Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: D2018/003188

Digital Platforms Inquiry
Australian Competition & Consumer Commission
GPO Box 3648
Sydney 2001

Via email: platforminquiry@accc.gov.au

Submission on Issues Paper—Digital Platforms Inquiry

The Office of the Australian information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Competition & Consumer Commission's (ACCC) Issues Paper on the Digital Platforms Inquiry (the Issues Paper).

The Issues Paper raises important matters about the data handling practices of digital platform service providers. Technological developments that have made providers' big data activities a part of everyday life, demand that careful consideration be given to the way individuals exercise choice and control over their personal information—particularly, how individuals can be given notice of, and exercise meaningful consent to, an entity's often complex information handling practices. These are timely considerations, which raise common areas of interest for the OAIC under the *Privacy Act 1988* (Cth).

The OAIC is a key advisory body on privacy and information management, drawing on our domestic and international networks to shape how organisations and Australian government agencies (APP entities)[1] harness emerging technologies and data practices to improve the lives of Australians. Central themes in the Privacy Act—such as transparency, choice and control for individuals and accountability for APP entities—are intended to support individuals in making decisions about their personal information, and to ensure APP entities protect personal information and are accountable for how it is handled.

The broad protections and requirements in the Privacy Act that apply throughout the information life cycle, complement consumer protections overseen by the ACCC in the Australian Consumer Law in Schedule 2 of the *Competition and Consumer Act 2010*, outlined in the Issues Paper.[2] As such, the Issues Paper presents an important opportunity for the OAIC and the ACCC to confer in addressing areas of mutual concern, to secure better data protection outcomes for all Australians. The benefits for consumers in taking such an

[1] APP entities include most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses: *Privacy Act 1988* (Cth), s 6(1).

[2] Issues Paper, pp 28–29.

approach were recently recognised in a 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*.[3]

The OAIC has appreciated the ACCC's early engagement with the OAIC regarding this Issues Paper, and looks forward to opportunities to work with the ACCC as this inquiry progresses.

About the Office of the Australian Information Commissioner

The Australian Parliament established the OAIC in 2010 to bring together three functions:

- freedom of information functions, including access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
- privacy functions (regulating the handling of personal information under the Privacy Act and other Acts)
- information management functions.

The integration of these three interrelated functions into one agency has made the OAIC well placed to assist APP entities to navigate the right to privacy in the context of other information policy objectives. It also provides the OAIC with a unique insight into some of the issues canvassed in the Issues Paper, particularly with regard to striking an appropriate balance between the need for protection of personal information and the free flow of information in the digital environment.

Guidance, advice and best practice

In the exercise of these functions, the OAIC is a key advisory body, both domestically and internationally. Recent OAIC guidance is set out in Attachment A.

In addition, the Australian Information Commissioner has a power to approve and register enforceable 'APP codes',[4] to support and elevate privacy practice where required. An APP code sets out how one or more of the Australian Privacy Principles (APPs) are to be complied with in practice. A Code may also introduce additional obligations to those imposed by the APPs (providing these are not inconsistent with the APPs), may cover an act or practice that would otherwise be exempt or may be expressed to apply to a particular industry or to entities that use technology of a specified kind.

For example, the Australian Government Agencies Privacy Code, which commences on 1 July 2018, sets out specific requirements and key practical steps that agencies must take as part of complying with APP 1.2. APP 1.2 requires entities to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding APP code, and is able to deal with related inquiries and complaints. It requires agencies to move towards a best practice approach to privacy governance to help build a

[3] <https://icdppc.org/document-archive/adopted-resolutions/>

[4] *Privacy Act 1988* (Cth), ss 26E, 26G, 26P and 26R.

consistent, high standard of personal information management across all Australian Government agencies.[5]

Privacy by design and privacy impact assessments

The OAIC's advice and guidance to regulated entities reflect the importance of adopting a 'privacy by design' approach to support innovation. 'Privacy by design' is about finding ways to build privacy into projects from the design stage onwards and is a fundamental component of effective data protection. This involves taking a risk management approach to identifying privacy risks and mitigating those risks. In applying this approach, entities take steps at the outset of a project that minimise risks to an individual's privacy, while also optimising the use of data.

Adopting a privacy by design approach can be extremely valuable when conducting data analytics activities involving personal information for the success of the project itself. This is because if a privacy risk with a data analytics project is identified, it can be an opportunity to find creative technical solutions that can deliver the real benefits of the project while also protecting privacy and enhancing trust and confidence in the project. An iterative privacy by design approach can be of significant benefit in the changing use of personal information, such as the regular evolution of digital platforms to provide new user experiences.

Privacy impact assessments (PIA) are an important tool that can support the 'privacy by design' approach. A PIA is a systematic assessment of a project that identifies the impact that it might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. The OAIC has developed the *Guide to undertaking privacy impact assessments*[6] and an elearning course on conducting a PIA,[7] which aim to assist APP entities undertaking a PIA.

