Consultation re Artificial Intelligence (AI)

Department of Industry, Science and Resources

Submission by Aulich & Co Pty Ltd

Chair: Terry Aulich

10 July 2023

Contents

1. Synopsis
2. About Aulich & Co Pty Ltd
3. The themes of this submission
4. Four key principles to deal with AI.
5. Education, ethics and law and AI
6. Some suggested changes in legislation
7. Glossary of terms
8. Contacts

1

1. **Synopsis**

This submission concentrates on two feedback questions raised in the Department of Industry’s consultation paper, namely:

1. the need for any further governance and regulatory requirements to deal with AI and
2. the need to increase trust in new technologies including AI.

This submission sets out the reasons why trust is critical: trust in the *ethics* of government and the private sector and trust in the *competence* of both sectors to deliver new technologies like AI.

The submission also outlines four key principles that must underpin any legislation or regulatory changes, namely:

1. Contestability by citizens; that is, the right to question decisions made about them.
2. The right of ready redress and possible compensation.
3. Truth and accuracy in business and legal operations.
4. Human accountability for and controls over generative artificial intelligence.

The submission also gives some real life or future examples of AI use and development; pointing to some areas where additional legislation or regulation may be required.

1. **About Aulich & Co**

Aulich & Co, established in 1993, is a strategic advisor in matters relating to privacy and public opinion assessment, including polling.

The Hon Terry Aulich was a pioneer in privacy legislation commencing with his chairmanship of the Joint Select Committee examining a national identification system in 1987 (The Australia Card). His committee recommended a number of key measures relating to fraud and privacy. Amongst those recommendations were the establishment of a Privacy Commissioner and privacy legislation and anti-fraud legislation such as the Tax File Number system, and banking requirements such as the 100 points ID system and money transfer controls. The then Government accepted all recommendations and legislated the provisions.

Since leaving Parliament Terry Aulich and his staff have conducted privacy audits or privacy impact assessments for a number of private and public sector clients in NZ and Australia. These include the NZ Department of Internal Affairs, the Commonwealth Department of Health, the Family Court of Australia, the Child Support Agency, the Commonwealth Rehabilitation Service and Clubs NSW.

Terry is also Head of the international Biometrics Institute’s Privacy Experts Group and for twelve years headed the privacy committee for the Australian Data and Insights Association which represents pollsters and researchers. He still acts as a consultant to the latter organisation which has the only Privacy Code accepted as part of Australia’s Privacy Act. He has also worked with other international groups such as INTERPOL and the UN’s Counter-terrorism Executive Directorate.

Terry speaks at and chairs many international forums on privacy, ethics and two of his three novels, *Clapperland* and *Sète*, deal with the ways new technologies such as AI and biometrics have transformed politics and religion.

2

Terry’s commentary in this submission is in a private capacity.

1. **The Themes of this Paper**

As Australia moves inexorably towards full online delivery of services and transactions there are two key requirements that must be met if that transition is to occur successfully. Those requirements are based on trust.

The first is public trust in the *competence* of service providers to collect personal data and deliver online services safely and the second is trust in the *ethics* of governments when they interact with their citizens.

This paper is an attempt to look behind those two requirements, noting that competence and ethical behaviour, have sometimes tragically been absent, even in a society as democratically stable as Australia.

If Australian governments and service providers lose that public trust, the result may be that our society will lose a golden opportunity to deliver the benefits that can be derived from the use of AI, including medical research, forensic science, travel, immigration and crime prevention and detection.

This submission also emphasises the fact that the information technology sector is truly global in its reach and impact, meaning that individual countries, businesses, and even individual citizens cannot rely solely on nationally isolated solutions to cyber insecurity, fraud, misuse, or privacy invasion. Therefore, it is strongly advisable for Australia to monitor and connect with international institutions like the International Standards Organisation, the Biometrics Institute, the European Union, various US jurisdictions and other bodies that have been working on technology and privacy issues over many years.

The rapid advent of artificial intelligence (AI) and related automated systems like biometrics will provide both a challenge and a benefit and the Australian government must be congratulated on beginning a formal comprehensive policy discussion about those challenges and benefits. Of particular note are other planned initiatives such as the National Anti-Scams Centre and the long overdue review of the Privacy Act.

In response, the following section looks briefly at four key principles that must underpin Australia’s framework for dealing with AI in this country, all of them principles that will help to protect and benefit our citizens and build a stable civil society.

1. **Four Key Principles to Deal With AI and Related Technologies.**

This paper identifies four key trust principles that must be written into appropriate law, regulation, government contracts and tender specifications to ensure that the move to AI and related automated machine learning is of benefit to and not oppressive of citizen rights. Those four principles are:

1. contestability
2. right of ready redress and possible compensation
3. truth and accuracy in business and legal operations
4. human accountability and controls over generative artificial intelligence

3

4.1 Contestability

The first principle is contestability, the right of citizens to easily question decisions made about them by government and private systems, especially when those decisions were based on erroneous calculations or unethical manipulation. This principle of contestability is an essential component of civil society, part of the social contract that holds democracies together.

