



Australian Government
**Office of the Australian
Information Commissioner**

Human Rights and New Technology

Submission on the Artificial Intelligence:
Governance and Leadership white paper

oaic.gov.au

OAIC

Contents

Introduction	3
International data protection developments on AI	3
The Responsible Innovation Organisation	5
Australia's Privacy Framework and AI	6

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make this submission to the Australian Human Rights Commission (AHRC) and World Economic Forum's (WEF) white paper, *Artificial Intelligence: governance and leadership* (the white paper). The white paper provides an opportunity to consider the potential impacts of artificial intelligence (AI) tools on human rights, including the right to privacy enshrined in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR),¹ and given effect in the Australian context by the *Privacy Act 1988* (Cth).

The use of AI has rapidly expanded in recent years and has the potential to create benefits both for organisations and individuals. There is also potential for AI to impact human rights. The right to privacy is an enabler of other human rights, and compliance with privacy obligations can mitigate against other adverse impacts, such as discrimination. Accordingly, given the inherently data-driven nature of AI technologies, which generally rely on personal information, privacy and data protection is a central pillar of the regulation of AI. Notably, personal information flows across national borders, so having a robust data protection framework, which is interoperable across international regulatory regimes, will be key to mitigating the impact of AI technologies on other human rights.

Accordingly, the OAIC suggests that any examination of the regulation of AI needs to take into account existing domestic and international privacy and related frameworks, policy and guidance, identify any regulatory gaps and seek to build on these current foundations. In this way, we can ensure a robust system that reduces duplication and fragmentation, and seeks alignment with global frameworks, for the benefit of organisations, governments and individuals.

This submission provides information on developments in AI regulation by international data protection regulators, presents details on where we see potential duplication with the proposed powers of the Responsible Innovation Organisation, sets out the current privacy regulatory framework and makes recommendations for further consideration of Australia's privacy laws to ensure that the privacy protection framework is fit for purpose in the digital age.²

International data protection developments on AI

The importance of data protection regulation and governance in addressing potential risks of AI is a current area of significant interest for Australian and international data protection regulators. The OAIC draws on the work of other data protection authorities and seeks to ensure global policy alignment where appropriate. The OAIC suggests that the AHRC may wish to have regard to the following examples of recent work in order to further inform this project:

- The International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a declaration on ethics and data protection in AI in October 2018 which endorsed principles including that AI and machine learning technologies should be designed, developed and used in

¹ Opened for signature 16 December 1966 (entered into force 23 March 1976), [1980] ATS 23, <www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

² See OAIC 2019, *Submission to the ACCC Digital Platforms Inquiry preliminary report* <www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-submission-to-the-australian-competition-and-consumer-commission>, page 9 where the OAIC has previously made this recommendation.

respect of fundamental human rights, and that unlawful biases or discriminations that may result from the use of data in artificial intelligence should be reduced and mitigated³

- The Privacy Commissioner for Personal Data in Hong Kong released a report titled ‘Ethical Accountability Framework for Hong Kong, China’⁴ in October 2018 which considers the ethical processing of data, including in relation to AI tools, and seeks to foster a culture of ethical data governance
- Singapore released the ‘Proposed Model Artificial Intelligence Governance Framework’⁵ in January 2019, aimed at providing detailed and readily implementable guidance to private sector organisations to address key ethical and governance issues when deploying AI solutions
- The European Commission adopted the ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679’⁶ on 3 October 2017 (last revised and adopted 6 February 2018) which provides guidance on the regulation of automated individual decision-making and profiling under EU’s *General Data Protection Regulation*⁷
- The High-Level Expert Group on Artificial Intelligence set up by the European Commission issued the ‘Ethics Guidelines for Trustworthy Artificial Intelligence’⁸ on 9 April 2019 which proposes privacy and data governance as one of seven requirements for trustworthy AI.⁹

On 22 May 2019, Australia signed onto the ‘Recommendations of the Council on Artificial Intelligence’, a non-binding agreement developed by the Organisation for Economic Co-operation and Development (OECD).¹⁰ The guidelines propose a range of principles, including that AI systems should be designed to respect privacy rights, and that the privacy risks of AI systems should be continuously assessed.

³ International Conference of Data Protection and Privacy Commissioners, *Declaration on ethics and data protection in artificial intelligence*, 40th International Conference of Data Protection and Privacy Commissioners, Tuesday 23rd October 2018, Brussels, <https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf>.

⁴ Office of the Privacy Commissioner for Personal Data 2018, *Ethical Accountability Framework for Hong Kong, China* <www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf>.

⁵ Personal Data Protection Commission Singapore 2019, *A Proposed Model Artificial Intelligence Governance Framework*, <<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/A-Proposed-Model-AI-Governance-Framework-January-2019.pdf?la=en>>.

⁶ European Commission Article 29 Working Party 2018, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826>.

