



Office of the Information Commissioner Queensland

31 May 2019

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

Artificial Intelligence
Strategic Policy Division
Department of Industry, Innovation and Science
GPO Box 2013
CANBERRA ACT 2600

By email: artificial.intelligence@industry.gov.au

Artificial Intelligence: Australia's Ethics Framework – A Discussion Paper

The Queensland Office of the Information Commissioner (**OIC**) welcomes the release of a discussion paper by CSIRO's Data 61 to inform development of an ethical framework to guide the use of Machine Learning (**ML**) and Artificial Intelligence (**AI**) in Australia (**Discussion Paper**). OIC appreciates the opportunity to provide comments on the Discussion Paper.

About the OIC

The OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the RTI Act and the IP Act to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office reviews agency decisions about access to information, mediates privacy complaints and monitors and reports on agency compliance to Parliament.

The Information Privacy Act in Queensland

Queensland's *Information Privacy Act 2009 (IP Act)* recognises the importance of protecting the personal information of individuals. It creates a right for individuals to access and amend their own personal information and provides rules or 'privacy principles' that govern how Queensland government agencies collect, store, use and disclose personal information. OIC has regulatory oversight of Queensland Government agencies' compliance with requirements under the IP Act.

OIC makes the following comments with a particular focus on the privacy aspects of an ethical framework for the collection, use or disclosure of personal information, noting that the right to 'privacy' is broader than merely information privacy. It also encompasses other types of privacy such as territorial and physical or bodily privacy.

General comments

AI has the potential to deliver enormous benefits to the broader community while at the same time poses a number of risks to the rights of individuals in society, including the right to privacy.

The Office of the Information Commissioner is an independent statutory authority.

The statutory functions of the OIC under the Information Privacy Act 2009 (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment.

This submission does not represent the views or opinions of the Queensland Government.

The right to access information, or right to know, is an integral part of the right to freedom of expression, and both are fundamental underpinnings of democracy and all other rights and freedoms.¹ The RTI Act reflects this fundamental premise by requiring government agencies to make information available to the public unless, on balance, it is contrary to the public interest to do so.

As outlined in the Discussion Paper, some of the risks posed by AI include, for example, algorithmic bias, discrimination, profiling, surveillance and re-identification of data. Concerns about the largely unregulated use of AI in China, leading to concerns about mass surveillance of its citizens, and the development of facial recognition software to predict the sexual orientation of people based on their facial characteristics² illustrate these risks.

OIC provides in-principle support for development of an ethical framework to guide AI and ML in Australia that is largely consistent with the *Declaration on Ethics and Data Protection in Artificial Intelligence* adopted at the 40th International Conference of Data Protection and Privacy Commissioners.³ The Declaration endorses six guiding principles, as core values to preserve human rights in the development of artificial intelligence. The Declaration also calls for common governance principles at an international level.

It is an important first step in promoting discussion, raising awareness and guiding decision making and implementation of AI. However, the complexities of the challenges posed by AI mean that this is unlikely to be sufficient and legal and other regulatory frameworks will be required to mitigate potential risks, including privacy risks, and provide robust governance and oversight of ML and AI. In summary, OIC provides the following general comments about the Discussion Paper:

a) Existing Frameworks, principles and guidelines on AI ethics

The Discussion Paper focuses (at 2.1.4) on the Commonwealth Privacy Act and fails to mention the range of Commonwealth, state and territory statutes and common law principles applicable to the protection of an individual's privacy in Australia, including human rights laws in Queensland, Victoria and the ACT.

Queensland's IP Act only applies to Queensland Government agencies, which include Ministers, Queensland State Government Departments, Local Government and Public Authorities. The IP Act does not apply to Government Owned Corporations (**GOCs**), individuals, the private sector or community organisations unless a contracted service provider is contractually bound to comply with the privacy principles. Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than \$3 million per annum. Even where an entity would ordinarily be covered by the Privacy Act, the IP Act may apply to a bound contracted service provider because exceptions apply.

