Ernst & Young
8 Exhibition Street
Melbourne VIC 3000 Australia
GPO Box 67 Melbourne VIC 3001

Tel: +61 3 9288 8000
Fax: +61 3 8650 7777
ey.com/au

Building a better working world

The Parliamentary Officer
Select Committee on Artificial Intelligence
GPO Box 572
ADELAIDE SA 5001

18 August 2023

By email: scai@parliament.sa.gov.au

SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE

We welcome the opportunity to respond to the Terms of Reference issued by the Select Committee on Artificial Intelligence on 11 July 2023.

Technologies underpinned by and integrated with Artificial Intelligence (AI) have undergone rapid development in recent years and have the potential to revolutionise productivity and democratise a wide range of important capabilities. Businesses and governments are poised to unlock this value. It is critical to position Australia at the forefront of this opportunity while remaining vigilant about potential harms.

The time for establishing effective state and federal frameworks for ethical AI use is now. Robust governance based on ethical principles can rise to the challenge of rapid change, and position Australia as a leading digital nation by 2030.

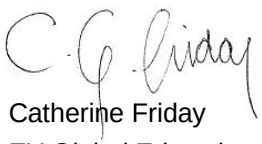
Our responses are based on our global experience partnering with government and industry in addressing the challenges and opportunities of AI and other similarly transformative technologies. They are not based on any specific scope of work undertaken by EY in Australia or elsewhere.

EY teams recently submitted a response to a discussion paper issued by the Commonwealth Department of Industry, Science and Resources (DISR). Our observations and recommendations are consistent across these submissions.

Any policy response in Australia should consider whether initiatives are best undertaken at the state or federal level. We have set out initiatives that may be suitable at the state level, avoiding measures that we believe would be best considered by the Commonwealth. Where initiatives could potentially be undertaken at either level of government, we have included them in our submission but have not made a recommendation as to which may be preferable.

The numbering in our submission reflects the terms of reference. We have responded to questions 1, 3, and 4 only.

Kind regards



Catherine Friday
EY Global Education Leader and EY Oceania Managing Partner,
Government and Health Sciences

Notice

EY teams have prepared this document based on research and surveys generally undertaken or information obtained from public sources. We make no representations as to the appropriateness, accuracy or completeness of the document for any reader's purposes. No reliance may be placed upon the Report or any of its contents by any party (Recipient). Any Recipient receiving a copy of the document must make and rely on their own enquiries in relation to the issues to which the document relates, the contents of the Report and all matters arising from or relating to or in any way connected with the document or its contents. It has been provided to Recipient for information purpose only.

EY teams disclaim all responsibility to the Recipient for any loss or liability that the Recipient may suffer or incur arising from or relating to or in any way connected with the contents of the document, the provi- sion of the document to third parties or the reliance upon the document by the Recipient. No claim or de- mand or any actions or proceedings may be brought against the EY organization arising from or connec- ted with the contents of the document or the provision of the document to the Recipient. The EY organization will be released and forever discharged from any such claims, demands, actions or proceedings.

In preparing this document EY teams have considered and relied upon information from a range of sources believed to be reliable and accurate. We have not been informed that any information obtained from variety of sources, was false or that any material information has been withheld from us. Neither EY teams nor any EY member firms or employee thereof undertakes responsibility in any way whatsoever to any person in respect of errors in this document arising from incorrect information provided to EY. We do not imply and it should not be construed that it has verified any of the information that it obtained from variety of sources.

Liability is limited by a scheme approved under Professional Standards Legislation.

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

Although AI has been successfully implemented in a range of use cases, it has most prominently served in specific domains (search, chatbots, image analysis, mapping, etc.) and received limited public attention until recently. The arrival of Generative AI offers the prospect of broader and more rapid adoption, both because of the inherent expansion in capabilities and also the scope for it to act as a "wrapper" to more specialised AI technologies, thereby increasing their accessibility.

South Australia has an excellent foundation to develop a competitive advantage in AI and Machine Learning. South Australia is home to the Australian Institute for Machine Learning (AIML), one of the first of its kind in Australia, with 160 researchers. AIML conducts globally competitive research and development in AI, machine learning, computer vision and deep learning.

