Flinders University

Business, Government and Law
Sturt Road, Bedford Park SA 5042
GPO Box 2100 Adelaide SA 5001
P: +61 8 8201 3300
[redacted]

18 August 2023

The Parliamentary Officer
Select Committee on Artificial Intelligence
GPO Box 572
ADELAIDE SA 5001
c/ email: SCAI@parliament.sa.gov.au

Submission to Select Committee on AI

Thank you for the opportunity to provide input on the issues you have raised. The views expressed in this submission are matters of personal academic opinion and do not purport to represent any institutional position. We are each academics from Flinders College of Business, Government and Law who have experience with AI and have contributed to past consideration of its implications and implementation, including industry based experience and projects and Federal consultations (further details are set out in an attachment at the end of this submission).

We take a broad conception of what AI is, without fixating on latest developments or definitions, as the field continues to evolve and has a long history. We conceive of it generally as a system that exhibits some behaviours that might be attributed intelligence. We include heuristic based systems alongside newer version of machine learning and neural networks. We believe that too narrow a conception or focus on definitions not only risks being outdated but also misses the real point surfaced by AI, which is a broader issue around the software-based automation of the socio-technical systems that mediate and shape most elements of our society and economy.

Given our relevant interdisciplinary backgrounds and experience we make a range of contributions to most of the questions highlighted by the Committee, with a particular focus on business, social, ethical and legal implications, as well as some business-related skill set issues for appropriate leadership and people management in implementing Responsible AI. We see significant potential for application of AI across many sectors, including those critical to this State. **Our core thesis is that to achieve the best out of this opportunity, and avoid or mitigate the downside risks, we need to have a clear focus on the people elements.** This includes a focus on leaders, workers, those developing AI and those using it, and those whose lives are impacted by its application whether they are aware of it or not. We advocate an interdisciplinary stance that includes but extends well beyond those skills we represent, and we suggest engagement with all those who shape the development of AI or who are impacted by its application.

1. The current state of AI development, deployment and application across various sectors, with a particular focus on the economic, social and ethical implications for South Australia

We will leave it to others to provide a more factual depiction of the current state of AI development, deployment and application across various sectors, rather we focus on the economic, social and ethical implications. We would however argue that we have more data about the presence of AI businesses, that is, businesses designing and selling AI tools, than we have about their customers, that is, the actual users and uses of AI.

Whilst recent evidence[1] from CSIRO analysis of data for 2015-2019 highlights Adelaide CBD as one of Australia's AI "hot spots" in terms of AI companies (and Prospect/Walkerville in terms of AI patents), it is Salisbury that was the state's highest ranking location for AI job ads, i.e., where the recruitment for AI literate personnel was taking place at the time. Importantly, though, the data also show that all three SA locations were a long way from being the kind of hot spots that distinguished areas in NSW, VIC, QLD and, in terms of job ads, the NT. Furthermore they tell us that narrowly focussing on identifying AI businesses tells only part of a much larger story of the utility and utilisation of AI in everyday business activities. The data are clearly dated and need urgent update,[2] and **we call upon the SA Government to facilitate and actively support this process, along with other research on the social and ethical dimensions of AI within our local context,** while acknowledging that a great deal of work has already been done nationally and internationally on these issues.

Implications for the workplace

Whilst much of the discussion about the risks potentially or provenly associated with AI has focussed on its generic characteristics and uses, there are very specific risk that emerge when AI tools are used in *workplaces*.[3] Conventional technology, from conveyor belts to robots, were designed to work under the guidance of humans. The purpose of (installing) AI, in contrast, is to guide humans, thus reversing the hierarchical relationship between human and machine. This has profound impacts on workplaces and creates new risk and stresses for people working 'in the loop' with automation – let alone for the subjects of decisions produced by fully or partly automated systems.[4] The application of AI in these contexts can be considered as part of the broader development and deployment of "suptech" or supervisory technology. This is a burgeoning field and more modern instances of such software seek to harness AI to this end. It is important to acknowledge that not all applications of such technology are adverse to worker interests, indeed some applications are directed at least in part to improving workplace culture.[5]

The surveillance function of AI, intended to guide workplace behaviour through monitoring and sanctioning, has already been well documented.[6] Other everyday workplace risks include but are not limited to:

[1] Alexandra Bratanova, Hien Pham, Claire Mason, Stefan Hajkowicz, Claire Naughtin, Emma Schleiger, Conrad Sanderson, Caron Chen, Sarvnaz Karimi (2022) Differentiating artificial intelligence activity clusters in Australia, Technology in Society, Volume 71, 102104, <https://doi.org/10.1016/j.techsoc.2022.102104>.