While it is widely acknowledged that significant gaps exist in the current legislative framework regarding intrusions into the privacy of an individual,⁴ the ethical

¹ Viewed at <http://www.unesco.org/new/en/unesco/events/prizes-and-celebrations/celebrations/internationaldays/world-press-freedom-day/previous-celebrations/2010/brisbane-declaration/>

² https://medium.com/@pervade_team/the-study-has-been-approved-by-the-irb-gayface-ai-research-hype-and-the-pervasive-data-ethics-3b36c5a53eec

³ https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

⁴ Standing Committee on Law And Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, Report (3 March 2016) at page 57;

framework is required to sit alongside existing laws. Accordingly, an AI ethical framework must ensure consistency with the terminology of privacy laws and accepted principles underpinning these laws.

b) Consent

Consent appears to be a central feature of the ethical framework to mitigate privacy risks posed by AI systems. However, the concept of consent is complex. Consent has been criticised, as it is not always specific, informed and freely given due to a range of factors, including imbalance in bargaining power.⁵

Artificial intelligence systems that collect, process, and generate our personal data intensify many ongoing problems with consent, such as giving us adequate notice, choice, and options to withdraw from sharing data.⁶ For example, in the context of being automatically identified by AI or equivalent technologies, such as facial recognition of use of biometric data, it has been argued that there is an ethical obligation to develop entirely new and practical means by which citizens can give verified consent to involuntary methods of identification.⁷

As such the notion of consent is problematic in the context of AI and poses considerable challenges that do not appear to have been fully explored in the Discussion Paper.

a) Transparency and Accountability

Transparency and accountability are essential principles underpinning democracy and are important for increasing public trust in government. Trust in government continues to decline with the OECD reporting only 43% of citizens trust their government.⁸ In Australia, it was recently reported that 41% of Australian citizens are satisfied with the way democracy works in Australia, down from 86% in 2007.⁹ Trust in institutions is important for the success of government, policies, programs and regulations that depend on cooperation and compliance of citizens.¹⁰

Transparency gives the public the right to access government information and requires that decisions and actions made by the government are open to public scrutiny. As outlined previously, the RTI Act in Queensland reflects this fundamental premise by requiring government agencies to make information available to the public unless, on balance, it is contrary to the public interest to do so. From our experience, in external review of decisions about access to information in particular, people tend to seek out information to understand decisions about themselves and especially where the initial explanation has been inadequate. If systems are designed to make it difficult to obtain clear reasons that a person can understand, it is likely they may pursue other less appropriate options.

The adoption of AI technology to automate government decision-making poses a number of challenges for transparency and accountability. While the Discussion Paper

Australian Law Reform Commission, *Serious Invasion of Privacy in the Digital Era*, Report No 123 (June 2014) at [3.50]; *Report: Eyes in the sky*, Inquiry into drones and the regulation of air safety and privacy, Parliament of Australia, Tabled 14 July 2014, Chapter 4.

⁵ Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Preliminary Report, December 2018.

⁶<https://publications.computer.org/security-and-privacy/2018/09/19/ai-and-the-ethics-of-automating-consent/>

⁷ <https://www.euractiv.com/wp-content/uploads/sites/2/2018/12/AIHLEGDraftAIEthicsGuidelinespdf.pdf>

⁸ <https://www.oecd.org/gov/trust-in-government.htm>

⁹ <https://theconversation.com/australians-trust-in-politicians-and-democracy-hits-an-all-time-low-new-research-108161>

¹⁰ <https://www.oecd.org/gov/trust-in-government.htm>

makes it clear that a core principle for use of AI is that a person should be provided with information used by the algorithm to make decisions, it is not clear that this is practicable or even achievable. It has been argued that a human being cannot make coherent sense of all that is going into an algorithm's decision-making process. This is because AI has made an immeasurable number of micro-decisions based on large sets of data, and based on an every evolving mathematical question.¹¹

Although the right to an explanation is meant to protect data subjects from biased and harmful automated decision making, it is also clear that the lack of certainty on how exactly this protection can be implemented creates serious obstacles to furthering the development of Artificial Intelligence, and therefore poses risks to the economy as a whole.¹²

Further, community concerns over privacy intrusions, whether real or merely perceived risks, have the potential to undermine community trust and confidence in the use of ML and AI and inhibit the realisation of the benefits of AI to the community.

Questions for Consideration

Q.1 Are the principles put forward in the Discussion Paper the right ones? Is anything missing?

As outlined in the Discussion Paper, countries worldwide are developing solutions to tackle emerging ethical issues regarding use of ML and AI. For example, the European Commission (**EU Commission**) has recently published *Ethics Guidelines for Trustworthy Artificial Intelligence*¹³ prepared by an independent expert group set up by the Commission. The Guidelines list seven key requirements that AI systems should meet in order to be trustworthy. Similarly, the New Zealand Privacy Commission and the Government Chief Data Steward have jointly developed six key principles to support safe and effective data analytics.¹⁴

Given the existence of these ethical frameworks, it is not clear why it was considered necessary to develop a further set of principles to guide the use of ML and AI in Australia. For example, the *Ethics Guidelines for Trustworthy Artificial Intelligence (Guidelines)* underwent an extensive consultation process and were developed by a High-Level Expert Group on Artificial Intelligence (**AI HLEG**) comprising representatives from a broad cross section of society including academia, civil society and industry. Further, the EU, with the introduction of the General Data Protection Regulation (**GDPR**) is widely considered to set a new gold standard for worldwide data protection and privacy law.