International partnerships

Increasingly, businesses are carried on globally, personal information moves across borders, and privacy threats and challenges extend internationally. A coordinated and consistent global approach can be an effective response to global privacy concerns, including privacy issues relating to the international cyberspace environment. In light of this, there is a trend towards increased cooperation and information sharing between data protection authorities.

The OAIC is actively engaged in a range of international privacy and data protection forums (see Attachment A for further detail).

The OAIC is also actively engaged with the Attorney-General's Department to facilitate Australia's participation in the APEC Cross Border Privacy Rules system, which was developed by the participating APEC economies with the aim of building consumer, business and regulator trust in cross border flows of personal information. APEC member economies and

---

[5] <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017>

[6] <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>

[7] <https://www.oaic.gov.au/elearning/pia/welcome.html>

EU officials have been collaborating to promote interoperability between the APEC and EU regional transfer mechanisms.

The OAIC has also been actively engaging with Australian businesses and government agencies and our APPA and European counterparts, regarding changes to the European data protection laws. The European General Data Protection Regulation (GDPR), which will commence on 25 May 2018, provides significant focus on privacy governance at an international level, with the requirements extending to businesses outside of Europe, where they have an establishment in the EU, offer goods and services in the EU, or monitor in the EU the behaviour of individuals in the EU. It introduces a number of new and expanded requirements, many of which are already reflected in Australian privacy law. The OAIC has published guidance, drawing on our international networks, to assist Australian businesses to understand the new requirements in the GDPR and how they can comply with Australian and EU privacy laws.[8]

The protection of personal information under the Privacy Act 1988 (Cth)

The international context for the Privacy Act

Privacy is a fundamental human right recognised in Article 12 of the UN *Declaration of Human Rights*, and in many other international and regional treaties. In Australia, the right to privacy is protected by a number of different regulatory schemes. The Commonwealth scheme applies to the handling of information by both the Commonwealth government and the private sector, while various State and Territory schemes generally apply to the handling of information by agencies of those governments.[9]

In the Commonwealth jurisdiction, the key piece of legislation regulating the right to privacy is the Privacy Act. The Privacy Act is intended to give effect to Australia's obligations under international agreements[10], including:

- Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)[11]
- the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines)[12]

The Privacy Act is consistent with these key international privacy agreements, and helps to ensure that Australia is able to meet the international community's expectations of privacy

---

[8] <https://www.oaic.gov.au/media-and-speeches/news/general-data-protection-regulation-guidance-for-australian-businesses>

[9] See the OAIC's information on other privacy jurisdictions for information on privacy regulation in the states and territories https://oaic.gov.au/privacy-law/other-privacy-jurisdictions

[10] P*rivacy Act 1988* (Cth), s 2A(h).

[11] Opened for signature 16 December 1966 (entered into force 23 March 1976), [1980] ATS 23. The full text of the ICCPR is available on the United Nations High Commissioner for Human Rights website, at: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

[12] See the OECD's *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (23 September 1980) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation>.

protection so that Australian businesses are able to participate in international markets, therefore supporting the Australian economy.

The Australian Privacy Principles

The Privacy Act provides a robust and flexible framework for facilitating community confidence in personal information handling practices.[13] The objects of the Privacy Act include facilitating the free flow of information, while ensuring that the privacy of individuals is respected, and promoting responsible and transparent handling of personal information. Importantly, the objects of the Act also include recognising that the protection of individuals' privacy is balanced with the interests of entities in carrying out their functions or activities. As privacy is not an absolute right, the Privacy Act provides a framework within which to balance the protection of individuals' privacy with other legitimate rights and public interests.[14]

The 13 Australian Privacy Principles (APPs) in the Privacy Act are the cornerstone of the privacy protection framework in the Privacy Act.[15] They are principles-based law, providing APP entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and the diverse needs of individuals. The APPs are also technology neutral, preserving their relevance and applicability to changing and emerging technologies including big data practices.

The APPs set out standards, rights and obligations in relation to governance and accountability,[16] and around the collection,[17] use and disclosure,[18] integrity,[19] and correction[20] of personal information, as well as individual's rights to access personal information held about them by regulated entities.[21] The principles are structured to reflect the information lifecycle and each of the principles interact with and complement each other.

APP 3 specifies that the personal information collected by businesses must be reasonably necessary for its functions and activities. When collecting sensitive information (such as health, racial origin, political opinions), generally there is an additional requirement for consent. Collection must also be by lawful and fair means.

APP 6 requires an APP entity to only use or disclose personal information for a purpose for which it was collected ('primary purpose') or with consent. Exceptions apply, for example, where the individual would reasonably expect the APP entity to use or disclose their personal

---

[13] 'Personal information' is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable: *Privacy Act 1988* (Cth), s 6(1).

[14] *Privacy Act 1988* (Cth), s 2A.

[15] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p 52.

[16] APP 1 outlines the requirement for an APP entity to manage personal information in an open and transparent way.

[17] See APPs 3, 4 and 5 which all deal with the collection of personal information.

[18] See APPs 6, 7, 8 and 9 which all deal with the use or disclosure of personal information.