[2] Noting that the more recent CSIRO report 'The geography of Australia's digital industries' (1 August 2023) looks at broader categories of ICT related professions but not AI specialisations <https://www.csiro.au/en/research/technology-space/data/The-Geography-of-Australias-Digital-Industries**>.**

[3] https://www.centreforwhs.nsw.gov.au/research/ethical-use-of-artifical-intelligence-in-the-workplace; Andreas Cebulla, Zygmunt Szpak, Catherine Howell, Genevieve Knight & Sazzad Hussain 'Applying ethics to AI in the workplace: the design of a scorecard for Australian workplace health and safety' <https://doi.org/10.1007/s00146-022-01460-9>.

[4] See e.g. some of the very interesting discussion on this issue in "Government use of Artificial Intelligence in New Zealand" (2019) - Final Report on Phase 1 of the New Zealand Law Foundation's Artificial Intelligence and Law in New Zealand Project <https://www.cs.otago.ac.nz/research/ai/AI-Law/NZLF%20report.pdf> (cited in Chalmers, Human Rights and Technology Project Discussion Paper submission (2020)).

[5] See e.g. Culture Amp <https://www.cultureamp.com/>.

[6] For discussion of some of the workplace surveillance implications of such technology see e.g. Dr Sun-ha Hong, 'Predictions Without Futures' (Public lecture , University of Melbourne Law School on 14 August 2023) https://www.youtube.com/watch?v=jif7_RvQUis.

- accelerated work processes, which has ripple effect in workplace areas and functions beyond the one in which AI is deployed (e.g., accelerated production also requires accelerated procurement or sales);
- new physical accident and health risks owing to the spatial integration of AI machine and human, and the use of AI instruments affecting the human body (e.g., AR and VR tools);
- modified supervisory and relational arrangements when human-human reporting lines are replaced or mediated by machine-human interaction with reduced reciprocity where AI decisions cannot or are difficult to overwrite/question;
- challenge to seniority status principles and/or experience-based decision making autonomy affecting the job content and status for individual employees and the balance of employee task profiles, responsibilities and accountabilities across an organisation.

Besides obvious implications for physical health, each of these risks has the potential to impact psychosocial well-being (as well as privacy).

Current workplace health and safety (WHS) regulations have a strong focus on the promotion of physical safety in workplaces. Whilst this remains relevant to AI applications in workplaces, additional psychosocial risks are insufficiently addressed by current regulation. The recent Australian WHS conducted by the NSW Centre for Work Health and Safety[7] showed that whilst 48% of respondents agreed with the statement that "WHS is a priority when new technology is introduced", 26% did not. Australian business are slow adopters of new technology and especially AI. If this changes, however gradually, the penetration of frontier technologies will affect an increasing number and share of employees – and do so much more radically than conventional, human-controlled technology. Regulation must prepare for this future, and Australia is not alone in being currently under prepared.[8]

Many businesses and government departments are already using AI as a screening tool to deal with job applications, so the impact of AI on work can operate also to exclude people from work opportunities at the outset. This means that AI alone may screen an applicant out of a process. We question the appropriateness of this approach: how is it possible for an AI to make an effective evaluation of a candidate's suitability for a complex role based on some form of automated review of isolated features of a video interview or other material? We are aware of one outstanding candidate that was screened out of consideration for a Federal government role recently by exactly such a process. These risks are not theoretical, they are not future, they are here and now and they have been introduced without any public debate, knowledge, nor necessarily any independent screening of the utility of validity of the tools employed (to say nothing of potential bias of those systems). We refer the committee to some of the issues discussed above in relation to workers' rights, consider the royal decree-law that updated Spain's Ley del Estatuto de los Trabajadores (Worker's Statute Law) in 2021 to include a provision requiring companies to inform employees of the parameters, rules and instructions of algorithms or artificial intelligence as they affect decision-making, working conditions, access to and maintenance of employment, including profiling.[9]

[7] NSW, 'Australian WHS Survey' <https://www.centreforwhs.nsw.gov.au/research/national-whs-radar/australian-whs-survey> .

[8] Simon Jack, 'AI: Workers need more protection, says TUC' <https://www.bbc.com/news/business-66248125> .

