25 July 2023

Technology Strategy Branch
Department of Industry, Science and Resources

By email: DigitalEconomy@industry.gov.au

Supporting responsible AI: discussion paper

The Queensland Office of the Information Commissioner (**OIC**) welcomes the release by the Department of the discussion paper 'Safe and responsible AI in Australia' (**Discussion Paper**). OIC appreciates the opportunity to respond to the Discussion Paper.

About the OIC

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.

Submission

Our submission – by way of responses to the various questions posed in the discussion paper – is set out below.

Definitions

1. *Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?*

OIC has no concerns with the definitions.

Potential gaps in approaches

2. What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?

As OIC noted in our 31 May 2019 submission replying to CSIRO's Data 61 AI discussion paper,[1] AI poses a range of risks that may not be adequately addressed by existing regulation. These include algorithmic bias, discrimination, profiling, surveillance and re-identification of data. Further, the adoption of AI technology to automate government and other entity decision making poses ethical, transparency and accountability challenges.

As the Discussion Paper notes, some of these issues are presently the subject of existing legislative review processes – the recent Privacy Act Review Report,[2] for example, containing several proposals intended to address the privacy impacts of Automated Decision Making (**ADM**).[3] Others may stand to be addressed by the adaptation of and incorporation into the Australian regulatory framework of governance responses either in place or under promulgation elsewhere, such as the proposed Artificial Intelligence Act currently before the European Parliament (**European AI Act**).

3. Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.

OIC notes and supports the eight Australian AI Ethics Principles, which establish useful non-binding parameters for AI development.

OIC has previously supported[4] development of a framework consistent with the Declaration on Ethics and Data Protection in Artificial Intelligence adopted at the 40th International Conference of Data Protection and Privacy Commissioners. 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. The eight AI Ethics Principles appear broadly consistent with these six guiding principles.

Guidance initiatives of the above kind are 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 it is likely that regulatory frameworks and responses will be required to mitigate potential risks, including privacy risks, and to provide robust governance and oversight of machine learning and AI. The absence of sufficiently robust governance responses risks undermining community trust and confidence in the use of machine learning and AI and inhibiting the realisation of the potential benefits each technology may otherwise offer the community.

4. Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.

Ensuring uniformity of approach across economic sectors and jurisdictions should be a key goal of any AI governance response. OIC notes recommendation 29.3 in the Privacy Act Review Report, which proposes establishment of a Commonwealth, state and territory

[1] 'Australia's Ethics Framework – A Discussion Paper', accessible at https://www.csiro.au/en/research/technology-space/ai/ai-ethics-framework (**CSIRO Data 61 AI discussion paper**).
[2] Published 16 February 2023, and accessed 26 June 2023 (**Review Report**).
[3] Proposals 19.1-19.3.
[4] See our 31 May 2019 submission in response to the CSIRO Data 61 AI discussion paper, noted above.

working group with responsibility for developing a harmonised approach to privacy regulation. A similar model would appear to be appropriate for AI regulation.

5. *Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?*

In our 27 November 2020 submission responding to the Commonwealth Attorney-General's Review of the *Privacy Act 1988* Issues Paper, OIC commented as follows:

> ***Ethical use and deployment of Artificial Intelligence (AI)***
>
> *It is OIC's view that a revised Privacy Act incorporates legislative restrictions on the types of decisions that can be fully automated. While OIC welcomes the development of ethical AI frameworks, privacy protections contained in these frameworks are not enforceable. Adoption of legislative restrictions modelled on those provided in the EU under the GDPR are recommended. The GDPR prohibits use of solely automated processing for decisions that produce legal or other significant effects for individuals (unless specific exemptions apply). It also creates rights for individuals who are affected by automated processing.*
>
> *A first step in reform of the Privacy Act is adoption of Article 22 i.e. the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, and potentially article 21 (right to object). Notice of processing is an important first step in building trust through transparency as governments increasingly look to automate government processes and pursue digital transformation. This is critically important, particularly following examples such as Robodebt and the trialling of AI technology in the detection of distracted drivers.*

We reiterated our position in favour of a strong regulatory framework in our 10 January 2022 response to the Attorney-General's Department's October 2021 Privacy Act Review Discussion Paper:

> *…adoption of legislative restrictions modelled on those provided in the EU under the GDPR are recommended. While privacy protections contained in policies and other ethical AI frameworks are welcome, they are not enforceable. The significant impacts ADM can have on an individual's privacy and other rights warrant legislated, enforceable protections. OIC also considers there is likely to be considerable uptake in the adoption of AI across government agencies and the private sector in the future. In the absence of a strong regulatory framework, the risks posed to an individual's privacy is significant.*

OIC maintains the above views,[5] and continues to support the implementation of strong, enforceable responses to the use and implementation of AI technology. To this end, OIC notes the proposed European AI Act may serve as a useful model to consider in developing any Australian approach. Formulated on a risk-based approach, that Act would set down rules establishing:[6]

> *obligations for providers and those deploying AI systems depending on the level of risk the AI can generate. AI systems with an unacceptable level of risk to people's safety would therefore be prohibited, such as those used for social scoring (classifying people based on their social behaviour or personal characteristics).*

Additionally, the European AI Act would entrench transparency, by requiring generative AI systems to both disclose that content was AI-generated, and make public detailed 'summaries of the copyrighted data' used to train such systems. The European rules would

[5] Which were again stated in our 5 August 2022 submission to the Queensland Department of Justice and Attorney-General, in response to its 'Consultation Paper – Proposed changes to Queensland's Information Privacy and Right to Information Framework'.

[6] https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai (accessed 23 June 2023).

also enhance citizen rights to complain about AI systems, and obtain '*explanations of decisions based on high-risk AI systems that significantly impact their fundamental rights*.'[7]

Any future AI governance response might also consider incorporating an overarching 'fair and reasonable' test. Proposed in the Privacy Act Review Report as regards the handling of personal information, a 'fair and reasonable' requirement could in OIC's view readily be extended to other domains such as AI regulation and governance. Such an obligation would confer a baseline, principles-based means of determining the permissibility of a specific AI act, use or practice.[8]

Target areas

6. *Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?*

OIC again emphasises the desirability of uniformity in developing governance responses across jurisdictions and economic sectors as far as possible.

7. *How can the Australian Government further support responsible AI practices in its own agencies?*

OIC notes the Australian Government's proposed Data and Digital Government Strategy, and considers that Foundation Mission 4 of the draft of this document - 'Trusted and Secure' - could be underpinned by a binding whole-of government code mandating responsible AI use within government. Such a code could be premised on the Australian Government's AI Ethics Principles, as further informed by, at a minimum, the Australian Human Rights Commission's 2021 recommendations[9] for legal accountability for government use of AI. Additionally, it may adopt some or all of the key elements of the GDPR, such as those summarised at page 16 of the Discussion Paper – ie, provisions obliging agencies to give individuals:

- *prior notice of the use of personal data in ADM,*[10] *including profiling*
- *a right to access information about the existence of ADM and 'meaningful information about the logic involved, as well as the significance and the envisaged consequences' of such processing to the individual*
- the '*right not to be subject*' to certain forms of ADM.
- rights to request human review/intervention,
- to 'express their point of view' and
- to contest/seek review of any automated decision.[11]

Any code should also restrict or discourage the use of confidentiality mechanisms (such as contractual clauses) by agencies when engaging AI service providers, in order that government use may be adequately explained to those potentially affected, and the subject of meaningful audit and testing procedures.[12]

[7] As above.
[8] Paraphrasing the Review Report's rationale for implementation of a fair and reasonable test within the *Privacy Act 1988*: para 12.3.2.
[9] Contained in its May 2021 'Human Rights and Technology Project Final Report' (**AHRC Report**), accessible at https://humanrights.gov.au/our-work/technology-and-human-rights/projects/human-rights-and-technology-final-report-project (accessed 23 June 2023).
[10] The AHRC Report contains a similar recommendation: Recommendation 3.
[11] Also the subject of an AHRC Report recommendation: Recommendation 8.
[12] A point first made by OIC in our 31 May 2019 CSIRO Data 61 submission (noted above -. see reply to Q 2).

8. *In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.*

No comment.