OIC supports consistency, wherever possible and practicable, with laws and frameworks that seek to protect the privacy and other human rights of individuals in the face of rapid technological advancements, including those posed by AI. In an increasing digital global economy consistency with national and international frameworks is becoming increasingly important as '*data protection and privacy risks can no longer be assessed from an Australian regulatory standpoint alone*'.¹⁵

For these reasons, OIC considers the development of core principles underpinning an AI Ethical Framework in Australia could draw on those already developed by the EU

¹¹ <https://techgdp.com/blog/artificial-intelligence-right-to-information-explanation/>

¹² See note at 7.

¹³ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

¹⁴ <https://www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/>

¹⁵ <https://www.pwc.com.au/assurance/gdpr.html>

Commission given the EU framework has undergone extensive consultation and for the purposes of aligning more closely with international frameworks for AI use. This approach is supported by the acknowledgement in the discussion paper that *'Australia is likely to be importing "off the shelf" AI developed internationally under different regulatory frameworks.'*¹⁶

Further, OIC considers that the drafting of some of the ethical principles, such as DO NO HARM (Principle 2) and the concept of 'private data' central to Principle 4 Privacy Protection, require re-working to ensure greater clarity about how the principles would apply in practice and to align more closely to existing privacy law.

Q.3 As an organisation, if you designed or implemented an AI system based on these principles, would this meet the needs of your customers and/or suppliers? What other principles might be required to meet the needs of your customers and/or suppliers?

See response to Question 1.

Q.4 Would the proposed tools enable you or your organisation to implement the core principles for ethical AI?

Some of the proposed tools appear to be more akin to high level statements rather than 'tools' to assist agencies to implement the core principles for ethical AI. As outlined above, more nuanced and succinctly worded ethical principles that align with the existing legislative framework, would assist in the development of tools to assist agencies to implement the core principles.

OIC notes that the EU has developed a specific non-exhaustive Assessment List¹⁷ that operationalises each of the key requirements (pilot version at this stage). Introductory information to the Assessment list notes that the aim of this list is to offer a set of specific questions that seeks to ensure the approach to AI development and deployment is oriented towards, and seeks to secure, Trustworthy AI. The EU tool also notes that it is important for those involved in AI development, deployment and use to recognise that there are various existing laws mandating particular processes and the prohibition of particular outcomes, which may overlap and coincide with the measures listed in the Assessment list.¹⁸

Q.5 What other tools or support mechanisms would you need to be able to implement principles for ethical AI?

As noted previously, implementation of ethical principles for AI requires a range of tools and support mechanisms including:

- community engagement and participation
- transparency and accountability to build public trust
- adoption of robust governance and oversight mechanisms; and
- development of regulatory and other legislative frameworks.

To ensure meaningful transparency and accountability it is necessary for government to limit the use of confidentiality clauses when engaging AI services to ensure that such claims cannot inhibit the ability to understand, audit or test their systems for bias,

¹⁶ At page 59.

¹⁷ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/2>

¹⁸ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/2>

error, or other issues.¹⁹ Opaque or ‘black boxes’ make it very hard for the community to understand the decision, or seek redress.

Q.6 Are there already best-practice models that you know of in related fields that can serve as a template to follow in the practical application of ethical AI.

A number of jurisdictions and private sector entities have developed best-practice models for the practical application for ethical AI. As outlined previously, these include the Ethics Guidelines for Trustworthy AI prepared by the High Level Expert Group on AI published by the European Commission.²⁰

OIC also notes that Allens Linklaters has published an AI Toolkit to provide practical guidance for AI projects focussing on ethical, safe and lawful implementation.²¹ The toolkit focuses on the position in Australia and, where relevant the UK and EU, and notes that much of its content is equally applicable to other jurisdictions.

OIC looks forward to opportunities for further consultation in the development of an Ethical Framework to guide the use of AI and ML in Australia.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

¹⁹ AI Now Report 2018 page 22.

²⁰ <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

²¹ <https://www.linklaters.com/en/insights/thought-leadership/artificial-intelligence-toolkit/ethical-safe-legal---a-toolkit-for-artificial-intelligence-projects>