[9] Royal Decree-Law 9/2021, which modifies the consolidated text of the Workers' Statute Law (Royal Legislative Decree 2/2015) to guarantee the labor rights of people dedicated to delivery in the field of digital platforms <https://boe.es/diario_boe/txt.php?id=BOE-A-2021-7840>; Carmen Villarroel Luque 'Workers vs Algorithms' <https://verfassungsblog.de/workers-vs-ai/>.

Government could promote a critical understanding of AI risks amongst the public in general and workforces specifically. Initiatives should aim to build 'critical AI resilience', whilst legislation ought to create the venues for the application of that critical resilience, e.g., by mandating employee consultation processes. **We also recommend that government review the Work Health and Safety Act 2012 (SA)** to see what adjustments might be made to safeguard against inappropriate use of AI that could have negative impacts on worker safety and wellbeing.

2. The potential for AI to transform sectors critical to the South Australian economy such as agriculture, mining, manufacturing, and services and the skills required for this transformation

We see significant potential for transformation across many sectors, including those listed but also well beyond. The additional sectors we see impacted include but are not limited to defence, health, education, finance, infrastructure and people management. Again we will leave it to others to provide a more factual depiction of most of these sectors – rather we will focus on a few elements of the skills required beyond those technical skills directly related to the development of AI, including:

- Broader education and awareness
- Design thinking, project management, stakeholder consultation
- Leadership, People management
- Law, ethics, privacy

Broader education and awareness

Broader education and awareness of the current and potential future application of AI is a key starting point. Many parts of our community have a role to play here, including government, the education sector, industry and the not for profit or for purpose sectors who are using these systems. We commend the recommendations of the Australian Human Rights Commission in relation to the importance of the role of education in enabling our society to understand and respond to the use of AI and Automated Decision Making (ADM).[10]

Design thinking, project management, stakeholder consultation

We believe these are critical skillsets for managing AI related issues, whether in terms of regulation or adoption. AI is a tool: like other tools it can be well or poorly used, and its design and implementation can be effective and useful, or wasteful or even destructive. While robodebt was not an example of the application of sophisticated AI, it was a clear example of how automated decision making with a flawed policy approach could lead to billions of dollars in costs, deaths and misery, as well as fracturing public belief in government.

The education system, from schools to higher education, is now delivering more training on these sorts of skillsets, and we believe that good use of human centric design thinking approaches will yield benefits in this area (as in others). Before we can solve problems – with AI or other approaches – we must first understand them thoroughly; and in designing solutions we need to engage those who will be affected by them as collaborators and adopt iterative styles of prototyping and testing potential solutions with those groups.

[10] AHRC, *Human Rights and Technology Final Report* (2021) <https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-final-report-2021>.

Implementing responsible AI – the role of leadership

The findings from the 2022 Responsible AI Global Executive Study and Research project, reported that “[i]n response to the heightened stakes around AI adoption and impending regulations, organizations worldwide are affirming the need for RAI, but many are falling short when it comes to operationalizing RAI in practice”.[11] Accordingly, strong human leadership is required to mentor and monitor responsible design and use of AI so that responsible AI (RAI) frameworks are operationalised effectively in practice. One of the non-regulatory Government initiatives, therefore, is to empower and build human leadership capacity through Responsible AI (RAI) leadership development programs. The focus of the RAI leadership development program should be to equip leaders with skills that would empower them to be actively involved in RAI practices at all levels. Following are the four types of involvement in responsible AI (RAI) practices that the RAI leadership development program can focus on, in no particular order of importance.

Human relations involvement

Human relations involvement signifies that leaders can play the roles of *mentor* and *facilitator* while being involved in operationalising RAI frameworks in practice. Leaders need training in *facilitating* an inclusive work culture and providing a human touch to embed trust and shared meaning regarding ethical AI practices among all stakeholders. Additionally, leaders ought to bridge the functional separation that exists between technical and non-technical experts, listen to ethical AI concerns, and provide empathic *mentoring* to clearly communicate human rights laws and responsibilities related to responsible AI design and use.[12]

Open Systems involvement

The open systems involvement is represented by the roles of *broker* and *innovator*. Being *innovative*, the leaders are required to be proactive visionaries, develop creative foresight and hyperawareness to be able to flexibly scan internal and external environments and identify opportunities and threats to responsible AI. Moreover, multiple perspectives, values and contributions are likely to complicate and challenge the framing of AI problems and responsible AI solutions within organisations. Therefore, leaders ought to be *brokers* with good negotiation skills to present and persuade all key stakeholders to commit collectively to RAI practices.[13]

