THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

4 August 2023

School of Law

Submission in respect Safe and Responsible AI in Australia – Discussion Paper

Introduction

I am a professor of law at The University of Queensland.

I studied AI (as part of a computer science degree) in 1986. I have worked as a technology lawyer since 1991 in both New York and Australia. I currently work with as a solicitor or advisor to several businesses who use AI in their products.

The University of Queensland offers a Masters of Law subject titled *Current Issues in Legal Practice - Internet law, AI and Information Technology issues*. I am course coordinator of that subject. I also run seminars for barristers and solicitors regarding how to use AI as part of a legal practice.

This submission represents my opinion. It does not represent an official position of The University of Queensland or any other entity.

I commend the Department of Industry, Science and Resources for conducting the Review. The information provided in the Discussion Paper is useful and advances the debate relating to the regulation of AI. I hope that the current review results in Australia becoming an AI leader.

I make the following comments on parts of the Report only.

General

The current wave of AI advances probably started in 2017 when Google developers published the paper "Attention Is All You Need", and in some peoples' view, only in November 2022 when ChatGPT was released.

Care must be taken not to over-regulate or regulate too early. AI is rapidly developing, both in its ability and application. What we see AI doing today is AI in its infancy. Today, AI is not always reliable or accurate. Tomorrow, that is likely to change. And change is likely to be rapid. What we see happening now is unlikely to be the case at the end of 2025. The factual scenarios regarding the issues currently being debated will also rapidly change in unexpected ways.

Regulation in respect of the camera, if devised in 1870 when the camera was new technology, is unlikely to be useful regulation for an iPhone today. The camera did result in new laws and changes to the law, in areas such as copyright law, privacy law and the law of evidence. But those regulations and changes were developed over decades, looking back at what actually occurred. In respect of AI, it is likely that many regulations if developed today will be outdated within a short period. For example, what may be considered high risk today may be commonplace and low risk tomorrow. Is it better to wait a year or two before making important decisions about the regulation of AI?

The University of Queensland
Brisbane QLD 4072 Australia
T +61 408 220 513
E j.swinson@uq.edu.au
W uq.edu.au
ABN: 63 942 912 684
CRICOS Provider 00025B

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

Access to Data

AI will produce better quality output if more data, more current data and real data is made available to train AI. More accurate AI output will increase public trust and confidence in AI.

The Australian Government has large volumes of data, documents, correspondence and information. It would be beneficial if all of the Commonwealth's data, documents, correspondence and information was made available to Australian AI developers and businesses to train and improve AI technology. This information should be provided by the Commonwealth in electronic form to business on a timely, no-fee copyright-free basis for use for AI training.

Of course, some data should not be provided, for example on grounds of national security or privacy. However, the presumption should be that all data be made available, unless there are real and justifiable reasons not to do so.

Waiting 20 or 30 years for access to this information, as set out in the *Archives Act 1983,* is too long.

I provide this example whether the Commonwealth could assist the advancement of more accurate AI systems:

AI developers have trouble obtaining many sets of data, such as agreed contracts. The full text of all government contracts could be disclosed electronically soon after being signed, to train AI. This should include the full contract terms and schedules.

This would not only be helpful for AI training, but for openness of government. For example, the Queensland Audit Office has reported:

> *"The Queensland Government has adopted a model of openness through the routine release of information to the public. The government aims to make information available to the public as a matter of course, unless there are compelling reasons for keeping it confidential.*
>
> *While confidentiality provisions are required for government to protect sensitive information for itself and its stakeholders, inappropriate use can reduce transparency and public trust in government." (Report 8: 2017–18).*

However, the default position in Queensland, and the actual practice, is not to disclose the terms of government contracts, with virtually all contracts considered to be confidential. It is hard to believe that there are "compelling reasons" to keep every government contract confidential.

Some States reportedly publish the full text of contracts. For example, in South Australia, PC 027 – DISCLOSURE OF GOVERNMENT CONTRACTS[1] requires that for significant contracts, the entire contract be published.

[1] Available at <https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/PC-027-Disclosure-of-Government-Contracts.pdf>.

The Commonwealth Government does not generally publish contracts entered into by the Commonwealth. But it should do so, to assist the training of AI.

In fact, virtually all Commonwealth data could be used to train AI.

Doing so would provide a vast repository of data to train AI, thus creating more accurate AI which would help develop trust in AI and advance the AI economy in Australia.

Similarly, the disclosure of email communications with or within our government would allow AI to be trained to be a better decision-maker in relation to the kinds of decisions regularly made by government.

The Department of Industry, Science and Resources could lead the way in this regard.

Use of AI by the Commonwealth for Providing Information

If Commonwealth information is used to train AI, then AI tools (similar to ChatGPT and Bard) could be used to better provide information to the public. Rather than looking at websites or FAQs, or calling help-lines, an AI tool could chat with a person who is seeking government information and guidance. Such a tool may be more transparent, more informative and provide answers to questions that are easier to understand.

Properly trained AI could be used to educate new government workers and contractors as to how to properly perform their roles – a personal AI tutor that coaches new employees.

Use of AI by the Commonwealth for Decision Making

Decision-making by the Commonwealth is sometimes very slow. Examples include the processing of visa applications, the examination of patent applications, and making decisions in the AAT. Use of AI to assist in government decision-making could only be beneficial for Australia.

For example, the parties to an AAT hearing could have the option of a Member make the decision within a year (such time is not uncommon for appeals regarding partner visa applications) or have AI make the decision within a day.