⁷ These guidelines were adopted by the European Data Protection Board in its first plenary meeting on 25 May 2018 <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>

⁸ High-Level Expert Group on Artificial Intelligence 2019, *Ethics Guidelines for Trustworthy Artificial Intelligence* <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477>. This guideline was first released for comment on 18 December 2018, and was issued as final on 9 April 2019.

⁹ For additional examples, see the Office of the Victorian Information Commissioner, *Artificial intelligence and privacy: Issues paper*, June 2018, <<https://ovic.vic.gov.au/resource/artificial-intelligence-and-privacy/>>, and Office of the Information Commissioner (UK), *Big data, artificial intelligence, machine learning and data protection*, 2017, <<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>>.

¹⁰ Organisation for Economic Co-Operation and Development 2019, *Recommendations of the Council on Artificial Intelligence* <<https://legalinstruments.oecd.org/api/print?id=648&lang=en>>.

The Responsible Innovation Organisation

The white paper asks whether there would be significant economic and/or social value for Australia in establishing a Responsible Innovation Organisation (RIO).

The OAIC recognises that increased collaboration and harmonisation of efforts across government and industry is desirable to manage AI risks as AI tools take on greater significance. There are a number of parallel processes occurring alongside the AHRC's work, including work by Australia's Data 61.¹¹

Accordingly, the OAIC considers that there may be benefit in an organisation having responsibility for leading research and ensuring coordination and collaboration. Such an organisation could act as a centre of expertise and a resource for regulators and others and may be performed by an existing or new body.

However, the OAIC considers that in developing any proposal for an RIO, caution should be exercised in considering any additional regulatory roles which risk duplication, inconsistency, increased complexity for regulated entities and a lack of clarity for individuals about their rights. Examples of these issues which may arise from the white paper's suggestions are set out below.

Coercive Powers

The white paper suggests that the RIO could have a range of coercive and non-coercive powers. Many of these powers mirror powers already available to the Australian Information Commissioner under the Privacy Act. For example, the Australian Information Commissioner currently has powers to:

- conduct assessments (audits) of regulated entities' regarding their compliance with the APPs¹²
- receive complaints and conduct investigations into breaches of the APPs¹³
- make APP codes (referred to above)¹⁴ and guidelines¹⁵
- examine proposed enactments that may have privacy impacts and conduct research into data processing and technology.¹⁶

In the OAIC's view, the creation of a new regulatory body with powers similar to those of the Australian Information Commissioner, in relation to a regulatory scheme that overlaps with the Privacy Act, could lead to regulatory duplication, fragmentation of privacy protections and has the potential to create uncertainty for both regulated entities and affected individuals.

¹¹ Department of Industry, Innovation and Science & Data 61 2019, *Artificial Intelligence: Australia's Ethics Framework, A Discussion Paper* < https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf>. Examples of relevant initiatives being undertaken in Australia and internationally are set out in pages 17-21 of this discussion paper.

¹² *Privacy Act 1988* (Cth), s 33C.

¹³ *Privacy Act 1988* (Cth), ss 36, 40, 40.

¹⁴ *Privacy Act 1988* (Cth), Part IIIB.

¹⁵ *Privacy Act 1988* (Cth), s 28.

¹⁶ *Privacy Act 1988* (Cth), s 28A.

Non-coercive powers

The white paper also suggests several non-coercive functions for the RIO, such as evaluating data sets, developing leading practices, and developing codes of ethics.

The recently introduced UK Centre for Data Ethics and Innovation (CDEI),¹⁷ referred to in the white paper, may be a suitable model to draw from when considering the role and powers of a proposed new body in this area. In particular, the OAIC notes that the CDEI is not in itself a regulatory body. Rather, the CDEI operates alongside and supports existing regulatory structures, drawing on evidence and insights from across the regulators, academia, the public and business. A similar body could have value in Australia, providing a central source of AI and technological expertise and capability to Australian Government agencies, including regulators.

It would be appropriate and necessary for existing regulatory bodies with expertise in particular areas (such as privacy, human rights, consumer protection or competition) to be closely involved in the exercise of these non-coercive functions. The OAIC has previously worked with Data 61 in developing a *De-identification decision-making framework*,¹⁸ and such collaborations may also be useful in addressing AI risks, by bringing together technical and regulatory capabilities.

The OAIC also suggests that clarity would be needed about the scope of any RIO's functions. While the white paper is focused on AI in particular, it appears the proposed RIO may have a role in a wider range of innovations, beyond AI. If the intention is for the RIO to have a wider role, then we again recommend that careful consideration be given to existing regulatory arrangements.

Australia's Privacy Framework and AI

The role of existing data protection regulations

The OAIC's view is that there is scope within the existing regulatory framework, with appropriate adjustments, to increase accountability in the use of AI and related technology and to ensure effective oversight.