But, the principle of contestability has been eroded over the last decade or so.

One milestone example is the case of Robodebt, where the Commonwealth Government failed this ethical and contestability test. Using automated decision making (related to AI), the previous Commonwealth Government placed the burden of proof on those they were accusing of suspected welfare fraud or providing misleading returns. Citizens, thus accused, were unable to contest decisions made by the system or at least had many obstacles put in their way. Worst still, the system made assumptions about guilt even though a significant amount of the debt claims were in serious error; a fact which was proved when, after major public and legal challenges and a Royal Commission, the Commonwealth was forced to pay compensation of $1.8 billion to the 443,000 aggrieved, affected citizens.

4.2 Right of Ready Redress and Possible Compensation

One of the tragic features of Robodebt saga was the extreme difficulty, indeed, impossibility in some cases, for aggrieved and /or persecuted welfare recipients to seek explanations or redress either from appropriately qualified public servants or the outsourced agents of authorities such as debt collectors. Even when mistakes had been made and /or the whole Robodebt system was held to be illegal, the welfare recipients faced many obstacles in seeking redress, compensation or even an acknowledgement that the relevant departments had made a mistake. The Royal Commission was also told that many staff were ignored or threatened with sanctions if they queried either the legality, ethics, or the effectiveness of the system.

The lesson from the Robodebt scandal must be learned when automated systems are planned for the future, covering all facets of the projects from their legality and fairness through to the need to acknowledge and redress mistakes or wrongdoing.

4.3 Truth and Accuracy in Business and Legal Operations

The third key principle is the need for truth and accuracy in business and legal operations. Although goods and products are covered in some ways by consumer law, the provision of services is a virtual orphan, especially when we deal with AI and any kind of automated decision making that affects citizens and even those organisations that purchase AI or AI related systems. Possibly through trade practices legislation, there will need to be special provisions to protect end-users and system purchasers from misleading claims being made by vendors of AI systems.

In addition, as in many areas related to AI, purchasers or clients must have the regulated right to know the algorithms that enable AI systems that affect them.

In courts of law we are already seeing the damaging effects of inadequate understanding or misuse of automated or “expert” opinions in evidentiary processes such as court reliance on DNA samples and interpretation.

4

Similarly, deep fakes will not only be a major issue for courts but are already a potentially misleading phenomenon of media and social media campaigns. It is now possible to manipulate photographs

and moving images of individuals and, without proper referral to the context, innocent individuals may suffer significant damage to their reputation or, literally, to their freedom.

The traditional “camera does not lie” evidence will need to be replaced by sceptical expert opinion. There are a number of legal cases which have shown the need for changes in evidentiary rules and improved education of both the public and the judiciary to prevent wrongful convictions and related media defamation. It is also time to make it easier and less costly for individuals to seek redress if they have suffered reputational and other damage from malevolent or incompetent media and legal processes.

4.4 Human Accountability and Controls Over Generative Artificial Intelligence

Traditionally, innovative new technologies such as super computers and social media targeting are usually in advance of the legislation or even standards that should be guiding them although organisations such as the Biometrics Institute and the International Standards Organisation assist best practice by producing guidelines and standards. Some governments and geopolitical blocs such as the European Union have written law or legally binding directives to cover human rights and privacy but usually such action is outpaced by the rate of change and innovation driven by commercial or other competition.

Generative artificial intelligence is an even greater challenge since it has the potential to make decisions without human prompting or ultimate control. This concern has been raised not by Luddites but by technology leaders (over 1000 signed a letter of concern, including Elon Musk and the project personnel from ChatGPT). Tellingly, the leading expert and head of the Google AI project, Geoffrey Hinton, has resigned, stating that he regrets being responsible for creating the algorithms that allow machines to learn and control their own development.

It is not too late to heed these expert warnings even though both private investors and governments, especially authoritarian governments, will attempt to covertly or openly engage in a technology arms race to seek competitive advantage. To justify or cover their planning they may well quote the obvious benefits that AI has brought to medicine, forensic analysis, DNA research, security and other research and operations that will benefit from AI.

Although pauses or bans have generally worked well with nuclear treaties, biological warfare agreements and ethical controls over human cloning, the Australian Government will need to ensure that it has the expertise and the will to require openness from technology companies that are developing AI. In particular that openness must apply to the algorithms that drive each AI based system.

This openness must also apply to education and welfare systems, areas where enthusiastic proponents are promoting the cost savings and benefits of AI. Both those sectors have already been primed by the rise of metric and efficiency “experts” who will be only too willing to promote the dubious benefits of handing control to machines without human discussion or intervention.

For those who are concerned that a mandatory pause for the development of AI would place Australia at a disadvantage compared with state or criminal bad actors, consideration should be

5

given to encouraging controlled trusted organisations such as the Australian Signals Directorate and University ethics committees to manage the development of AI within a strict ethical regime.