Additionally, the decision-making AI tool could be made publicly available by the Commonwealth so that the applicants could test what decision is likely to be made before submitting an application for a decision. This would improve the quality of applications for decisions, as the public could then ensure that the appropriate information is provided with the application for a decision and receive feedback from the AI decision-maker. Moreover, third parties could test the AI tool to ensure that it is acting appropriately and lawfully.

Tests could be run to determine whether better decisions are being made by AI or Commonwealth personnel.

In short, the Commonwealth should be developing and testing AI for government decisions and making the AI decision-making technology available to the public. Over the next few years, this technology can be tested on less important decisions, and the learnings can be fed into the development of AI policies of the Commonwealth. Such projects should be trialled sooner rather than later. Doing so will also improve the development of AI skills for Australians.

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

I am cautious regarding a risk-based approach.

Banning technology, at this point in time, based upon a risk (which is a chance of something negative happening – not a certainty), seems to be premature and overkill. There are ways to deal with risks other than making something illegal.

The EU has developed categories of risks, and put uses of AI into categories. This itemisation is subject to debate, is potentially incomplete, and is not future-proof. For example, "AI used by public authorities to verify documents" does not appear to me to be "high risk" for most documents. Maybe it is "high risk" for a special category of document, but not for most categories of documents.

Most AI that I have seen in operation assists with administrative tasks and would be considered low risk. The risk is even lower if the AI is used to provide input to a human decision-maker, because the human can discount or ignore the AI output where appropriate.

I have seen AI used to prepare a meeting summary and a to-do list based on listening to a meeting. For most meetings, this would be low risk. And the output of the AI can be easily checked by attendees who were at a meeting (similar in the way that minutes of meetings prepared by a human are checked and adopted at the next meeting). Moreover, the output of the AI meeting summary program appears to me to be more accurate and helpful than notes taken by a disinterested human.

As another example, I have seen AI used to prepare chronologies from a bundle of documents. This involves identifying all events, determining the date/time of the event where possible, and then producing a short summary of what happened at that date/time. Junior lawyers often spend days preparing chronologies for court cases. AI does this accurately in seconds.

These two examples, like many examples of the use of AI that I have seen, are benign. I cannot image what new regulation is needed for such use of AI.

There is a risk that a risk-based approach to AI creates unworkable categories and extra overhead, for little benefit for the majority of uses of AI.

That being said, the use of many of the high-risk categories identified by the EU do require significant care, and a number of the requirements identified by the EU in relation to AI use appear to be good practice regardless of the risk category. For example, the requirements of:

- Notify humans that they are interacting with an AI system
- Inform provider of any serious incidents or malfunctioning
- Keep up-to-date technical documentation
- Ensure robustness, accuracy and cybersecurity

are worthwhile requirements. One may question whether the current law already requires many of the identified practices, regardless of the level of risk.

Generally, I favour a "right to know" when AI is being used, and the right to opt-out or require a human only or a human second stage review. However, as use of AI becomes more

commonplace, we may become overwhelmed with disclosure and opt-out notices (similar to what happened in Europe in relation to online cookie notices), and we may just tune-out rather than opt-out. Do I really need to know that AI is being used to assess my credit card application (compared to a non-AI decision engine that has been used for many years or to a poorly trained offshore business processing outsourced service provider)? Do I care that AI was used to rewrite in simpler English an email that my lawyer sent to me? What does it matter if I make a restaurant reservation by chatting with an AI system rather than a (potentially biased) hotel concierge or restaurant employee?

What troubles me the most is that AI is producing outputs that the developers and users of the AI cannot explain. AI is not human and does not act in the same way as a human. Transparency is difficult. Ensuring an appropriate degree of transparency may be impossible today for the best AI systems. Does this mean we do not use these systems? Or should we just push on and use them with caution? Are these AI products inherently unsafe? Who should be responsible for these AI products – the person who developed the AI engine, the person who trained it, the application developer who incorporated it for a specific application, or the user who deployed and used it?

AI systems are being developed by teams of people, often in different locations, and these AI systems can be used remotely. I can access an AI system in Singapore to create a meeting summary of a meeting on Zoom that has participants from Australia, New Zealand and Canada. I can access an AI system in Ohio to assist me prepare a contract for use for the sale of an Australian business to a French company. I can access an AI system in Ireland to help me decide what tourist attractions I should visit in Miami. An important question is when Australian law should apply (or should not apply) to the development and use of "global" AI technology. It would not be helpful to have contradictory rules from more than one jurisdiction apply to a single act. It would not be helpful to drive AI development or use offshore because of overbearing or premature regulation in Australia.

On the other hand, Australia is too reliant on data centres, cloud computing and AI technology owned by foreign multi-nationals, who do not necessarily act in Australia's interest and who send billions of dollars in profits offshore. These multinationals even threaten to move jobs away from Australia if their demands for operating unfettered by Australian law are not met.

It is difficult to balance the need for regulation to protect Australians with over-regulation that may create unnecessary complexity and drive innovation offshore to the detriment of the Australian economy.

Conclusion

There are many other AI issues to be considered that appear to be outside the scope of this review. For example, many private businesses who train AI regularly infringe copyright. Content creators are not being compensated even though rich multi-nationals are profiting from this content. Many of these infringers advocate that this is "fair use" but it does not appear fair to all. These infringers have a history of seeking forgiveness tomorrow rather than acting lawfully today.

Another important issue is the reliability of evidence in court proceedings when "deep fakes" can be created by AI to "prove" that almost anything you can dream of occurred.

Further consultation on a range of AI issues is no doubt necessary.

I look forward to the outcome of this consultation.

If I can be of any further assistance, or provide you with any further information, please do not hesitate to contact me.

John Swinson
Professor of Law

4 August 2023