The OAIC regulates under the Privacy Act, which contains the 13 Australian Privacy Principles (APPs), designed to be technology neutral, flexible, and principles-based which can adapt to changing and emerging technologies – including AI. The existing framework contemplates that additional regulation may be required and contains mechanisms to adapt the regulatory regime to changing circumstances.¹⁹ For example, the Australian Information Commissioner and Privacy Commissioner has the power to approve and register enforceable 'APP codes' or prepare guidelines which can provide greater particularity around the application of principles-based law.

Data protection regulation, both in Australia under the Privacy Act and internationally,²⁰ typically includes a number of core data protection principles, such as:

- Collection limitation - An entity may only collect personal information that is reasonably necessary for the entity's functions or activities. This principle is reflected in APP 3

¹⁷ <www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei>.

¹⁸ OAIC & Data61 2017, *The De-Identification Decision-Making Framework* <www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework>.

¹⁹ For example, if a need was identified to make AI algorithms more transparent, this could be achieved by enhancing existing transparency requirements under the Privacy Act (in particular APPs 1 and 5).

²⁰ Many data protection regulations, including the Privacy Act, draw on the principles set out in the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); see <www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

- Purpose specification and use limitation - Personal information should be collected for specified purposes, and those purposes should be made known to the individual. Personal information should generally not be used or disclosed for purposes other than the specified purpose of collection. This principle is reflected in APPs 5 and 6
- Openness and accountability - An entity should be open and transparent about the way it deals with personal information and should be accountable for complying with data protection principles. This principle is reflected in APPs 1 and 5
- Data quality - Personal information should be relevant, accurate, complete and up-to-date for the purpose for which it is to be used. This principle is reflected in APPs 3 and 10
- Individual participation - Individuals should have rights to access personal information held about them, and to have inaccurate, out of date, incomplete, irrelevant or misleading personal information corrected. This principle is reflected in APPs 12 and 13.

Adherence to these principles can address privacy-specific risks of AI tools.

Additionally, these data protection principles have an important role to play in addressing broader AI risks. For example:

- a lack of transparency about the algorithm used in an AI tool could be addressed through increased openness and accountability
- poor quality data used to train an AI tool, or poor quality predictions of an AI tool, could be addressed through the data quality and individual participation principles.

AI presents challenges to individuals' privacy—including ensuring that personally identifiable information used to train AI systems is accurate, and is collected and handled in accordance with legal requirements and community expectations. While these challenges are heightened, they are not unique to AI. In general, there is a need to ensure that organisations using a range of technologies are accountable for handling personal information appropriately. This may be achieved through increased transparency, building in privacy by design and putting in place an appropriate system of assurance. Such assurance could include third party audit or certification,²¹ in addition to regulatory oversight, to increase consumer trust and confidence.²²

Further review of privacy protections in Australia

The OAIC appreciates that some international data protection regulations include additional principles beyond those rights and obligations in the Privacy Act. In particular, the EU's *General Data Protection Regulation* (EU GDPR) includes certain rights and obligations in relation to automated decision making and profiling,²³ which may be of direct relevance to AI tools that are used to assist or replace human decision-makers.

²¹ See the OAIC 2019, *Submission to the ACCC Digital Platforms Inquiry preliminary report* <www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-submission-to-the-australian-competition-and-consumer-commission>, page 5 where the OAIC has previously recommended independent third party certification as a proactive method to increase organisational accountability.

²² The OAIC considers that it is important that technologies that may impact on the lives of individuals, such as AI, have sufficient community support ('social licence'). The OAIC suggests that a social licence for AI should be built on several elements including increasing transparency around AI tools, and ensuring that the community trusts AI tools and understands how their personal information is being used.

²³ EU GDPR, articles 13–15, 21 and 22.

The OAIC recognises the importance of ensuring that Australia's privacy protection framework is fit for purpose in the digital age and suggests that further consideration should be given to the suitability of adopting certain EU GDPR rights in the Australian context where gaps are identified in relation to emerging and existing technologies, including AI.²⁴ Other rights in the EU GDPR that may merit further consideration include the rights relating to compulsory data protection impact assessments for data processing involving certain high risks,²⁵ the right to erasure,²⁶ and the right of an individual to be informed about the use of automated decisions which affect them and express requirements to implement data protection by design and by default.²⁷

²⁴ See the OAIC 2019, *Submission to the ACCC Digital Platforms Inquiry preliminary report* <www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-submission-to-the-australian-competition-and-consumer-commission>, page 9-10 where the OAIC has previously recommended a review of Australia's privacy protection framework. We also note in this respect that the European Commission has sought feedback on the application and implementation of the EU GDPR, including the operation of specific articles under this legislation, and participated in a stock-taking exercise on 13 June 2019 with relevant stakeholders.

²⁵ EU GDPR article 35.

²⁶ EU GDPR article 17.

²⁷ EU GDPR article 25.