Internal Processes involvement

The ability to *monitor* and *coordinate* ethical and responsible AI practices effectively is one of the key roles of responsible AI leadership. The *Monitoring* function is key to ensuring proper implementation of RAI

[11] Elizabeth Renieris, David Kiron, Steven Mills ‘To Be a Responsible AI Leader, Focus on Being Responsible’ <https://sloanreview.mit.edu/projects/to-be-a-responsible-ai-leader-focus-on-being-responsible/>.

[12] Ben Shneiderman, ‘Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy’ <https://doi.org/10.1080/10447318.2020.1741118>; Sarah-Louise Richter & Dörte Resch, ‘Leadership in the Age of Artificial Intelligence—Exploring Links and Implications in Internationally Operating Insurance Companies’ <https://link.springer.com/chapter/10.1007/978-3-030-48332-6_21>.

[13] Bogdana Rakova, Jingying Yang, Henriette Cramer, Rumman Chowdhury ‘Where Responsible AI meets Reality: Practitioner Perspectives on Enablers for Shifting Organizational Practices’ <https://doi.org/10.1145/3449081>; Mathieu d'Aquin, Pinelopi Troullinou, Noel E. O'Connor, Aindrias Cullen, Gráinne Faller, Louise Holden 'Towards an "Ethics by Design" Methodology for AI Research Projects’ <https://doi.org/10.1145/3278721.3278765>.

practices such as impact assessment, auditing trails, bias testing, compliance procedures and accountability traces. Developing close supervision skills would result in risk mitigation from the design to deployment stages of AI. In addition, miscommunication may limit the ability of all stakeholders to support RAI development in a unified manner within organisations. Hence, leaders' *coordination* skills are vital to engage in collaborative relationships and effectively manage multiple teams towards the successful implementation of responsible AI practices.[14]

Rational Goal involvement

The rational goal leadership involvement is focused on productivity and is represented by the roles of *producer* and *director*. The leadership skills development in *direction* entails responsible judgement, goal clarification, goal attainment and the ability to evaluate employees' needs and inspire them towards implementation of responsible AI practices. As a task-oriented *producer* responsible for ethical AI outputs, leaders ought to have the ability to clearly define ethical protocols, create ethical AI roadmap, update policies, define system boundaries and implement correct parameters to evaluate AI outputs.[15]

By promoting and supporting the RAI leadership development program as one of the key initiatives across organisations nationwide, the Government can ensure the operationalization of AI regulatory frameworks in practice at all levels.

Law, ethics, privacy

Governance systems, both ethical and legal, have a clear role to play in shaping the appropriate use of AI, and some specific issues are discussed below. There is a lot of available material on ethics issues and guidance that has been adopted at the federal level, although the challenge is really the contextual application of ethics rather than generation of more sets of abstract principles to add to what is already a crowded set of advisory material locally and globally.

Most of the legal frameworks that apply to AI more particularly will be determined at a global or federal level, however there are some important areas that the State Government could examine and look to improve upon. One key area is privacy, and this is an area where existing state controls are particularly poor, acknowledging that the federal government is also reforming this area at the moment within the sphere of its responsibilities. **We see this as a key area for action and recommend that government review the Cabinet Administrative Instruction (Information Privacy Principles Instruction) and consider what more comprehensive privacy protection might be put in place in South Australia, consonant and compatible with pending Federal reforms** as those emerge. Other areas of potential action include WHS laws as discussed above. In addition to legislative reform we acknowledge courts may make determinations that will impact the use of AI.[16]

[14] Keng Siau, Weiyu Wang 'Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI' https://www.igi-global.com/article/artificial-intelligence-ai-ethics/249172; Daniel Schiff, Bogdana Rakova, Aladdin Ayesh, Anat Fanti, Michael Lennon, 'Principles to Practices for Responsible AI: Closing the Gap' <https://doi.org/10.48550/arXiv.2006.04707>.

[15] Keng Siau, Weiyu Wang 'Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI' https://www.igi-global.com/article/artificial-intelligence-ai-ethics/249172; Kolbjørnsrud, Vegard; Amico, Richard & Thomas, Robert J. 'How AI will redefine management' <https://enterprisersproject.com/sites/default/files/how_artificial_intelligence_will_redefine_management.pdf>.

