certification of parties carrying out audits and approving use of the mark or seal; and
2. identify the OAIC as the scheme's regulator for privacy breaches and the ACCC for breaches of competition and consumer law.

The OAIC supports the introduction of a third party certification scheme. Such a scheme could assist in ensuring that regulated entities are meeting their obligations under the Privacy Act without the need to substantially increase direct regulatory action. It also provides consumers with evidence-based information about the privacy credentials of entities with which they may engage.

The preliminary recommendation currently states that 'the parties carrying out such audits would first be certified by the OAIC.' The OAIC suggests it would be preferable for an independent third party to administer the scheme to ensure the functional independence of the OAIC. As an independent, statutory regulator, the OAIC is concerned to ensure both the fact and perception of independence are maintained by retaining separation between the certification of entities carrying out audits and the broader regulation of the scheme. The OAIC suggests further consideration could be given, as part of the implementation process, to whether there is a current government body that could undertake the certification function.

Preliminary recommendation 8(c): stronger consent requirements

The OAIC suggests that the word 'express' in this preliminary recommendation be amended to 'affirmative, unambiguous act'.

The OAIC proposes that the word 'express' in this preliminary recommendation be amended to 'affirmative, unambiguous act.' The OAIC recognises that there are some limited circumstances, outside the digital environment, where an individual's consent can be conveyed in an unambiguous manner, but may not amount to 'express' consent. This amendment will also bring Australia's interpretation of 'consent' closer in line with the EU GDPR.[8]

While the OAIC welcomes the elevation of its guidance on consent in relation to digital platforms, it also recognises that there are some broader limitations of privacy self-management tools, such as consent, in the context of digital platforms and in the online environment more broadly. As canvassed by the Office of the Victorian Information Commissioner in its submission on the preliminary report,[9] consumers may be informed and understand the inherent privacy risks of providing their personal information, but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative.[10] Further, while 'consent' is only a meaningful and effective privacy self-management tool where the

[8] Article 4(11) of the EU 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.

[9] Reference to OVIC sub Office of the Victorian Information Commissioner's submission to the ACCC Digital Platforms Inquiry preliminary report, page 2: < https://www.accc.gov.au/system/files/Office%20of%20the%20Victorian%20Information%20Commissioner%20%28February%202019%29.PDF >.

[10] UK ICO, *Big Data, AI, Machine Learning and Data Protection, 2017, page 24.*

individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment.[11]

The burden of understanding and consenting to complicated practices should not fall only on individuals, but must be supported by appropriate accountability obligations for entities, as well as other regulatory checks and balances. The limited role of consent is being considered by regulators around the world. For example, in Canada consent is considered the cornerstone of privacy law, and the Canadian regulator, the Office of the Privacy Commissioner of Canada, has noted the challenges of expecting individuals to always make meaningful decisions about consent in increasingly complex digital environments.[12]

The OAIC proposes that introducing a general fairness requirement for the use and disclosure of personal information will supplement this preliminary recommendation in addressing the overarching issue of power imbalances between entities and consumers. The practical application of concepts of fairness and the role of consent will be central to the future of privacy in Australia, including protecting the privacy of vulnerable Australians including children. The OAIC's proposed recommendation to introduce a fairness requirement on the use and disclosure of personal information is further explored at part 2.2 of this submission.

The ACCC has highlighted a further area of analysis, under which entities must expressly opt-in to receive targeted advertising.[13] The OAIC supports the ACCC's recommendation that this requirement extend beyond entities covered by the Privacy Act to ensure coverage of all entities which may collect data for this purpose.[14] This raises a broader issue of whether the current exemptions to the Privacy Act continue to reflect community expectations and are fit for purpose in the digital age, which is discussed further at part 2.1 of this submission.

Preliminary recommendation 8(d): erasure of personal information

The OAIC suggests that this preliminary recommendation be 'subject to appropriate public interest exceptions'. The OAIC also suggests that a further recommendation is made to allow an individual a right to object.

[11] Consumer Policy Research Centre report, *Consumer data and the digital economy – Emerging issues in data collection, use and sharing, 2018 page. 9.*

[12] In its 2016-2017 annual report to Parliament, the Canadian Privacy Commissioner noted that consent 'needs to be supported by other mechanisms, including independent regulators that inform citizens, guide industry, hold it accountable, and sanction inappropriate conduct.'< https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1>.

