Making privacy core business

Submission –

Safe and responsible AI

in Australia

Discussion paper

26 July 2023

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000

Technology Strategy Branch
Department of Industry, Science and Resources
Via email: DigitalEconomy@industry.gov.au

26 July 2023

Submission:
Consultation on Safe and Responsible AI in Australia – Discussion Paper

Introduction

Thank you for the opportunity to participate in the consultation on Safe and Responsible AI in Australia – Discussion Paper (the Discussion Paper). This submission can be made publicly available. In this submission, Privcore references, where relevant, points made in its submission in response to the 2019 Discussion Paper on Artificial Intelligence: Australia's Ethics Framework.

This consultation is taking place against the backdrop of generative AI being developed and rapidly deployed globally, often in circumstances where it is not compliant with existing laws and with limited consideration of the risks to people and their personal information. As such, numerous lawsuits have commenced and regulators are intervening and blocking advancement until compliance issues are resolved and risk assessments undertaken.

The use of well-funded regulatory sandboxes in Australia to test the risks of such technology before rolling out to the mass public and generating harms would be beneficial to all stakeholders. The OECD has recently released a report assessing the use of regulatory sandboxes, including in economies which have established AI regulatory sandboxes which discuss the benefits of this approach from a multi-stakeholder perspective.

Privcore's submission is most relevant to addressing the following five questions. An additional point that has not been raised in the Discussion Paper is also addressed:

- Coordination of AI governance (Question 4)
- Approach to regulation of government and private sector (Question 6)
- Building public trust (Question 11)
- Existing privacy assessment frameworks (Question 18)
- Accountability (Question 20)
- Failure management, remedies and penalties (not considered in Discussion Paper)

About Us

Privcore's team with over 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, algorithmic impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.

Annelies also studied artificial intelligence and machine learning at tertiary level, is a qualified legal practitioner and holds an international MBA. Her bio is available at: www.privcore.com/bios.

Coordination of AI governance (Question 4)

As the Discussion Paper highlights, there are many existing laws that already regulate AI and generative AI including critically privacy and data protection laws globally. These laws are generally technology neutral, including Australia's Privacy Act.

As generative AI becomes immersed into existing services and products, it will become difficult to regulate the technology in a siloed manner. What matters is the impact and the harms created. Any form of regulation should focus on preventing and remediating harms. AI and generative AI doesn't create new harms, it just scales the frequency and impact of existing harms, such as being defamed, being discriminated against, having your privacy or copyright infringed, being subjected to misleading information, being sold products that are defective in the intended context of use etc.

Any new regulation should not duplicate or overlap with existing regulations. The challenge is ensuring that regulators who have subject matter expertise in particular harms can provide their expertise in a coordinated fashion. This could be to an AI coordinator/regulator that can then apply that expertise along with any regulatory gaps it may have carriage of to form a fully informed view without duplicating existing expertise from other regulators. This would also ensure consistency with existing regulatory interpretations of harms that are already regulated, should a separate AI coordinator/regulator be established.

Existing regulators tasked with providing their areas of expertise to an AI coordinator/regulator should be provided additional resources to undertake that work.

Equally important is determining the scope of regulated entities, as existing regulators for the various harms that AI and generative AI exacerbate have varying scope. For example, currently

small businesses are not regulated under the Privacy Act. Consideration may also be given to appeal processes and whether expert appeal bodies are required. For example, in Canada a dedicated privacy appeal body is planned to be established.

Approach to regulation of government and private sector (Question 6)

Both government and the private sector need to ensure appropriate use of AI. Indeed, government should meet a higher standard than the private sector as citizens have no choice but to engage with government agencies. For example, the recent Royal Commisison into the Robodebt scheme showed the impact of the public service not upholding its own standards, not assessing risks and harms and not responding appropriately to concerns raised.