[16] 'How judges, not politicians, could dictate America's AI rules' https://www.technologyreview.com/2023/07/17/1076416/judges-lawsuits-dictate-ai-rules/

3. Issues surrounding the use of AI in the commission of criminal offences

We note that Cyber related offences are more a matter of federal jurisdiction though we can certainly see that AI is potentially a tool used across the full range of criminal activity. **AI deep fake technology poses severe threats to the integrity of online and biometric identification measures used for access to key services, including those provided by government**.[17] We will leave it to others to expand on these matters.

4. The challenges and opportunities of AI in relation to privacy, data security, and the ethical use of AI, including the risk of bias in AI decision making

Privacy and Data security

Whilst the term 'artificial intelligence' implies a degree of independence or autonomy, all AI based systems depend on data. Machine learning systems depend on large amounts of data which can be then used to make predictions about other data sets. The datasets used to train machine learning models frequently contain sensitive personal information. This sensitive information could include health status, sexual and gender identity, political allegiance such as union membership or criminal history. Even where machine learning models are not trained using sensitive personal information, they may still be used to infer this sensitive information about individuals.[18] Initially machine learning models were targeted at generating inferences about individuals for targeted advertisements but can be used to draw inferences in almost any domain.[19] For instance, a machine learning model to predict the likelihood of a person being diagnosed with a disease could be used by health insurers to offer discriminatory pricing.[20] Further, machine learning models have significant potential for 'dual use'.[21] These dual use capabilities have the potential to risk fundamental human rights or lead to unintended consequences. For example, a machine learning model trained to identify sexual identity could be used in a country where homosexuality remains a criminal offence.[22] Another potentially problematic application of AI is the use of AI to determine private sector rents.[23]

The use of machine learning to derive inferences represents a fundamental challenge to both privacy law and a risk assessment-based approach to regulating AI. Under the notice and consent model underpinning Australian privacy law, most regulatory activity focuses on how data is collected rather than how it is used.

[17] <https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai>

[18] Sandra Wachter, 'Data Protection in the Age of Big Data' (2019) 2(1) Nature Electronics 6.

[19] 'Generating User Information for Use in Targeted Advertising' *United States US20050131762A1*, filed on 31 December 2003 (Issued on 16 June 2005) <https://patents.google.com/patent/US20050131762A1/en>.

[20] For discussion of broader abuses see e.g. Adrián Astorgano From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You (8 June 2023)<https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you>

[21] Anna Jobin, Marcello Ienca and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1(9) *Nature Machine Intelligence* 389.

[22] Marcello Ienca and Effy Vayena, 'Dual Use in the 21st Century: Emerging Risks and Global Governance' (2018) 148(4748) *Swiss Medical Weekly* w14688

[23] https://www.analyticsinsight.net/this-companys-ai-algorithm-is-why-us-house-rents-are-going-up/

Once the data collector has obtained valid consent from an individual to use their information, they face limited restrictions on how they use this information. As others have written about extensively, the notice and consent model does not anticipate inferences being drawn using machine learning. Although an individual can access information which has been collected about them, or amend this information if incorrect, exercising this right depends on the individual knowing about this information. If individuals themselves are not aware of what these inferences are, they will not be able to exercise these rights.[24] Therefore, the notice and consent model offer limited tools for regulating the use of machine learning tools. Further, consent does not offer a guarantee against the use of machine learning tools for dual use purposes which the individual may not have anticipated.

There are two legal requirements which should be integrated into Australian privacy law to respond to the risks of big data exceptionalism and machine learning. These legal requirements can exist alongside a risk-based approach to regulating artificial intelligence and machine learning. First, privacy law should mandate that any organisation or entity using personal information to train a machine learning model must follow a 'privacy by design' approach. This approach would require the entity training the model to ensure appropriate technical and organisational measures exist to guarantee the security of personal information. These requirements would need to be implemented prior to the processing of any personal information, including training machine learning models. Implementing this requirement as a pre-requisite would help to ameliorate some of the weaknesses of the notice and consent model with respect to big data research. This privacy by design approach should also require consideration of any potential dual use risks that might arise with that machine learning model in the future.