[19] APP 11 requires an APP entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

[20] APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

[21] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

information for the secondary purpose, and that purpose is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose.[22]

Where personal information is handled in reliance on an individuals' consent the OAIC recognises that a challenge is to ensure that any consent obtained is meaningful, and gives the individual the choice and control the provisions are intended to provide.

The Privacy Act is also about ensuring transparency and accountability. Transparency enables individuals to make informed choices about sharing their personal information and to exercise control. Transparency also ensures APP entities are accountable for personal information protection where personal information is mishandled. For example:

- APP 1.2, as noted above, requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.[23] Entities must also have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information.[24]
- APP 5 requires APP entities to take reasonable steps notify, or ensure an individual is aware of certain matters when personal information is collected about them, including the purposes of collection and the entity's usual disclosures of that kind of personal information.
- The Notifiable Data Breaches scheme in Part IIIC of the Privacy Act, which commenced on 22 February 2018, formalises a long-held community expectation around transparency. The requirements formalise data breach notification and assessment obligations for APP entities with personal information security requirements under the Privacy Act.

A breach of an APP is an 'interference with the privacy of an individual'.[25] The OAIC's regulatory powers include undertaking assessments of regulated entities,[26] investigating individuals' complaints and commencing Commissioner initiated investigations, making a determination about breaches of privacy,[27] and applying to the Federal Court for a civil penalty order for serious or repeated interferences with privacy.[28] The OAIC's approach to using its privacy regulatory powers is outlined in the OAIC's *Privacy regulatory action policy*.[29]

---

[22] APP 6.2(a).

[23] APP 1.2.

[24] APPs 1.3 and 1.4.

[25] *Privacy Act 1988* (Cth), s 13.

[26] *Privacy Act 1988* (Cth), s 33C.

[27] *Privacy Act 1988* (Cth), ss 36, 40 and 52.

[28] *Privacy Act 1988* (Cth), s 80W.

[29] <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>

Implications for media content creators, advertisers and consumers—implications for consumers questions

The Issues Paper raises a number of questions about the impacts of using digital platforms on consumers (questions 3.18–3.25).

The importance of transparency, notice and consent is borne out in the OAIC's research into privacy trends and individuals' privacy concerns, notably the periodical Community Attitudes to Privacy Survey (ACAPS).[30] The 2017 ACAPS[31] produced statistics that may be relevant to some of the questions posed in the Issues Paper, such as:

- 69% of Australians are more concerned about their online privacy than five years ago
- 83% of people believed there are greater privacy risks dealing with an organisation online compared to traditional settings
- 93% of people were concerned about organisations sending their personal information overseas
- only 21% of people feel comfortable with targeted advertising based on their online activities
- only 17% of people feel comfortable with social networking companies keeping databases of information on their online activities.

It is also clear from the 2017 ACAPS results that many Australians do not feel empowered to exercise their privacy rights, particularly in online contexts

- 47% of Australians do not know which organisation to report misuses of information to
- 58% of people were not aware of their ability to request access to their personal information
- only 29% of people normally read online privacy policies.

These concerns are magnified where individuals are unfamiliar with new technologies or unclear on how new applications will affect the way their personal information is handled.

As noted above, the Privacy Act promotes transparency, accountability and choice. The challenge is to ensure that such transparency is meaningful in an environment of complex information handling practices. I would welcome the opportunity to work with the ACCC in addressing the privacy aspects of issues raised by the Issues Paper and would be pleased to offer further assistance to the ACCC as this inquiry progresses.

[30] <https://www.oaic.gov.au/engage-with-us/community-attitudes/>

[31] <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>

If you would like to discuss these comments or have any questions, please contact

Yours sincerely

Angelene Falk
Acting Australian Information Commissioner
Acting Privacy Commissioner

17 April 2018

Attachment A

Recent OAIC guidance

- a *De-identification Decision-Making Framework* (in collaboration with Data61)[32]
- a guide to De-identification and the Privacy Act[33]
- a privacy resource for start-up businesses[34]
- a *Guide to Data Analytics and the Australian Privacy Principles*.[35]

OAIC engagement in international privacy and data protection forums:

- the Asia Pacific Privacy Authorities (APPA) Forum, which brings together privacy and data protection authorities in our region
- the Global Privacy Enforcement Network (GPEN), which facilitates cooperation between privacy and data protection authorities globally on cross-border privacy matters
- the International Conference of Data Protection and Privacy Commissioners, which seeks to provide leadership at an international level in data protection and privacy by connecting the efforts of privacy and data protection authorities from across the globe
- the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement,[36] which creates a framework for regional cooperation in the enforcement of privacy laws and information sharing among privacy enforcement authorities in APEC economies. For example, under this framework, the OAIC commenced a joint investigation with the Office of the Privacy Commissioner of Canada to establish whether the parent company of online dating website, Ashley Madison, had interfered with the privacy of its users. In August 2016, the two offices released joint findings that included court-enforceable commitments by the parent company, Avid Life Media Inc.[37]

---

[32] <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework>

[33] <https://oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act>

[34] <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-18>

[35] <https://oaic.gov.au/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles>

[36] <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>

[37] <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison>