Australian Government
Office of the Australian Information Commissioner

[redacted]

Mr Edward Santow
Human Rights Commissioner
Australian Human Rights Commission
175 Pitt Street
SYDNEY NSW 2000

Submission on Human Rights and Technology Issues Paper

Dear Mr Santow,

I welcome the opportunity to provide input to the important matters raised by the Australian Human Rights Commission's (AHRC's) *Human Rights and Technology Issues Paper* (the Issues Paper). The project is a timely opportunity to explore the protection of human rights including the right to privacy, in an era of unprecedented technological change.

The *Privacy Act 1988* (Privacy Act) provides a legally binding, principles-based and technology-neutral framework for protecting individuals' information privacy in Australia. The principles-based approach, supported by a range of regulatory oversight powers, is designed to be adaptable to changing technologies, community expectations and business needs. Central themes in the Privacy Act — transparency, choice and control — are intended to support individuals in making decisions about their personal information, and to ensure entities are accountable for how it is handled.

As the national privacy regulator, the Office of the Australian Information Commissioner (OAIC) recognises that global and technological developments are creating unparalleled opportunities and challenges for regulating the right to privacy – including how individuals can be given notice of, and exercise meaningful consent to, an entity's often complex information handling practices. This is coupled with a heightened community awareness of privacy risks, with recent examples including community concerns regarding the prolific sharing of data by social media platforms, broad community debate about the My Health Records scheme, and increasing media coverage of data breaches.

The central focus of the Issues Paper, how to protect and promote human rights in an era of unprecedented technological change, presents an important opportunity for the OAIC and the AHRC to continue to engage in addressing areas of mutual concern.

These comments focus on the consultation questions set out below. We offer the learnings from privacy frameworks and regulatory experience that may also be applicable to protecting other human rights in the context of new technologies:

- How should Australian law, as well as Government, the private sector and others, protect and promote human rights in the development, use and application of technologies? (Questions 3 and 4)

- How should Australian law, and Australia, protect human rights in AI-informed decision making? (Questions 6 and 7).

About the OAIC

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*

- privacy functions through regulating the handling of personal information under the Privacy Act and other Acts, and

- information management functions.

The integration of these three interrelated functions into one agency positions the OAIC to assist Australian government agencies and businesses to navigate the right to privacy in the context of other core information policy objectives and their application in the global digital environment.

An overview of privacy regulation in Australia

As noted in the Issues Paper, privacy is a fundamental human right recognised in Article 12 of the *UN Declaration of Human Rights*,[1] in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), [2] and in many other international and regional agreements.

The Privacy Act is intended to give effect to Australia's obligations under international agreements,[3] including:

- Article 17 of the International Covenant on Civil and Political Rights (ICCPR)

- 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 and helps to ensure that Australia is able to meet the international community's expectations of privacy protection.

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.[5] They also recognise 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, provided that restrictions on privacy are necessary, reasonable and proportionate to achieving those interests.[6]

Consultation questions

How should Australian law, as well as Government, the private sector and others, protect and promote human rights in the development, use and application of technologies?

The Privacy Act provides a legally binding and flexible framework for facilitating community confidence in personal information handling practices.[7]

The thirteen Australian Privacy Principles (APPs) in Schedule 1 of the Privacy Act are technology neutral, and have the advantage of preserving their relevance and applicability to changing and emerging technologies, including artificial intelligence (AI) and data analytics activities. The APPs are structured to reflect the information lifecycle, that is, personal information is protected in the way it is collected, stored, used and disclosed. To this end, the APPs require that entities establish accountable privacy governance arrangements,[8] alongside requirements for the collection,[9] use and disclosure,[10] security,[11] access[12] and correction of personal information.[13]

This principles-based law can also be supplemented by legislative instruments that provide greater particularity. The Australian Information Commissioner has a power to approve and register enforceable 'APP codes'[14], to support and elevate privacy practice where required. An APP code sets out how one or more of the 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,[15] which commenced 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 applicable binding APP code), and to deal with related inquiries and complaints. The Code requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies. This in turn will provide a basis for information sharing that manages privacy risk appropriately and builds community confidence.

In addition, 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 mandate data breach notification and assessment obligations for APP entities with personal information security requirements under the Privacy Act.[16]

The OAIC agrees with comments in the Issues Paper that where personal information is misused, the consequences can be grave.[17] This is reflected in the way in which the protections in the Privacy Act are supported by a broad range of regulatory powers. These include undertaking assessments of regulated entities,[18] investigating individuals' complaints and commencing Commissioner initiated investigations, making a determination about breaches of privacy,[19] and applying to the Federal Court for a civil penalty order for serious or repeated interferences with privacy.[20] The OAIC's approach to using its privacy regulatory powers is outlined in the OAIC's *Privacy regulatory action policy*.[21]

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 a *Guide to undertaking privacy impact assessments*[22] and an eLearning course on conducting a PIA[23], which aim to assist APP entities undertaking a PIA.

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 will be key to ensuring an effective response to privacy concerns. 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 fora, including:

- 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, which creates a framework for regional cooperation in the enforcement of privacy laws and information sharing among privacy enforcement authorities in APEC economies[24]

- OAIC is working with the Attorney-General's Department to implement the APEC Cross Border Privacy Rules system in a way that will ensure long term benefits for Australian businesses and consumers.[25]

These arrangements enable the OAIC to confer with international regulatory authorities about matters of mutual interest, and provide another mechanism to respond to privacy breaches. For example, the OAIC has conferred internationally in relation to Facebook's data sharing practices.[26] In addition, under the APEC Cross-border Privacy Enforcement Arrangement, the OAIC completed a joint investigation with the Office of the Privacy Commissioner of Canada into the data handling practices of online dating website, Ashley Madison. This investigation concluded with an enforceable undertaking by the website's parent company to address the Commissioner's recommendations relating to the security, retention and accuracy of personal information holdings.[27]

The OAIC has also been actively engaging with Australian businesses and government agencies and our APPA and European counterparts, regarding recent changes to the European data protection laws. As noted in the Issues Paper, the European General Data Protection Regulation (GDPR) commenced on 25 May 2018. The GDPR 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 the behaviour of individuals in the EU. It introduces a number of new and expanded requirements, many of which are reflected in Australian privacy law and the most recent Australian Government Agencies Privacy Code. As referenced in the Issues Paper, 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.[28]

As the GDPR only recently commenced, the OAIC is monitoring its implementation progress with interest, with a view to assessing whether any aspects of the GDPR could be replicated in the Australian context to secure better data protection outcomes for all Australians.

Community engagement

The importance of effective privacy protection to the Australian community is borne out in the OAIC's research into privacy trends and individuals' privacy concerns, notably the periodical Australian Community Attitudes to Privacy Survey (ACAPS).[29] The 2017 ACAPS produced statistics relevant to questions posed in the Issues Paper, including:

- 69% of Australians are more concerned about their online privacy than five years ago
- 58% have decided not to deal with an organisation because of privacy concerns
- 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.[30]

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.

For example, privacy policies and notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. An OAIC assessment of Australian government and businesses' privacy policies found the median length to be 3,413 words, making it difficult to locate important information and limiting the choice and control practically available to individuals.[31]

New technologies present the opportunity for more dynamic, multi-layered and user centric privacy policies and notices. The OAIC supports government and businesses to develop innovative approaches to privacy notices, for example 'just-in-time' notices, video notices, privacy dashboards and multi-layered privacy policies to assist with readability and navigability.

The OAIC also undertakes substantial work with the community to help Australians understand their privacy rights and safely participate online. For example, we:

- host the Consumer Privacy Network (CPN), with representatives from 14 consumer organisations, which regularly meets to discuss consumer-specific privacy issues[32]
- hold an annual Privacy Awareness Week (PAW), which included 360 private and public sector partners this year[33]
- maintain strong working relationships with the State and Territory data protection authorities, peak industry groups and other regulators
- continue to develop educational resources and materials for individuals, such as our suite of data breach guidance for consumers,[34] FAQs for individuals[35] and *Ten privacy tips to assist parents and carers*.[36]

How should Australian law, and Australia, protect human rights in AI-informed decision making?

The OAIC acknowledges that the use of AI is becoming increasingly common across government agencies and the private sector.[37] This is supported by a fundamental shift in analytical processes, together with the availability of large data sets, increased computational power and storage capacity. As recognised in the Issues Paper,[38] AI has the potential to yield great benefits, including in predictive capabilities, and it can also have significant impacts on privacy. These may include:

- collating data from a wide variety of different sources, including from third parties
- generating new information through 'collection via creation'
- inferential decision-making based on data which may not be accurate
- embedding bias in AI-informed decision-making
- using data insights for a range of different purposes, including new purposes that may not have been anticipated
- limited transparency around algorithmic decision-making
- retaining data for a longer period of time than usual, in case it may be useful in future for an unspecified purpose.

The APPs provide a foundation to address many of these challenges, particularly requirements for transparency, data quality, and access rights. For example APP 10, which requires entities to take reasonable steps to ensure the quality of personal information, is an important safeguard in ensuring AI decision-making based on accurate, up to date and relevant information.

The OAIC has developed a *Guide to Data Analytics and the Australian Privacy Principles* (Data Analytics Guide), [39] which highlights strategies to manage potential privacy risks for analytics processes. Strategies include that organisations:

- use de-identified data where possible (discussed further below)
- embed good privacy governance into the organisation by taking a privacy-by-design approach
- conduct Privacy Impact Assessments
- limit the collection of personal information where appropriate, and ensure that only personal information that is reasonably necessary to pursue a legitimate function and activity, is collected

- maintain awareness that data analytics may lead to the creation of and, consequently, the collection of, additional personal information, particularly when sensitive information may be generated, based on inferred or derived data

- make notices as dynamic, clear and user-friendly as possible. This includes considering how to allow individuals to choose which uses and disclosures they agree to and which they do not.

- protect information in line with risk assessments.

The OAIC's Data Analytics Guide also provides some examples of how ethical considerations can be incorporated into analytics activities.

In addition, the OAIC and CSIRO Data 61 have released the *De-Identification Decision-Making Framework*[40] to assist organisations to de-identify their data effectively. De-identified information is information which has undergone a process of de-identification, and no longer falls within the definition of 'personal information' under the Privacy Act. This is a practical guide for Australian organisations that handle personal information and are considering sharing or releasing it, to meet their ethical responsibilities and legal obligations, such as those under the Privacy Act.

The OAIC's guidance notes it is not always possible to draw a bright line between personal and de-identified information. We also recognise the legitimate concerns referred to in the Issues Paper associated with connecting disparate data sets and the re-identification of previously anonymised data.[41] The OAIC's guide, *De-identification and the Privacy Act,* frames de-identification as a risk management exercise, not an exact science.[42] In all cases, for data to be considered 'de-identified', it makes clear that the risk of re-identification in the data access environment must be very low (no reasonable likelihood of re-identification).

Addressing challenges and opportunities into the future

The OAIC agrees that there is work to do to take advantage of the opportunities and meet the challenges for privacy and other human rights, in a globalised and rapidly evolving data environment. In doing so, it is desirable to pursue a coordinated approach domestically and internationally.

The issue of artificial intelligence, algorithmic bias, and ethics are currently central considerations for the domestic and international data protection regulatory community. For example, the Issues Paper[43] refers to the new rights in the EU GDPR for individuals to not be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning them or similarly significantly affects them.[44] The GDPR also provides a right for individuals to be provided with information about the existence of automated decision-making including profiling, and meaningful information about the logic involved .[45] In addition, a range of relevant papers have been developed by domestic and international regulators and think tanks, including the Office of the Victorian Information Commissioner,[46] the French data protection authority,[47] and the Centre for Information Policy and Leadership that considers these issues.[48] AI is also a key subject for

discussion at the International Conference of Data Protection and Privacy Commissioners to be held in October 2018.[49]

The OAIC is also considering the role of certifications, seals and marks as an accountability mechanism. As noted in the Issues Paper with reference to a 'Turing stamp', trust marks can indicate to consumers that an organisation is 'worthy of trust', in circumstances where an entity's complex information handling practices may otherwise be difficult to understand.[50] It can also elevate good privacy practice as a market differentiator. The OAIC is actively engaging with our international counterparts regarding the implementation of a pilot Data Protection Trustmark (DPTM) certification scheme for businesses in Singapore[51] and a privacy trust mark scheme for products, services or processes launched by the New Zealand Privacy Commissioner in 2018.[52]

The OAIC is also monitoring implementation of trust mark provisions in the EU GDPR, where member states and regulators are called to encourage the establishment of data protection certification, seals and marks for the purpose of demonstrating compliance with the GDPR.[53] Adherence to these mechanisms can also be taken into account in imposing penalties under the GDPR.[54]

While the OAIC considers that the Privacy Act provides a strong basis for the protection of personal information in Australia, there is also great interest in understanding other emerging models for privacy and human rights regulation that are intended to enhance protections. The OAIC is particularly interested in the AHRC's work with the World Economic Forum which will explore the idea of an Australian organisation to lead responsible innovation in areas of new technology.[55] The OAIC would welcome the opportunity to engage with the AHRC about these matters in the future as well as other measures considered in the course of this inquiry to enable and empower individuals to make informed decisions about their personal information.