Second, privacy legislation should mandate that entities implement security measures to protect any data used for training or processed with machine learning systems. There is a risk that even without releasing training dataset, inversion attacks can be conducted on a machine learning model to retrieve data.[25] Although specific technical measures should not be mandated in legislation, advanced privacy enhancing technologies could include homomorphic encryption, differential privacy, and secure multiparty computation. These technical measures should be complemented with appropriate organisational solutions such as separating data custodians and data processors.[26] This combined approach recognises that guarding against privacy threats is contextual and requires continual revision. We note that the Federal government has recently amended some of the privacy law framework and more changes are pending.

Ethical use of AI

The evidence is clear: AI can be bias prone; AI producers and users do not always share the same understanding of the purpose, utility and functionality of AI tools; AI producers cut corners to sell products that may not be suited to the task they are intended for; AI users are not fully aware of how and when their AI tools operate beyond their intended scope (boundary creep).

All these risks require monitoring, which in turn requires transparency. As a matter of principle, there is no point at which transparency ought not to be an option. Transparency may not equate to understanding but

[24] Helen Nissenbaum, 'Deregulating Collection: Must Privacy Give Way to Use Regulation?' *SSRN* (Working Paper, 2017 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092282>.

[25] Michael Veale, Reuben Binns and Lilian Edwards, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law' (2018) 376(2133) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180083.

[26] James Scheibner et al, 'Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis' (2021) 23(2) *Journal of Medical Internet Research* e25120.

is essential for enabling critical review and reflection by users as well as producers of AI. In a workplace context, the national and international evidence is clear: open consultation, information, debate, and discussion across an organisation are key in enabling the safe introduction of AI technology. They also facilitate the collective monitoring of AI impacts on workplaces over time. This is important as those impacts are changeable and vary with the AI implementation stages, use and reach (across part of the organisation).[27] The verdict on the value of mandating transparency may yet be open, however as a minimum, transparency mandates disclosure and documentation of algorithm design and programming, and independent review prior to point of sale.

ADM + risk of bias

Consider the example of the failures connected to the 737MAX. There may be arguments as to whether that software fits within a given definition of AI or ADM. But does that debate really matter in the context of risk and responsibility and regulatory responses? Arguably not: perhaps it is splitting hairs.
Let us then consider 'soft' automation in the broad: robodebt illustrates this. It was not a sophisticated 'AI' based implementation, but in the public imagination and debate it has been cast within the broader schema of AI, robo-advice etc. Really it was a policy decision implemented through a simple algorithm, deployed at scale and speed through software-based implementation, and developed, protected, and sustained by a policy position, failure of oversight and broader culture that was fundamentally human in origin and with dire human costs as well as the obvious financial and reputational impacts. ADM magnifies underlying flaws in our own cultures, processes, and systems of regulation.[28] Technology is not just a tool: "technology is not neutral".[29] Rather: it embodies, and is situated within, culture.

In respect of the risks of ADM we commend the work of the Australian Human Rights Commission to the Committee.[30] **We believe State government has a clear responsibility to ensure that its use of AI takes full account of these issues and is an exemplar of good design and implementation.** The last thing we need – especially if there is a desire to cultivate AI in SA – is to see a rushed and poorly designed implementation result in a state based version of a robodebt style problem. **Provided that State government goes about its work astutely, there is good potential for it to use its role as an acquirer/developer/implementer of AI to drive both economic outcomes and improved societal outcomes, but this is not a given**. The danger of conceiving of AI as a 'magic wand' solution is that we will end up with a 'sorcerer's apprentice' outcome.

5. The potential for South Australia to develop a competitive advantage in AI, including through the development of a strong AI research and development sector, the attraction of AI investment, and the training and retention of AI talent

There are areas where SA already has a competitive advantage in AI, at least with respect to certain sectors and centres. The most prominent of those is defence, which has been using AI in many systems for many

[27] Andreas Cebulla, Zygmunt Szpak, Genevieve Knight 'Preparing to work with artificial intelligence: assessing WHS when using AI in the workplace' <https://doi.org/10.1108/IJWHM-09-2022-0141>.
[28] "The issues that AI governance is often truly about are not technical but deeply normative and distributive—which actors make decisions in society, who bears risks and errors, and what justice should look like procedurally and substantively (Balayn & Gürses 2021)" from Veale, Matus & Gorwa 'AI and Global Governance: Modalities, Rationales, Tensions' Annual Review of Law and Social Science, vol 19, 2023 17.
[29] Melvin Kranzberg, 'Kranzberg's Laws' (July 1986) 27(3) *Technology and Culture* 544.
[30] AHRC, *Human Rights and Technology Final Report* (2021) <https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-final-report-2021>.