[13] The ACCC is considering whether, in addition to proposed preliminary recommendation 8(c), consumer consents in relation to targeted advertising should be further strengthened by prohibiting entities from collecting, using, or disclosing personal information of Australians for targeted advertising purposes unless consumers have provided express, opt-in consent. Under such a proposal, consumers receiving advertising-funded services (including via a social media platform or search engine) can still be required by the platform to consent to view advertisements but the user must not be required to consent to view targeted advertisements based on their user data or personal information in order to use the platform. Such a requirement would be proposed to apply beyond entities covered by the Privacy Act to ensure coverage of all entities which may collect data for this purpose.

[14] ACCC Preliminary report, page 17.

The OAIC supports this recommendation, including the need to limit this right in certain circumstances.[15] For example, under the EU GDPR, the right to erasure does not apply where processing is necessary for:

- the exercise of the right of freedom of expression and information[16]
- compliance with a legal obligation[17]
- for reasons of public interest in public health (such as protecting against cross-border health threats and for preventative or occupational medicinal purposes)[18]
- archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing[19]
- the establishment, exercise or defence of a legal claim.[20]

The OAIC recommends that consideration be given to appropriate exceptions as part of the implementation process.

The OAIC notes that under the EU GDPR, individuals also have a right to object to the processing of their personal information for specified purposes.[21] The OAIC suggests that such a right complements the ACCC preliminary recommendation on enabling the erasure of personal information, as it would apply in circumstances where an individual wishes to continue using a service, but objects to certain types of data processing.[22]

The ACCC has highlighted a further area of analysis, under which entities have an explicit obligation to delete all user data at a certain point in time. The OAIC notes that such a requirement would align with agency record destruction practices, and considers that the obligation should also take account of consumer expectations about continuing access to data. The OAIC therefore recommends that consultation be undertaken to ensure alignment and identify any exceptions that may also be required to balance competing public interest objectives such as compliance with legal obligations.

Preliminary recommendation 8(e): increase the penalties for breach

> The OAIC suggests this recommendation be amended to: Increase penalties for breaches of the Privacy Act to at least mirror the increased penalties for breaches of the Australian Consumer Law or penalties under the EU GDPR, whichever is highest.

The OAIC supports this preliminary recommendation to increase the penalties for breaches of the Privacy Act. There has been an international trend to increase the penalties for breaches of data

[15] ACCC Preliminary report, page 231.

[16] EU GDPR, article 17(3)(a).

[17] EU GDPR, article 17(3)(b).

[18] EU GDPR, article 17(3)(c).

[19] EU GDPR, article 17(3)(d).

[20] EU GDPR, article 17(3)(e).

[21] EU GDPR, article 21.

[22] Whereas the right to erasure prevents processing of any kind as the data can no longer be stored by the controller.

protection laws, and this recommendation is consistent with that trend.[23] For penalties to act as effective deterrence for large multinational corporations, it is important that maximum penalties cannot easily be absorbed as a minor cost of doing business in Australia.

Preliminary recommendation 8(f): a direct right of action for individuals

The OAIC supports this recommendation in principle (see discussion of preliminary recommendation 10 at 1.3 below).

Preliminary recommendation 8(g): expand resourcing to support further enforcement activities

The OAIC supports this recommendation and a recent commitment to increase the OAIC's resources.[24] These strengthen the OAIC's capacity to provide effective oversight of entities in the digital economy, which would have significant additional benefit for Australia.

To address the challenges outlined in the preliminary report across the economy, the OAIC should be resourced to undertake its broad range of complementary functions and activities. This will ensure an economy wide uplift in privacy practices while maximising the positive contributions online technologies make to Australian consumers. The changes to the Privacy Act indicated by the preliminary recommendations will be most effective in protecting personal information and addressing information asymmetries if the increases to resources apply across the OAIC's functions and activities.

1.2 Preliminary Recommendation 9: Code of practice for digital platforms

> The OAIC suggests that this recommendation be amended to specify that the Code may be developed by the OAIC through a new rule-making power.

The OAIC supports this recommendation and agrees that a code would allow greater proactive and targeted regulation of digital platforms' data collection practices through the existing provisions in the Privacy Act.

