Submission for Safe and Responsible Ai in Australia

By Gregory Long BA(Hons), BSc(Computing), Grad Dip Ed, MMgt

ABOUT ME

I have been an IT professional since the 1980s, and sub-majored in Artificial Intelligence in my computer science degree. During my career, I have played key roles in implementing Practice Management Systems, Data Warehouses, Business Intelligence Systems and Geographical Information Systems. I also implemented ISO 27001:2013 Information Security for the Audit Office of NSW and was one of the three authors of the 2010 Electronic Information Security Performance Audit of the NSW Public Sector. I work with Artificial Intelligence in my current role.

Please find in **blue** my responses to “How to get involved”. I have only addressed some of these as some fall outside my expertise.

**Definitions**

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

**and why?**

I disagree with the definition, not so much because it is inaccurate (it’s not really) as much as because the wording can be unintentionally misleading, especially the use of the term “automation” which is open to misinterpretation. I would prefer:

“Artificial Intelligence (AI) refers to an engineered system that emulates human-like learning and behaviour. In doing so it can generate outputs such as speech, content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without requiring explicit programming.”

NOTE: There are also several thoughts on how to classify AI, such as the seven patterns of AI. Maybe worth looking at those.

**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?**

**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.**

**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.**

* Establishment of AI governance framework similar to governance and security frameworks currently in place for general ICT, including establishment of responsibilities and key roles
* Establishment of an Australian AI Professional Body requiring recognised professional qualifications and a set of professional standards and ethics
* Establishment of an AI Body of Practice within Australian and State Governments to share best practices and coordinate aforementioned governance mechanisms
* Establishment of AI Auditing framework and appropriately qualified teams within National and State Audit Offices.

**Responses suitable for Australia**

**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?**

**Target areas**

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

Generally, no. The approaches should be the same. However, I feel that in small businesses (sole proprietors etc) the assurance costs may be prohibitive. In such cases, an alternative pathway may be considered.

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

* Agencies must not be permitted to implement AI without appropriate governance, monitoring and retraining practices in place.
* Agencies must train AI users in appropriate practices and regulations
* Agencies must have qualified Data Engineers and Data Scientists involved with every AI implementation.
* Agency Annual Reports must include an AI component that lists AI systems and must have the Agency CEO/CIO sign-off on appropriate governance being in place.
* The Australian National Audit Office (and all state Audit Offices) must form teams specialising in AI performance audits (probably outsourcing in the short term but with the goal of eventually forming in-house teams). These teams must include qualified Data Engineers and Data Scientists.

**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.**

**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?**

The nature of Deep Learning models is that they contain so-called Hidden Layers and these are impossible to examine. Some people wrongly believe Algorithmic Transparency is possible at this level. It’s not. However, Systemic Transparency is possible. For example, training data is easy to verify and validate. Another example, compare expected outputs to actual outputs. Both of these are good means of transparency. Basically, visibility of everything else that went into building the AI even if the AI model itself is not transparent.

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

* Mandate AI workers as **qualified** professionals like doctors, lawyers, accountants etc who must maintain professional standards (including ethics and transparency). Set up a professional body to manage this. Exclusion from that professional body prevents both public and private sector organisations from employing such individuals.
* Include AI component in all Annual Reports.

**10. Do you have suggestions for:**

**a. Whether any high-risk AI applications or technologies should be banned completely?**

**Lethal autonomous weapons** are problematic. On one hand, I can understand their use in an international or criminal conflict situation. By using them we reduce the risk to the lives of our own people (soldiers in combat, police in high-risk criminal encounters). But in using them we also introduce the risk of lethal consequences to civilians and bystanders. Perhaps the use of these should somehow be tied to human handlers, without which they automatically switch off. Or else, we limit the extent of damage with which these type of Ais can inflict by restricting them to small arms or anti-weapon use.

**Deep Fakes of Public Figures** (especially politicians and senior government officials) are dangerous as they can destabilise society. I would say this is important and should even cover situations such as comedy and parody.

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

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

**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?**

In this I would follow international conventions to ensure that our trade is inline with other nations.

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

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

Yes. This said, the risk-based approach should be sufficiently rigorous to demonstrate that all risks have been identified and appropriately mitigated. Perhaps the introduction of a template or guide to assist?

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

The application of a risk-based approach in an organisation by an individual without suitable understanding of AI would render it useless. A risk-based approach only works where a suitably qualified individual makes the assessment.

**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?**

No. Risk assessments must consider:

1. Who is making the risk assessment
2. Which stages in the pipeline the risk assessment is applied.

Hence all AI implemented on-premises or as a paid service:

* must be risk assessed by the creator/vendor for assurance of validity of the model and verification of outcomes (some sort of certification provided to customers/clients). The person conducting the assessment would be a data scientist and/or data engineer.
* must be risk assessed by the implementor to assure ethical concerns have been considered. In this case a business expert (a proprietor in a small business or a business analyst in a large corporation) can use a provided framework to make the assessment.

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

I generallysupport Attachment C but feel that the establishment of a profession to ensure that this is undertaken consistently and comprehensively is key to success. I understand that the argument against such a profession will revolve around the higher salaries expected by such professionals (and therefore the cost to the private and public sectors). The decision to not support such a profession will be based upon the government’s appetite for risk should AI cause a major public crisis resulting in death, injury or major financial losses.

**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?**

The establishment of an AI Professional Practice would approach this question.

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

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**?