decades, including but not limited to multi sensor data fusion (Defence, industry and Flinders University worked on use of ‘blackboard’ agent AI for this application in the 1990s), network intrusion, electronic warfare, a broad range of sensing applications (across all emissions spectra including infrared, radio and optical, from tight beam to broadscale over the horizon), biomimetic vision, command, control, communications, computers, cyber-defence and combat systems and intelligence, surveillance, reconnaissance and beyond. It has involved all of the local Universities, and many specialised co-operative research centres and groups, as well as an array of industry, from defence primes to SMEs. It has also involved international and interstate collaborations, including research, government and industry links. That defence work has had some spillover effects including into health areas: for example earlier work on sensor signal and information processing that was originally defence in application was transposed into cancer screening technologies. Other more recent examples of local spillover include the emergence of Fivecast[31] from intelligence synthesis and processing activities within the Data to Decisions CRC.

There are many other sectors that have developed and deployed AI systems in SA, including in healthcare, agriculture, education and human resource management to name only a few. Some of these are obvious and well known, others less so. Government could engage with other sectors to compile a better picture of the existing deployment to define areas of actual or potential strength.

However clearly this is a very busy space, with extensive and well-resourced competition interstate, let alone the vast majority of funding and expertise which is international. Realistically in AI as in every other field Australia is and will remain a net importer. Still, pockets of opportunity may remain to excel in various niches twinned to areas of existing or emerging competitive strength or natural advantage such as defence, agriculture, and environmental applications. SA should be able to use its general advantages as a place to live and work to help develop and attract talent. We should make more of a virtue of the realities of our position: our smaller scale makes collaboration and action easier - if there is common will and co-operation across different sectors.

Regards,

Robert Chalmers, Senior Lecturer
Dr Andreas Cebulla, Associate Professor in The Future of Work
Dr Rajesh Johnsam, Senior Lecturer
Professor Tania Leiman, Professor and Dean of Law
Dr James Scheibner, Lecturer

[31] A great local startup that now employs hundreds of people and has offices internationally - <https://www.fivecast.com/>.

Attachment – Group Background in AI related matters

Robert Chalmers has worked on AI related matters since the early 1990s in the course of legal and commercial work for Defence and the University of Adelaide, including as a board member on an AI spinout company. He has a keen interest in AI regulation and has submitted to a range of recent consultations, including the Australian Human Rights Commission's report, and the recent Federal consultation on responsible AI regulation. Rob teaches innovation and technology topics that examine a range of issues including the application of AI. He is interested in the development of participative regulatory frameworks that might better avoid the negative effects of poorly targeted excessive regulation while still curbing harms.

Andreas Cebulla has collaborated with colleagues at the University of Adelaide and in AI businesses in the private sector, supported with NSW government funding, to develop a framework for assessing workplace health and safety risks in environments increasing exposed to AI. The research team worked closely with national and international data science experts and businesses across Australia that were deploying AI in the workplace. The resulting framework provides a step-by-step guide for assessment AI-related risks during the design, deployment and application of AI tools modifying workflows and rosters, production processes or service delivery, or supply chains.

Rajesh Johnsam is working on multiple projects in collaboration with researchers from India and Australia on human leadership in responsible AI; over-reliance on AI decision tools, and human treatment of AI. In 2022, Rajesh worked on a Govt project with AITI team at Flinders on the 'Evaluation of the Australian Government AI Capability Fund (AICF)'. Rajesh was involved in developing a Theoretical Framework (Technology, Organisation and Environment) to evaluate AI capability development initiatives by Government and Organizations.

James Scheibner teaches a range of relevant topics, looking at both the regulation of AI and its development in the law. He has a strong interest in data protection and health law. His research interests also extend to bioethics, institutional economics (such as common pool resource theory) and the application of these fields to these areas of law.

Tania Leiman has researched the legal implications of future mobility solutions (including automated vehicles & advanced driver assistance systems), sex robots, ovulation apps and wearables, AI and legal tech, and the future of legal education. She has previously served as SA representative, National Advisory Board of the Australian Society for Computers and Law; invited member, National Transport Commission's Automated Vehicles Industry Insights Group; and member, Legal sub-group, Australian Driverless Vehicle Initiative's Policy & Risk Group.