Yours sincerely,

Angelene Falk

Australian Information Commissioner
Privacy Commissioner

19 October 2018

[1] <http://www.un.org/en/universal-declaration-human-rights/>.
[2] 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>.
[3] *Privacy Act 1988* (Cth), s 2A(h).
[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] Section 2A of the Privacy Act.
[6] Section 2A of the Privacy Act.
[7] 'Personal information' is defined in s 6(1) of the Privacy Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable.
[8] APP 1 outlines the requirement for an APP entity to manage personal information in an open and transparent way.
[9] See APPs 3, 4 and 5 (collection of personal information).
[10] See APPs 6, 7, 8 and 9 (use or disclosure of personal information).
[11] 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.
[12] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.
[13] 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.
[14] *Privacy Act 1988* (Cth), ss 26E, 26G, 26P and 26R.
[15] <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017>
[16]<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
[17] Issues Paper, p. 15
[18] Privacy Act 1988 (Cth), s 33C.
[19] Privacy Act 1988 (Cth), ss 36, 40 and 52.
[20] Privacy Act 1988 (Cth), s 80W.
[21] <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>
[22] <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>
[23] <https://www.oaic.gov.au/elearning/pia/welcome.html>
[24] <https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx>.
[25] <https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx>
[26] <https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica>.
[27] <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison>.
[28] See *Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation* <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>.
[29] <https://www.oaic.gov.au/engage-with-us/community-attitudes/>

[30] <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>.
[31] Online privacy policies: Australian Privacy Principle 1 – Summary of assessment
[32] <https://www.oaic.gov.au/engage-with-us/networks>.
[33] <https://www.oaic.gov.au/paw2018/>.
[34] <https://www.oaic.gov.au/individuals/data-breach-guidance>.
[35] <https://www.oaic.gov.au/individuals/faqs-for-individuals/all/>.
[36] <https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-48-ten-privacy-tips-for-parents-and-carers>.
[37] Chapter 6 of the Issues Paper.
[38] Issues Paper, p. 28
[39] < https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles>.
[40] <https://www.data61.csiro.au/en/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework>
[41] Issues Paper, p.30
[42] <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act>
[43] Page 33 of the Issues Paper.
[44] Article 22 of the GDPR.
[45] EU GDPR, Articles 13(2)(f), 14(2)(g), 15(1)(h)
[46] Office of the Victorian Information Commissioner, June 2018, *Artificial intelligence and privacy – Issues paper*, available at <https://ovic.vic.gov.au/resource/artificial-intelligence-and-privacy/>
[47] Commission Nationale Informatique & Libertes (CNIL), December 2017, *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*, available at <https://www.cnil.fr/en/how-can-humans-keep-upper-hand-report-ethical-matters-raised-algorithms-and-artificial-intelligence>
[48] See outline of CIPL's project on *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice* at <https://www.informationpolicycentre.com/ai-project.html>
[49] Updates including adopted resolutions are progressively posted to <https://icdppc.org/>; see also <https://icdppc.org/document-archive/adopted-resolutions/>
[50] Issues Paper, p.24
[51] In March 2018, the Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) launched an open call for organisations to participate in a pilot for Singapore's Data Protection Trustmark (DPTM) certification. According to the IMDA, the scheme aims to foster sound, transparent and accountable data protection practices among Singapore-based organisations and was developed in consultation with the industry. Organisations certified under the DPTM scheme will be able to use and display a DPTM logo in their business communications for the duration of the certification, which is three years. <https://www.imda.gov.sg/about/newsroom/media-releases/2018/imda-and-pdpc-launch--pilot-of-data-protection-trustmark-certification-scheme>
[52] <https://www.privacy.org.nz/news-and-publications/statements-media-releases/new-privacy-trust-mark-certifies-privacy-and-customer-control/>
[53] EU GDPR, Articles 42 and 43 and *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (see <https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_en>).
[54] EU GDPR, Article 83(2)(j)
[55] Issues Paper, p. 24 and 35