9. *Given the importance of transparency across the AI lifecycle, please share your thoughts on:*
   a. *where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?*

Transparency is crucial to fostering community trust in the use of AI technology. OIC agrees with the AHRC that '[i]*ndividuals should be made aware when they are the subject of AI-informed decision making*',[13] and supports relevant AHRC Report recommendations to this effect.[14] OIC further considers that the GDPR and draft AI Act currently before the European Parliament together set transparency benchmarks that might be considered for emulation in Australia. OIC further considers that the GDPR and draft AI Act currently before the European Parliament together set transparency benchmarks that might be considered for emulation in Australia, including:

- making it clear at the point of collection if personal information is going to be used with or subject to ADM
- requiring AI-generated content or information to be clearly 'labelled' as such, and
- the various transparency obligations imposed on ADM usage, as imposed by the GDPR and summarised in earlier responses.

   b. *mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.*

As noted above, OIC's view remains that AI governance requires robust and enforceable regulatory responses. The GDPR, and the European Parliament's proposed AI Act currently appear to stand as informative AI governance models.[15]

10. *Do you have suggestions for:*
   a. *Whether any high-risk AI applications or technologies should be banned completely?*

OIC notes the European AI Act risk grading matrix at Attachment B to the Discussion Paper, and suggests this provides useful guidance for both categorisation of and governance response to AI risk in Australia. In short, practices classed as 'Unacceptable' should be subject to prohibition, with obligations then scaled according to assessed risk.

(As the Department is likely aware, the European Parliament has recently expanded the proposed list of 'Unacceptable' – prohibited – practices – to include certain practices such as 'real-time" remote biometric identification systems in publicly accessible space.)[16]

[13] AHRC Report, page 61.
[14] Recommendations 3 (public sector) and 10 (private sector).
[15] A comment made in acknowledgment of the potential shortcomings of the European AI Act, as identified at page 15 of Bell, G., Burgess, J., Thomas, J., and Sadiq, S. (2023, March 24). *Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs).* Australian Council of Learned Academies (accessed 26 June 2023).
[16] Which appears to be graded as a lesser-level 'high' risk in the Attachment B matrix, acknowledging that the Discussion Paper was released prior to the European Parliament's 14 June 2023 consideration of the proposed European AI Act.

b. Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?

Again, the approach adopted in the European AI Act may be instructive – prohibiting, in general terms, AI systems posing an unacceptable level of risk to peoples' safety (such as social scoring), and banning various intrusive and discriminatory uses of AI.

11. What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

OIC suggests that public trust in the use of AI will be best nurtured by promulgation and enactment of comprehensible, robust and enforceable regulatory responses; frameworks that mandate transparency, accountability, adopt best-practice measures,[17] and confer, where relevant, rights of review for those impacted by the deployment of AI systems.

Implications and infrastructure

12. How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?

No comment.

13. What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?

No comment.

Risk-based approaches

14. Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

OIC supports a risk-based approach, as embodied in the European AI Act canvassed earlier in this submission.

15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?

A risk-based approach would allow for proportionate and flexible regulatory responses to identified risks, taking into account all relevant circumstances.

16. Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?

In the interests of harmonisation and simplicity and comprehensibility, it seems to OIC that a uniform, risk-based approach covering all relevant sectors may be desirable.

17. What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?

OIC supports the several principles stated in Attachment C, which together reflect the importance of transparency and accountability regarding AI use and deployment. As noted,

[17] Such as those contained in the GDPR and proposed in the European AI Act.

the European AI Act appears to reflect the 'fullest and latest' iteration of a risk-based approach, which may stand to serve as a useful model for Australian application.

18. *How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?*

Potential duplication might be addressed by appropriately drafted overlap provisions, with a generalised framework 'yielding' or being read subject to the more targeted, specific regulatory regime.

19. *How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?*

No comment.

20. *Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:*

    a. public or private organisations or both?
    b. developers or deployers or both?

As canvassed in earlier responses, OIC considers that the complexities of the challenges posed by AI mean that this is likely that regulatory frameworks and responses will be required to mitigate potential risks, including privacy risks, and to provide robust governance and oversight of AI and associated technologies. The absence of sufficiently robust governance responses risks undermining community trust and confidence in the use of AI and inhibiting the realisation of the potential benefits each technology may otherwise offer the community.

Conclusion

As noted, OIC appreciates the opportunity to make this submission. Should you have any questions or require further information in relation to our submission, please do not hesitate to contact us on 07 3234 7373 or email: administration@oic.qld.gov.au.

Yours sincerely

Paxton Booth
Privacy Commissioner