The concept that government is required to meet a higher standard than the private sector is also seen in the application of the Australian Privacy Act. Under the Australian Government Agencies Privacy Code (the Code), government agencies are required to conduct privacy impact assessments for high risk processing activities, whereas this is not mandated for the private sector (though the current privacy reform recommends that this also apply to the private sector).

Algorithmic impact assessments and privacy impact assessments should be required for both government and private sector to assess the risks of AI and generative AI.

Building public trust (Question 11)

The public needs to be confident that risks have been addressed in the development and deployment of AI and generative AI. To that effect, the conduct and the publication of those assessments would assist with building trust, as it enables public scrutiny. Some Australian government agencies build trust through the publication of privacy impact assessments, such as the Australian Bureau of Statistics (ABS). Every Australian government agency is required to keep a publicly accessible register of all privacy impact assessments conducted, and some, like ABS also publish them in full.

Similarly when AI and generative AI is subject to algorithmic impact assessments and privacy impact assessments, these could be published (or at least lodged with the relevant AI coordinator/regulator). In particular, all assessments conducted of medium and high risk applications should be published.

Existing privacy assessment frameworks (Question 18)

The risk methodologies privacy practitioners deploy can be applied to AI and generative AI – commonly known as privacy impact assessments and algorithmic impact assessments.

In particular, as outlined in Privcore's 2019 submission to the Department, AI needs to be assessed when the potential harm from false positive or false negative decisions is either medium or high. The need for assessment further increases when the likelihood that the individual is aware of the

automated processing becomes lower as shown below in the table Privcore developed in its earlier submission.

Table: When AI Needs to be Assessed. Developed by Privcore.		Harm resulting: False Positive or False Negative Decision		
		High	Medium	Low
Probability of individual being aware of the autonomous processing	High			
	Medium			
	Low			

Should those developing or deploying AI or generative AI decide the classification (ie low, medium, high risk) this should be communicated publicly and or to the AI coordinator/regulator. Should an AI coordinator/regulator classify the risk-level of the AI, this should also be made publicly available. Where AI or generative AI has been misclassified, such as low harms when in fact high harms have been generated, greater penalties should be applied, particularly if a self-regulatory approach is adopted.

Accountability (Question 20)

There has been significant discussion, particularly from developers of generative AI that accountability for harms created should flow downstream to the deployers, rather than rest with the developers. See for example IBM's discussion on accountability in its white paper, "A policymaker's guide to foundation models", published 1 May 2023.

In Privcore's opinion, accountability needs to rest with both developers and deployers. The party best able and positioned to mitigate the risks should do so. Often deployers have limited ability to influence the development of AI and generative AI that they wish to deploy in their businesses or government agencies. Developers are generally well-resourced and funded and design the technology in such a way that alterations cannot always be undertaken by deployers, or deployers may not have the bargaining position to commission alterations.

Both private sector and public sector organisations need to be accountable where they develop and/or deploy AI and generative AI.

Failure management, remedies and penalties (not raised in Discussion Paper)

There is no consideration in the Discussion Paper regarding the recourse, remedies and penalties that should exist for the increasing harms that AI, in particular generative AI causes.

Should the existing recourse, remedies and penalties under existing regulatory regimes apply in this context? What safety net for citizens should be in place?

The European Commission published two proposed Directives impacting AI liability in September 2022. The intent is to ensure that people harmed by AI have the same level of protection as those harmed by other technologies in the EU. It would also create a rebuttable 'presumption of causality' to ease the burden of proof for victims to establish damage caused by AI.

Conclusion

Generative AI is a rapidly evolving area which may also have unintended consequences, for example, its impact on climate change. Significant computer graphic, computing power, processing and storage are needed to train models as well as engage in human-like conversations. As such, government policy should look holistically at AI and generative AI's impact on other areas of government policy, such as climate change.

Any approach taken to addressing and minimising risks of AI and generative AI should focus on ensuring the harms are minimised or eliminated. If they are not, the risks and costs are likely to outweigh the benefits to people and society.

Privcore would be pleased to contribute further to this important and challenging area of work.