More than 1,500 people from over 150 businesses work in Lot Fourteen, Adelaide's innovation district, including Google Cloud, Amazon Web Services, Microsoft Azure and MIT.[1] There are also regular sessions on AI and ML with start-ups speaking about their current projects and challenges.

Lot Fourteen is supported by the Government of South Australia and the Australian Government, with a combined investment of $757 million as a focus of the Adelaide City Deal. Capital and operational expenditures in Lot Fourteen are projected to generate $3.5 billion in economic activity for South Australia by 2028.[2] Lot Fourteen is considered by the Premier of South Australia, Peter Malinauskas, as a cornerstone of the innovation ecosystem in South Australia delivering economic, social and cultural prosperity for the State.

A recent report by the Australian Council of Learned Academies stated that, "given the speed of innovation, quantum of investment and lack of technical information, it is almost impossible to accurately forecast opportunities over the next decade."[3] There are significant opportunities across a range of sectors, and it is only possible to give a sense of them with example use cases, as set out in the following table.

Industry	Example AI Use Cases
Health	▸ Improve patient care through medical image analysis and data consolidation. ▸ Personalise treatment plans with AI-driven analysis of patient histories and genetic data. ▸ Aid in drug discovery and medical treatments.
Engineering	▸ Enhance design efficiency and optimisation. ▸ Predictive maintenance in manufacturing.
Creative industries	▸ Content recommendation and personalisation. ▸ AI-driven film and video editing.
Education	▸ Integrate advanced learning models in classroom activities. ▸ Personalised learning experiences in universities.

1 Lot Fourteen (link).
2 Lot Fourteen, Strategic Plan 2022 – 2026 (link).
3 Bell, Burgess, Thomas, Sadiq *Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models* (MFMs), 2023, (link).

Industry	Example AI Use Cases
Social services	‣ Analyse and predict societal needs. ‣ Optimise distribution of social welfare.
Finance	‣ Predict stock market trends. ‣ Fraud detection in banking.
Business	‣ AI for supply chain optimisation. ‣ Personalise e-commerce experiences. ‣ Enhance experiences with chatbots and virtual assistants.
Mining and resources	‣ Predictive maintenance of mining equipment. ‣ Optimisation of resource identification and extraction.
Agriculture	‣ Precision agriculture and crop disease prediction. ‣ AI-driven drones for crop monitoring.
Defence and manufacturing	‣ AI in defence systems for threat detection. ‣ Quality control in manufacturing.
Renewable energy	‣ Optimise renewable energy storage and distribution. ‣ Predict energy demand.
Tourism	‣ Personalise travel experiences. ‣ Predict tourism trends and marketing.
Food and beverage processing	‣ AI for quality control in food processing. ‣ Optimise storage and distribution.
IT	‣ AI for cybersecurity and threat detection. ‣ Tools for software development and testing.
Aerospace and Aviation	‣ Flight optimisation and predictive aircraft maintenance.

Many important sectors of the South Australian economy are poised to benefit, including mining and resources, agriculture, defence and manufacturing, renewable energy, tourism, education and research, health and biotechnology, food and beverage processing, and information technology.

More generally, Generative AI will allow rapid access to wider idea generation, automated document drafting and process completion, and advanced quantitative analysis across the whole of the public and private sector.

EY's regular survey of 1,200 CEOs of large global companies, the CEO Outlook Pulse, found that CEOs recognise its potential to drive productivity and positive outcomes for all stakeholders. Two-thirds (65%) agree or somewhat agree that AI is a force for good – driving business efficiency and therefore creating positive outcomes for society, such as innovations in health care treatments.

At the same time, the transformative impact of AI is likely to be a source of considerable disruption. AI is likely to facilitate certain kinds of criminal behaviour, as set out in our response to question 3 from the Terms of Reference. Its widespread adoption will likely create challenges to privacy and data security and require new rules to ensure that it is being used ethically and fairly, as discussed in our response to question 4.

A further challenge is the likely impact on the labour market. A recent paper by OpenAI, OpenResearch and the University of Pennsylvania listed a wide range of occupations, many currently well paid, that will be exposed to AI, including mathematicians, tax preparers, financial quantitative analysts, writers and

[4] EY, *If AI holds the answers, are CEOs asking the right strategic questions? EY CEO Outlook Pulse Survey,* July 2023, page 2 (link).

authors, web and digital interface designers, accountants and auditors, news analysts and journalists, legal secretaries and administrative assistants, clinical data managers and climate change policy analysts.[5] On the positive side, two-thirds of global CEOs are confident that the impact of AI replacing humans in the workforce will be counterbalanced by the new roles and career opportunities that the technology will create.[6] That does not mean that the transition will be painless for the people concerned, or for wider society. Governments will need to consider how they may play a role in shaping and managing the transition by, e.g., providing training and support as roles and responsibilities evolve.

5 Eloundou, Manning, Pamela Mishkin and Rock, *GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models*, March 2023, page 16 (link).

6 EY, note 3.

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

Although we believe AI will mostly bring economic and social benefits, it has the potential to increase access to tools and resources to commit crimes at greater pace and scale than previously. For example, making a deepfake video was previously a relatively time-consuming process that required special skills. AI can:

- Make the basic software technology more available by allowing users to interact via prompts, avoiding the need to master complex interfaces and parameters.
- Assist in scaling up activity by managing the batch processing of images and automating account generation and activity to:
  - Automate distribution
  - Facilitate anonymity, and
  - Boost reach by simulating genuine engagement.
- Greatly increase the speed at which this behaviour occurs.

Accordingly, the deepfaking of documents, still images, video and audio is likely to be greatly facilitated by AI, for the purposes of targeting individuals for bullying and/or embarrassment, fraud or influencing public opinion. Interactive deepfakes are also foreseeable.

Other areas where AI may have a similar negative impact include:

- Increasing the availability of easy-to-use tools and resources for unauthorised access to digital infrastructure, data and information. The automation of these tools could also greatly increase the volume and speed of both malicious attacks (noting that the current average time for detection of a manual cybersecurity breach is in the order of 90 days) and unintended data losses.
- Increasing the volumes of high-quality, personalised spam that is designed to evade detection (e.g., robocalls and personalised emails based on detailed profiling).
- Increasing the availability of information and planning capabilities that are dangerous to the public and previously difficult to obtain (e.g., information on the manufacture of certain kinds of weapons).
- Increasing access to information and resources for innovating new forms of damaging behaviour (e.g., the development of new drugs that fall outside of existing prohibitions).
- Increasing the availability of information and planning capabilities that may be legal in isolation, but that can nonetheless be applied to reducing the enforceability of criminal law (e.g., establishing shell companies, facilitating money transfers, conducting business offshore, encrypting information).

- Increasing the difficulty of attributing responsibility for offences, most notably through the creation of black-box AIs that may be able to run without human supervision for an extended period.

Conceptually, much of this activity is already controlled by existing laws and regulations, including privacy laws, cyber and data protection, anti-discrimination, tort, criminal law, deceptive practices, product liability, and so on.

There could be substantial challenges at a practical level, however, as the regulatory system implicitly assumes some limits around the volume of activity to be controlled, the speed at which offences occur (and new offensive behaviours are created) and the required level of sophistication in the methods used to identify and prosecute crime.

Governments will need to consider carefully how to address these challenges. It is not feasible within the scope of this submission to make specific recommendations about what changes to legal frameworks may be required. A robust response could include:

- Actively reviewing legislation to ensure that offences are appropriately defined and that punishments are proportionate to the harms in an AI context.

- Increasing investment in the detection of offences through technology (including using AI) to increase the speed and scale of enforcement capabilities (while maintaining appropriate controls over its use by, e.g., requiring human supervision over all decision-making). The balance of rights will need to be resolved, and it is instructive in this context that the Australian Human Rights Commissioner has recommended a moratorium on the use of facial recognition and other biometric technology for law enforcement, pending the development of stronger, clearer and more targeted human rights protections. (Most uses of biometric identification systems for law enforcement will also be banned or highly regulated in the EU under the proposed EU AI Act.)

- Potentially, considering making the use of AI an aggravating element in sentencing.

· In respect of the suppliers of AI services, requiring the inclusion of "content guardrails", mechanisms for user feedback or guidelines for "red team" testing of AI products and services. Although this is likely to assist, the increasing distribution of open source / uncontrolled models means this should not be regarded as a panacea.

There is a clear risk that the use of AI will lead to an arms race between governments and offenders. Unfortunately, the incentives for both sides to adopt AI may make this inevitable, and government will need to respond appropriately to ensure that its laws and enforcement tools remain relevant.

