Human Rights Law Centre

Senator Tony Sheldon
Chair of the Senate Committee on Adopting AI
Parliament House
Ngunnawal and Ngambri Country
ACT 2600

via email: aicommittee.sen@aph.gov.au

30 July 2024

Dear Chair,

Re: Human Rights Law Centre's answers to question on notice

The Human Rights Law Centre wishes to thank the Select Committee on Adopting Artificial Intelligence (**AI**) for considering our submission to this inquiry and for calling on us to give evidence at a public hearing held on 16 July 2024.

At the hearing the we undertook to provide answers to questions on notice, our responses are outlined below.

Question from Senator Darmanin
Provide some examples of where AI has been used for public decision-making and where it has impacted on people's human rights, and whether you've got a transparency model in mind.

- In the United Kingdom, a 2018 trail of facial recognition and AI technology by the London Metropolitan Police, was used to identify 104 previously unknown people who were suspected of committing crimes, all but 2 of the identifications were incorrect.[1] This significant error rate raises serious concerns about the accuracy and fairness of AI in law enforcement, potentially breaching the right to a fair trial and the right to privacy by subjecting individuals to unwarranted scrutiny and mistaken identifications.

- In China a facial identification system powered by AI and other technologies has been used to create a 'social credit' system- a surveillance system to assess the trustworthiness of individuals- which could be used to penalise people for breaches of laws and regulations.[2] This system, particularly when applied to ethnic groups like the Uighur people, could pose risks of human rights violations, including breaches of privacy, freedom of expression, and the right to non-discrimination, as it can lead to excessive surveillance and control, disproportionately affecting marginalised communities.

- In the United States of America, the Correctional Offender Management Profiling for Alternative Sanctions tool (**COMPAS**) uses AI to conduct a risk assessment on the likelihood an offender will re-

[1] Edward Santow, 'Can artificial intelligence be trusted with our human rights?' (2020) *Australian Quarterly,* 10, 14-15.
[2] Ibid.

offend. The tool is used in a number of jurisdictions as a case management tool and to support judicial decisions in sentencing. The algorithms and processes that COMPAS relies on are trade secrets and are not publicly known. In 2016 researchers identified that African American defendants were more likely to be given a false positive indicator of being considered to be high-risk whereas high-risk white defendants were more likely to be given a false positive low-risk score.[3] The COMPAS tool could undermine the right to equality before the law and fair trial by perpetuating discriminatory practices and lack of transparency in judicial processes.

- In Australia, the Australian Federal Police's (**AFP**) use of Clearview AI- highlights significant concerns about how AI tools can impact human rights, particularly the right to privacy. An investigation by the Australian Information Commissioner found that the AFP failed to comply with Australian privacy law and the *Australian Government Agencies Privacy Code* by not conducting a mandated privacy impact assessment (PIA) before using Clearview AI. This tool, which scrapes biometric data from the internet for facial recognition, was used by the AFP without assessing the risks associated with handling personal information, particularly of people not suspected or a crime, or implementing adequate safeguards. The AFP's lapses in privacy governance and training underscored the potential for serious privacy breaches, emphasising the need for robust privacy assessments and oversight when deploying high-risk AI technologies.[4]

- In New Zealand, police use SearchX, an AI tool to predict harm or risk that may arise during a call-out. The tool runs in the background and draws connections between suspects of crime and their wider social networks, geographic, locations, criminal charges and other factors. AI use in predictive policing often relies on data from over-policed neighbourhoods, which can ignore crime in other areas and directs further surveillance to these already over-policed communities. The use of SearchX could lead to a breach of the right to privacy and equal protection under the law, as it could disproportionately target already marginalised communities, exacerbating inequalities and potentially violating individuals' rights to non-discrimination and fair treatment.[5]

- A recent report on the use of AI by the New Zealand government identifies several significant risks in AI-driven decision-making. It stresses the need for independent and public oversight to ensure the accuracy of predictive models. The report also highlights legal challenges, particularly in contexts where statutory powers cannot be delegated without parliamentary approval, and warns against improper reliance on algorithmic tools. Transparency is emphasized as crucial, with a focus on providing understandable explanations for decisions made by automated systems and ensuring that algorithms are publicly inspectable through appropriate policies.[6]

The Human Rights Law Centre recommends that Australia adopt a regulatory model for AI similar to the European Union's (**EU**) AI Act, the EU's model has a particular focus on transparency obligations.

The EU mandates that AI developers and deployers maintain detailed documentation of their processes and products. The EU also requires that AI-generated content is identifiable, and provides clear information about the system's purpose and operations. Such transparency is essential for safeguarding human rights and ensuring public oversight and accountability.

The EU framework also categorises AI systems according to the risks they pose, imposing stringent requirements on high-risk applications, such as those used in predictive policing. Under the EU's framework AI applications that pose an unacceptable risk to safety, livelihoods or human rights are banned outright, which

[3] Felicity Bell, Lyria Bennett Moses, Michael Legg, Jake Silove, Monika Zalnieriute, *AI Decision-Making and the Courts* (Report, 2022), 22. <https://www.unsw.edu.au/news/2022/08/the-ai-decision-making-and-the-courts-research-report-has-been-released>.

[4] Office of the Australian Information Commissioner, *AFP Ordered to Strengthen Privacy Governance* (Media release, 16 December 2021) <https://www.oaic.gov.au/newsroom/afp-ordered-to-strengthen-privacy-governance>.

[5] Alexandra Sims, *NZ Police Are Using AI to Catch Criminals- but the Law Urgently Needs to Catch Up Too*, (Website, 13 October 2023) <https://theconversation.com/nz-police-are-using-ai-to-catch-criminals-but-the-law-urgently-needs-to-catch-up-too-214833>.

[6] Colin Gavaghan, Alistair Knott, James Maclaurin, John Zerilli, Joy Liddicoat, *government Use of Artificial Intelligence in New Zealand* (Report on Phase 1 of the New Zealand Law Foundation's Artificial Intelligence and Law in New Zealand Project, 2019) 3 <https://www.otago.ac.nz/__data/assets/pdf_file/0027/312588/https-wwwotagoacnz-caipp-otago711816pdf-711816.pdf>.

could include AI social scoring systems or toys using AI voice assistance to encourage dangerous or unlawful behaviour.

By implementing a similar approach, Australia can address AI risks effectively while enhancing transparency and accountability in AI development and deployment, thereby fostering public trust while also protecting fundamental rights.

Question from the Chair, Senator Sheldon
Provide commentary on how other regulatory reforms, like those regulating occupational health and safety, could inform the regulation of AI.

The principles underlying Australia's Workplace Health and Safety (**WHS**) laws, which focus on protecting workers by requiring duty holders to eliminate or minimise risks, provides a valuable framework for developing a risk-based regulatory model for AI. Although WHS laws and AI regulation address different domains, both prioritise risk management and safety.

Just as WHS laws mandate that employers take proactive steps to minimise workplace hazards, a risk-based approach to AI regulation, similar to the EU's AI Act, would require AI developers and deployers to identify, assess, and mitigate risks associated with their systems.

By applying this risk-focused mindset, AI regulation can ensure that potential harms are addressed effectively, promoting safety and accountability in the development and deployment of AI technologies. This approach will foster a culture of continuous improvement and compliance, paralleling the proactive risk management seen in WHS laws.

We wish to thank the Committee once again for calling on the Human Rights Law Centre to inform its work. We would be delighted to assist the Committee in any way as it advances its important work in regulating the uptake of AI technologies in Australia.

We have no objections to this correspondence being made public.

Regards,

[redacted]

David Mejia-Canales
Senior Lawyer