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: D2018/004204

Secretariat
Office of the United Nations High Commissioner for Human Rights
Geneva, CH 1211

via email: privacyreport@ohchr.org

Dear Secretariat

OHCHR report on the right to privacy in the digital age

Thank you for the opportunity to provide comments to the Office of the United Nations High Commissioner for Human Rights (OHCHR) for its forthcoming report, 'the right to privacy in the digital age'.

The Office of the Australian Information Commissioner (OAIC) recognises that global and technological developments are creating unprecedented opportunities and challenges for privacy regulation, in particular for how regulation can support individuals to exercise meaningful choice and control in how their personal information is handled by governments and businesses.

The Australian *Privacy Act 1988* (Privacy Act) provides a principle-based and robust framework for protecting individuals' information privacy in Australia. Our comments provide an overview of how the protections and oversight mechanisms in the Privacy Act operate, and interact with other privacy laws where the OAIC has oversight functions. When exercising these functions, the OAIC draws on our domestic and international networks to shape how entities harness emerging technologies and data practices to improve the lives of Australians.

About the Office of the Australian Information Commissioner

The OAIC is an independent statutory agency within the Commonwealth Attorney-General's portfolio. 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 1988* (Privacy Act) and other Acts)
- information management functions.

The integration of these three interrelated functions into one agency provides the OAIC with a unique insight into the challenges of the digital age, particularly with regard to striking an appropriate balance between individuals' right to privacy and the flow of information in the digital environment.

Privacy regulation in Australia

In Australia, information privacy is protected by a number of regulatory schemes at the national and state levels. Australia's national privacy law is the *Privacy Act 1988* (Privacy Act), which applies to the handling of information by both Australian (Commonwealth) Government agencies and the private sector, while various State and Territory schemes generally apply to the handling of information by agencies of those governments.[1]

The Privacy Act is intended to give effect to Australia's obligations under international agreements,[2] including:

- Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR),[3] and
- the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines).[4]

The Privacy Act is consistent with these key international privacy agreements. It aims to ensure that Australia is able to meet the international community's expectations of privacy protection so that Australian organisations are able to participate in international markets and Australians have comparable privacy protections.

The 13 Australian Privacy Principles (APPs) in the Privacy Act are the cornerstone of the privacy protection framework in the Privacy Act.[5] They are principles-based, providing regulated entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and the varied needs of individuals. The APPs are also technology neutral, preserving their relevance and applicability to changing and emerging technologies. The APPs set out obligations in relation to governance and accountability,[6] and

---

[1] See the 0AIC's information on other privacy jurisdictions in the Australian states and territories <https://oaic.gov.au/privacy-law/other-privacy-jurisdictions>

[2] As reflected in the objects of the Privacy Act, at s 2A(h).

[3] 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>.

[4] 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>.

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

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

around the collection,[7] use and disclosure,[8] integrity,[9] and correction[10] of personal information, as well as individuals' ability to access personal information held about them by regulated entities.[11]

The Notifiable Data Breaches scheme in Part IIIC of the Privacy Act, which commenced on 22 February 2018, formalises long-held community expectations around data transparency. The scheme requires regulated entities with information security obligations under the Privacy Act to notify affected individuals, and the OAIC, in the event of a data breach that is likely to cause serious harm[12].

A breach of an APP, or a failure to report a notifiable data breach, is an 'interference with the privacy of an individual'.[13] The OAIC's regulatory powers include undertaking assessments of regulated entities,[14] investigating individuals' complaints and commencing Commissioner initiated investigations, making a determination about breaches of privacy,[15] and applying to the Federal Court for a civil penalty order for serious or repeated interferences with privacy.[16] The OAIC's approach to using its privacy regulatory powers is outlined in the OAIC's *Privacy regulatory action policy*.[17]

Balancing privacy with other interests

The right to privacy is not absolute, and privacy rights will necessarily give way where there is a compelling public interest reason to do so. The Australian privacy framework recognises that entities may have legitimate reasons to undertake projects that may limit or interfere with privacy, provided that any impacts are reasonable, necessary and proportionate for the achievement of the particular policy objective. The OAIC plays a leading role, across both the private and public sectors, to support entities in striking the right balance between the right to privacy and legitimate functions or activities, including through:

- promoting an understanding and acceptance of the APPs and the objects of those principles[18]

---

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

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

[9] 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.

[10] 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.

[11] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request. For more information about the APPs see < https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>, or for detailed guidance see https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

[12] For more information about the Notifiable Data Breach scheme see < https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

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

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

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

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

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

[18] Section 28(1)(c) of the Privacy Act

- examining draft laws,[19] and proposals for data matching or linkage, [20] that may involve an interference with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals
- ensuring that any adverse effects of draft laws or proposal for data matching on the privacy of individuals are minimised[21]
- undertaking research into, and monitoring developments in, data processing and technology to ensure that any adverse effects on the privacy of individuals are minimised[22]
- providing reports and recommendations to government in relation to any matter concerning the need for, or desirability of, legislative or administrative action in the interests of the privacy of individuals[23]
- directing an agency to give the Commissioner a privacy impact assessment[24]
- an oversight role in aspects of mandatory data retention and other requirements under the *Telecommunications Act 1997*[25] and the *Telecommunications (Interception and Access) Act 1979* (TIA Act),[26] and
- engaging with government on the development of its biometric face matching capability, focussing on the need for a robust governance framework and independent oversight.

In performing these functions, the OAIC's key message is often the importance of adopting a privacy by design approach from the outset of a proposal, including conducting privacy impact assessment where appropriate.[27]

To support entities in leveraging the value of data while protecting privacy, the OAIC has developed a range of practical tools and guidance. Recently for instance, the OAIC and Data61[28] have jointly produced a *De-identification Decision-Making Framework,*[29] and the OAIC has released a guide to *De-identification and the Privacy Act*. [30]

---

[19] Section 28A(2)(a) of the Privacy Act.

[20] Section 28A(2)(b) of the Privacy Act.

[21] Section 28A(2)(c) of the Privacy Act.

[22] Section 28A(2)(d) of the Privacy Act.

[23] Section 28B(1)(c) of the Privacy Act.

[24] Section 33C of the Privacy Act.

[25] regulates the activities of a number of participants in the telecommunications industry, including the use and disclosure of information obtained by certain bodies during the supply of telecommunication services.

[26] Under the TIA Act the Australian Security and Intelligence Organisation (ASIO) and certain domestic law enforcement agencies can authorise the disclosure of telecommunications data by a carrier or carriage service provider, including telecommunications data collected and retained under the data retention scheme. Under s 183(3) of the TIA Act, the Information Commissioner must be consulted about requirements relating to the form of those authorisations.

[27] The OAIC has developed the *Guide to undertaking privacy impact assessments* <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments> and an eLearning course on conducting a PIA < https://www.oaic.gov.au/elearning/pia/>, which can be used by any entity undertaking a PIA.

[28] Part of Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO).

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

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

Leveraging 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 is important for responding to global privacy concerns. The OAIC is actively engaged in a range of international privacy and data protection forums and enforcement arrangements.[31]

The OAIC looks forward to reviewing the OHCHR's report and stakeholder comments, to inform our regulatory approach to the challenges of safeguarding privacy in the digital age.

If you would like to discuss these comments or have any questions, please contact me or Sophie Higgins, Director, Regulation & Strategy, on (02) 9284 9775 or sophie.higgins@oaic.gov.au.

Yours sincerely

Angelene Falk
Acting Australian Information Commissioner
Acting Privacy Commissioner

30 April 2018

[31] <https://www.oaic.gov.au/engage-with-us/networks>.