We recommend that the government continue to undertake detailed consideration and consultation, ideally before significant harms emerge.

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

AI has created unique and unprecedented challenges and opportunities. Whilst AI technology facilitates the processing of enormous amounts of data at rapid speed, and has accelerated analytical ability, such computational power has the potential to drastically magnify potential privacy harms. The increased use of AI has challenged the traditional notion that the individual maintains a high degree of control over their personal information and raises significant concern about how privacy principles of collection, purpose and use are honoured by organisations and government.

AI systems have largely developed using models that learn, adapt, and predict without providing explanations or transparency. While privacy is first and foremost a legal obligation, considering privacy as a foundational ethical element in designing AI provides scope for organisations and governments to both improve existing data management processes and provide greater visibility of AI development and use.

Increased education and awareness will empower individuals to exercise informed consent to privacy and collection notices, including any secondary use of their data (e.g., to train AI models), and remind agencies and organisations of their privacy obligations.

Consideration could be given to requiring further controls on the acquisition and use of certain kinds of information, such as biometric data, facial recognition data, publicly available text, and the collation of any data into formats that may be usable for social scoring-type analysis by the public or private sector.

Regulatory frameworks across Australia should be strengthened, both to address these challenges and to remove inconsistencies. The Commonwealth Attorney-General's Report on the Privacy Act 1988 (Cth) is indicative of the future direction of privacy policy in Australia. The proposed requirement to act fairly and reasonably when collecting, using and disclosing personal information (Proposal 12) would apply readily to AI in respect of both model training and the use of data in the provision of services. [7] Consideration should also be given to the intersection and compliance with other frameworks and obligations, such as the Consumer Data Right (CDR) in the management of personal data, noting possible changes to a Data Holder or Data Receiver as a result of using AI.

Data Security

The ability of AI to grow the availability of high-quality and innovative tools for unauthorised access, manipulation and destruction of networks, data and information is likely to increase concerns at the intersection of AI, cyber security and privacy, particularly as it may also increase the value of data that may be stolen. The manipulation of data also has the potential to reduce the value of data (by reducing its reliability) or inappropriately inflate its value, resulting in market instability and/or distrust.

---

[7] Attorney-General's Department, *Privacy Act Review Report 2022*, pages 8 and 9 (link).

These concerns intersect with other trends that increase the overall risks, including huge and continuing increases in the volumes of valuable data, the transition to cloud computing, and the growing reliance on a diverse ecosystem of services by the private and public sector.

AI systems themselves already represent attractive targets, noting the complexity of the models and the potential to introduce malicious changes that may be difficult to detect. 'Malicious AI', presented as being legitimately designed and developed, has already been used to secretly embed controls and content into digital infrastructure by criminal organisations and nation states.

Academic and policy researchers are also investing time into the intersection between cyber security, IoT, space tech, AI and quantum technologies as the world starts to prepare for a post quantum computing era.8 While much public discourse on this intersection is focusing on agricultural and medical use cases, there is a growing focus across the defence,9 financial services, industrial manufacturing and education sectors.

Given these concerns, it is imperative that policy and programs around AI take these factors into consideration. The public sector and strategically significant businesses in the private sector will need to consider their investments in cyber security, and governments should consider updating their obligations to do so. They will also need to consider how to define standards and practices on an industry basis to manage possible exposures from the use of third-party services.

The investments made by the South Australian government in its own planning around cyber security capabilities for government services, together with policy attention and funding to encourage innovation and the growth of new industries, has established the knowledge infrastructure to ensure that security considerations in the development and use of AI are embedded into practice.

Ethical use of AI

The use of AI has raised ethical concerns due to a combination of its potential power, their complexity, and recent Australian experience.[10] Areas most relevant to ethical consideration include:

- The potential need to review datasets to mitigate inaccuracies and historical bias.
- The use of AI in high-value / high-risk areas, including legal analysis, personal financial management (e.g., debt management), social welfare eligibility and decision-making around access to resources (e.g., school or university selection)
- The use of AI in decision-making generally, as opposed to using it merely for analysis, particularly if the AI system is not transparent in its processes or doesn't provide rationales for its decisions

Bias and inaccuracy may be serious without being readily observable, except over time and with a sufficient sample size. Even where differences are detected, mere differences may not be indicative of bias and could require detailed and resource-intensive technical investigation.