While the OAIC recognises that this may lead to different privacy protections across different sectors, the approach is consistent with the existing framework in the Privacy Act. That is, the APPs are intended to ensure regulated entities apply privacy protections to individuals' personal information. The code-making power in Part IIIB of the Privacy Act envisages that additional requirements can be imposed for practices that involve an increased or particular privacy risk. Part IIIB states that a code may be expressed to apply to a specified type of personal information, a specified activity, a specified industry sector or profession, as well as to entities that use a specified kind of technology.[25] For example, the Privacy (Credit Reporting) Code 2014 (Version 2) deals with issues and privacy risks identified as characteristic of the credit reporting sector.[26]

The ACCC has identified a number of heightened privacy risks in the digital platforms sector. Given the range of issues identified in the preliminary report, the OAIC agrees that the handling of personal information by digital platforms is an area where higher or more particular standards are

---

[23] For example, in the EU there can be administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): EU GDPR Art 83(6)). In Singapore there can be financial penalties of up to $1million: *Personal Data Protection Act 2012* (Singapore) s 29)).

[24] Portfolio Budget Statements 2019-20, Office of the Australian Information Commissioner, <https://www.ag.gov.au/Publications/Budgets/Budget2019-20/Pages/Portfolio-Budget-Statements-2019-20.aspx>.

[25] Privacy Act section 26C(4).

[26] <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-credit-reporting-code-2014-version-2>.

warranted. The OAIC suggests that this proposed recommendation also address the organisational accountability of digital platforms through mechanisms such as Privacy Impact Assessments and Privacy Management Plans, for ensuring transparency about how personal information is handled.

Part IIIB currently requires a code developer to develop a code for approval by the Australian Information Commissioner,[27] or for the Australian Information Commissioner to develop a code in limited circumstances.[28] Given the ACCC's clear policy objectives that the code will seek to address in the digital platforms context, it is desirable to introduce a new rule-making power for the Australian Information Commissioner. A rule-making power would allow the Australian Information Commissioner to issue binding rules addressing the governance and handling of personal information by digital platforms. This power will ensure that the OAIC has leadership over the code development process, and that a collaborative process, with input from other regulators such as the ACCC and other community groups, is undertaken. The OAIC anticipates that rules made under such a rule-making power would be a legislative instrument, and as such would be subject to Parliamentary scrutiny. [29]

1.3 Preliminary Recommendation 10: Serious invasions of privacy

The OAIC supports this recommendation.

As outlined in the preliminary report, this would generally align with previous findings and recommendations that Australia's privacy framework should include additional remedies for invasions of privacy.[30] Introducing a statutory tort for serious invasions of privacy would be an important addition to the suite of regulatory measures needed to address online harms, including the serious risks that can be posed to individuals' privacy by live streaming technologies.[31]

Part 2: Further proposed recommendations

The OAIC suggests two additional recommendations for incorporation in the final report.

2.1 Ensure Australia's privacy protection framework is fit for purpose in the digital age

The OAIC proposes an additional recommendation to ensure that Australia's privacy protection framework is fit for purpose in the digital age.

The OAIC proposes that over the next 12 months, a review considers whether:

- there is an appropriate balance between effective privacy self-management and organisational accountability. This includes evaluating the suitability of EU GDPR privacy rights and protections in the Australian context, such as rights relating to profiling and automated decision making,[32] compulsory privacy impact assessments for data

[27] Privacy Act section 26E.

[28] These circumstances include instances where the Commissioner's request for a code to be developed under section 26E(2) has not been complied with, or where a Commissioner has decided not to register a code that was developed by a code developer: Privacy Act section 26G.

[29] *Legislation Act 2003* (Cth) sections 36–48.

[30] Preliminary report, page 222.

[31] See for example, Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (No. 38, 2019) and https://www.attorneygeneral.gov.au/Media/Pages/Tough-New-Laws-to-protect-Australians-from-Live-Streaming-of-Violent-Crimes.aspx

[32] EU GDPR articles 13(2)(f), 14(2)(g), 15(1)(h), 22.

processing activities involving certain high risks[33] and express requirements to implement data protection by design and by default[34]

- the exemptions under the Privacy Act are warranted and align with current community expectations of privacy
- the definition of 'personal information' within the Privacy Act is fit for purpose, and
- the OAIC's resourcing and regulatory powers continue to ensure it is a fit for purpose regulator in the digital age.

1. Striking the balance between privacy self-management and organisational accountability

The ACCC's inquiry draws out a key challenge for regulating privacy in the digital era, that is, whether privacy laws appropriately balance privacy self-management and organisational accountability.

Notice and consent provide foundational protections in privacy law across the world, including in the APPs. Their purpose is to ensure that individuals have knowledge of, and choice and control over, how information about them is handled by organisations. Transparency obligations, through privacy policies (APP 1.3), collection notices (APP 5), and obligations to obtain consent when collecting sensitive information and handling personal information beyond the primary purpose of collection (APPs 3.3 and APP 6.1) are aimed at privacy self-management.[35] Other common requirements in privacy law, such as privacy governance obligations (APP 1.2), data minimisation (APP 3), data quality (APPs 10 and 13) and data security (APP 11) require organisational accountability.

While the OAIC supports the ACCC's preliminary recommendations 8(a) and (c) to strengthen notice and consent requirements in the Privacy Act, it recognises the limitations of privacy self-management in the context of digital platforms and more broadly. Striking the right balance between privacy self-management and organisational accountability has been a central consideration for the Australian and international data protection regulatory community. For example, Canada has reviewed their data protection legislation and introduced further guidance around 'no-go zones' which prohibit certain information handling practices by an organisation (with or without consent).[36] This followed extensive consultation on the challenges that the digital environment poses to the protection of privacy and the effectiveness of the current consent model in that environment.[37]

The recent introduction of the EU GDPR embedded key rights aimed at ensuring individuals have adequate mechanisms to control how their personal information is handled. The preliminary recommendations reference some of these rights, such as stronger consent requirements and the right to erasure (recommendations 8(c) and (d)). The OAIC suggests that further consideration should be given to the suitability of adopting other EU GDPR rights in the Australian context,

[33] EU GDPR article 35.

[34] EU GDPR article 25.

[35] This expression is used by Daniel J Solove in 'Privacy Self-Management and the Consent Dilemma', 126 *Harvard Law Review*, 2013, page 1880.

[36] For example, these include profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>.

[37] <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1 >

including rights relating to profiling and automated decision making,[38] compulsory data protection impact assessments for data processing involving certain high risks[39] and express requirements to implement data protection by design and by default.[40]

2. Review of exemptions

Recently, there has been heightened community discussion around many of the existing exemptions in the Privacy Act, including the journalism exemption,[41] political parties' exemption,[42] and the small business exemption.[43] The preliminary report and some submissions to this inquiry also considered whether these exemptions reflect current community expectations.[44] The OAIC acknowledges that privacy is not an absolute right, and that privacy interests in some cases may be outweighed by other public interests. However, given current practices and the increased ability of organisations to collect and store large volumes of personal information regardless of organisational size, the OAIC considers that it is appropriate to reconsider these exemptions.

3. Definition of 'personal information'

The OAIC suggests that consideration is given to the definition of 'personal information' in the Privacy Act, to amend it to align with the definition of 'personal data' in the EU GDPR. This is consistent with stakeholder feedback provided through engagements related to this inquiry.[45] The challenges posed by emerging technologies such as artificial intelligence and data analytics necessitates a clear, contemporary definition of personal information.

In comparison to the definition of 'personal information' in section 6(1) of the Privacy Act, the EU GDPR has a more detailed definition of personal information, and outlines a range of data that constitutes personal information.[46] In the EU GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[47]

The OAIC notes that there is precedent for extending the coverage of the Privacy Act to cover online identifiers (such as an Internet Protocol address allocated to an internet account, or a unique identification number attached to a mobile phone) under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Part 5-1A of the TIA Act requires service providers to

---

[38] EU GDPR articles 13(2)(f), 14(2)(g), 15(1)(h), 22.

[39] EU GDPR article 35.

[40] EU GDPR article 25.

[41] Journalists are exempt pursuant to section 7B(4) of the Privacy Act.

[42] Political acts and practices are exempt pursuant to section 7C of the Privacy Act.

[43] Small businesses are exempt pursuant to the definition of organisation as set out in section 6C of the Privacy Act.

[44] Preliminary report, p. 222.

See for example the submission of the UN Special Rapporteur on the Right to Privacy (<https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report-submissions>).

[45] As set out in the summary of the ACCC Digital Platforms Inquiry Privacy Roundtable <https://www.accc.gov.au/system/files/DPI%20privacy%20roundtable%20summary.pdf>.

[46] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person: EU GDPR article 4(1).

[47] EU GDPR article 4.

retain certain information (including identifiers used by the service provider in relation to the relevant service or related account, service or device) and comply with the Privacy Act in relation to the data they collect and retain under Part 5-1A of the TIA Act.

4. OAIC resourcing

As discussed above, the OAIC supports preliminary recommendation 8(g) to expand its resourcing to support enforcement activities.

The Commissioner's existing powers conferred under the Privacy Act include powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers for cases where a privacy breach has occurred. These relevantly include:

- developing guidance about the operation of the Privacy Act—such as the *Guide to securing personal information*[48]
- advising regulated entities about the operation of the Privacy Act[49]
- conducting assessments (audits) to identify privacy risks and recommend ways to reduce these risks[50]
- handling enquiries and investigating complaints from individuals about possible interferences with privacy[51]
- conducting Commissioner initiated investigations (CII) about potential interferences with privacy of an individual[52]
- making a public determination in a complaint investigation or a CII and, where necessary, bringing proceedings to enforce the determination[53]
- accepting enforceable undertakings and, where necessary, bringing proceedings to enforce these undertakings[54]
- seeking a civil penalty from the courts in the case of a serious or repeated interference with privacy, or in the case of a breach of certain credit reporting provisions.[55]

These functions extend beyond supporting enforcement activities, including to proactive regulatory work and educative activities. By way of example, the OAIC's power to conduct privacy assessments of APP entities provides a professional, independent and systematic appraisal of an entity's compliance with all or part of its privacy obligations. These assessments encourage APP entities to move from minimum mere compliance with the Privacy Act towards implementing best privacy practice. By expanding the OAIC's resources in this area, the OAIC could more effectively and comprehensively target particular sectors (in addition to digital platforms) or entity types (such as large publicly listed companies).

[48] Privacy Act section 28.

[49] Privacy Act section 28B(1).

[50] Privacy Act section 33C.

[51] Privacy Act section 36.

[52] Privacy Act section 40(2).

[53] Privacy Act sections 36, 40 and 52.

[54] Privacy Act section 33E.

[55] Privacy Act section 80W.

To address the challenges outlined in the preliminary report, a review should ensure that the OAIC is resourced to undertake its broad range of complementary functions and activities, and drive an economy wide uplift in privacy practices while maximising the positive contributions online technologies make to Australian consumers.

2.2 The 'fair' use and disclosure of personal information

The OAIC proposes a new recommendation codifying the fair collection, use and disclosure of personal information.

Many global privacy regulations require entities entrusted with individuals' personal information to handle that information fairly and ethically.

For example, the first data processing principle in the EU GDPR is that data controllers' 'process' personal data 'lawfully, fairly and in a transparent manner in relation to the data subject'.[56] 'Processing' is defined broadly, and includes 'collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[57] An infringement of this provision can be subject to administrative fines of up to €20 million or 4 per cent of annual worldwide turnover, (whichever is higher).[58] Guidance published by the UK Information Commissioner's Office states that 'fairness' requires personal data to be handled in a way that can be reasonably expected by an individual and not used in a way that results in unjustified adverse effects on that individual.[59] Similarly, the Canadian *Personal Information Protection and Electronic Documents Act* includes a foundational principle that states 'an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'.[60]

The OAIC considers that a further recommendation which requires entities to fairly collect, use and disclose personal information will assist in addressing some of the information asymmetries identified by the ACCC. It will strengthen the existing obligation in APP 3.5, which requires an APP entity to *collect personal information by lawful and fair means*. This will ensure that all handling of personal information by APP entities is underpinned by obligations to act fairly, enhancing the organisational accountability obligations under the Privacy Act.

[56] EU GDPR article 5(1)(a).

[57] EU GDPR article 4(2).

[58] EU GDPR article 83(5).

[59] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ >.

[60] Canada *Personal Information Protection and Electronic Documents Act* section 5(3).