---

8 EY Australia, *Beyond the Hype: A Critical Look at Quantum Computing' Potential for Business and Society in Asia-Pacific* (link).
9 EY Australia, *Quantum Power Play: Navigating the New Landscape of Cybersecurity and Defence* (link).
10 *Report of the Royal Commission into the Robodebt Scheme*, page 472 (link).

Concerns are likely to apply mostly to government agencies and strategically significant businesses. Government in particular should carefully consider its responsibilities given its direct accountability to citizens and its combined role as legislator, regulator and actor within the regulatory system.

A range of measures could be considered to support the development and implementation of ethical AI:

Within government

- Adopting ethical principles and frameworks to guide agencies in AI implementation, addressing transparency, the pace of adoption, and establishing rights to complain and obtain an effective remedy. The NSW Government AI Ethics Principles and AI Assurance Framework may provide a suitable basis for developing a framework for South Australia. Government action in this area can serve as a model for the private sector.

- Establishing a task group within a department or agency to advise on AI matters across Government.

- Addressing Government's training needs to ensure that they are informed and capable buyers and users of AI services. We note that, during this open consultation period, the Digital Transformation Agency issued *Interim Guidance for agencies on government use of generative AI platforms.* This Commonwealth model may be applicable to South Australia.

- Creating roles within the South Australian public sector at a senior level to oversee AI initiatives with a focus on safety and responsibility.

Market-wide initiatives (applying to the public and private sectors)

- Requiring government agencies and strategically significant businesses to provide a technical summary of their AI systems, including information about the underlying algorithms, training processes, and measures taken to ensure fairness and avoid bias.

- Requiring checks for potential bias and fairness in AI decision-making processes, using a mix of auditing and the implementation of fairness metrics. This may lead to a broader focus on the ability of AI models to transparently explain their decision-making, in order to ensure that potential bias is capable of being evaluated.

- Placing controls on the development of foundation AI models. The rapid progress in AI's capabilities has the potential to become an area of significant public concern. Although much of the advanced work is undertaken overseas, consideration could be given to requiring the submission of applications to undertake model development meeting certain thresholds, in much the same way as applies to research in other regulated industries, such as biotechnology and nuclear energy.

Non-regulatory initiatives

- Funding of collaborative research, encouraging the sharing of resources, and continuing to support the development of standards and best practices across government, academia and industry.

- Supporting training opportunities across the range of needed technical skills, and encouraging AI's responsible use in the university sector. Education will be critical to ensuring that South Australia has the skills needed to participate in AI and to build public trust, and can also play a vital role in improving access to skilled work in the sector for disadvantaged groups.
- Supporting programs to educate the public about AI by raising awareness and addressing myths. Information packages could also be developed to support better, more accurate media coverage of AI myths.
- Establishing an independent panel of recognised experts to evaluate significant / new generative AI solutions that are to be commercialised in South Australia (with the ability to recommend sandboxing / other testing procedures before widespread implementation)

Coordinating action across privacy, data security and ethical use of AI

There are some technical and policy overlaps across these three areas. Consideration should be given to establishing an integrated monitoring and reporting regime involving:

- Requiring government agencies and strategically significant businesses to undergo regular independent audits to verify compliance with AI ethics guidelines, data handling practices, algorithmic fairness, system security and privacy protections.
- Requiring higher-risk AI systems to be subject to regular testing for robustness against adversarial attacks and penetration testing to evaluate system security.

At the federal level, our recent submission to the DISR consultation on safe and responsible AI recommends:

- Establishing a senior governmental presence in the sector to provide appropriate leadership across the Commonwealth, states and Territories, such as a committee of the National Cabinet
- Establishing a central regulatory body to oversee the sector, issue binding market guidance, monitor compliance and undertake necessary enforcement actions.
- Establishing certification bodies to independently assess and validate AI systems against both regulatory and voluntary standards.

Certifications could be along the lines of the CertifAIEd issued by The Institute of Electrical and Electronics Engineers (IEEE).[11] Work to set Australian standards should be undertaken alongside participation in the continued development of international AI standards, such as ISO/IEC JTC1 SC42.

[11] IEEE CertifAIEd™, The Mark of AI Ethics (IEEE CertifAIEd).

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 000466-24Gbl

ED None