1. **Some Examples Where Education, Ethics and Law are Required to Deal With AI**

5.1 Example: AI Takes the Human Out of Killing. A Future or Current Scenario?

Autonomous drones use biometric recognition to track and kill human targets, the whole sequence requiring little or no human intervention or ethical overview. Wars like that in Ukraine and other troubled countries are already stimulating not only deadlier and less costly weaponry but are pushing the boundaries generally controlled by human agency and international agreements such as The UN Convention on Human Rights and the Geneva Convention. The ethical issue here needs public discussion and guidelines along the lines of those that arose over alleged SAS murders in the Middle East.

5.2 Example: AI and Propaganda Warfare

AI is already being used to fight war or rebellions at a psychological level. Deep fakes can be used to win world opinion or, especially in autocracies, rally citizens behind a war mongering government, as in Russia.

5.3 Example Three: Cyber Warfare and Infrastructure Targeting

Wars are being fought using both physical and cyber-attacks on enemy critical infrastructure such as dams, hospitals, power stations and traffic and water systems, the use of AI making the breeching of defences much easier. Even worse will be the unregulated use of AI driven cyber-attacks by bad actors such as terrorists or the criminal fraternity.

5.4 Example: AI and Politics

As elections become more influenced by social media which tends to create rather than ameliorate differences, the use of deep fakes will be increasingly a problem for social discourse and respect for the compromises that underpin functioning democracies. The next Presidential elections in the US will be a test of how AI generated deep fakes will be used to put words into the mouths of opponents with such sophistication that the average voter and journalist will be unable to discern the fakes. Australia election officials will need to observe this phenomenon and prepare to deal with the use of deep fakes in politics and the media.

5.5 Example: AI and Education

In education, there has been a steady growth in metrics designed to measure student and school performance for purposes related to comparative league tables and university entrance selection. Already AI is challenging the purpose and usefulness of those performance metrics. When an AI chat bot can write competent exam or essay papers, the whole system of competitive measurement will be challenged and will require new paradigms of education or, in some cases, even a return to more established pedagogies; it may simply require a greater emphasis on teacher-student face to face relationships and assessments.

5.6 Example: AI and Journalism

6

In journalism, the use of AI generated stories based on internet trawling will have significant impacts as traditional mainstream media struggle to remain viable in the face of social media and online information. For example, automated bots are likely to draw on information and news from free sources on the internet; a challenge to the journalist profession and the viability of media that rely on paywalls to maintain revenues. After all, the business case for using AI generated searches and stories is precisely to cut costs; experienced journalists and payment for information feeds being two such costs.

5.7 Example: Government Accountability for Data Breaches

Government accountability will require prompt open communication with the public. For example, after one such government wide data breach the relevant State Minister described, one week later, a major 140,000 business and personal data breach simply as “a third party file transfer problem” when, in fact, best practice would have required an early significant warning to all citizens given that the Russian hackers intended to publicly release many of the personal details they had stolen. This type of data breach can be expected to occur more frequently which once again raises the critical concept outlined in section 3 of this paper, namely the need for governments and other service providers to ensure public trust in their competence and ethics.

5.8 Example: Interrelationship of Government and Private Sector Responsibilities

Melding of Government and Private Sector IT Services has been a phenomenon of recent decades, especially as privatisation of public infrastructure has been a method used by governments to improve their nominal budget bottom lines. The critical issue in this space is to recognise that data collection and management infrastructure is now more often than not shared between governments and the private sector. For many years that shared responsibility was not recognised in relevant legislation such as the Privacy Act where the private sector and governmental responsibilities were governed by separate parts of the Act. Even after the consolidation of Privacy Principles between the two sectors, small business continues to be exempted from the provisions of the Act.

This dichotomy has practical and often deleterious consequences as shown by any analysis of the most significant data breaches of the last three years. The list of data breach failures includes universities, telecommunication companies, health insurers and providers, parliaments, ambulance services and personal loans and financial services organisations. The failures differed in their nature but many constituted damaging breaches of sensitive financial, medical, and other personal data, much of it retained for periods that were either too long or stored negligently or re-acted to inadequately.

1. **Some Suggested Changes in Legislation**

Following are some key amendments to legislation which may help provide a framework to meet the principles outlined in Section 4 of this submission, that is:

1. contestability
2. right of ready redress and possible compensation
3. truth and accuracy in business.
4. human accountability and controls over generative artificial intelligence

7

6.1 Changes to consumer and competition policy legislation.

As citizens are encouraged or forced into online activities for many aspects of their lives, the requirement to protect their involvement will require at least the following changes:

* To ensure that consumers are able to contest decisions which unfairly damage their private lives, especially their financial situations.
* To ensure that consumers and purchasers of services and goods are able to seek redress and compensation for breaches of their privacy, especially financial privacy.
* To ensure that consumers, faced with misleading, untruthful, or inaccurate descriptions from suppliers can seek ready redress and compensation.

6.2 Changes to Privacy, Defamation and Consumer Protection Law

Privacy is still a critical area where the protection of reputation is fundamental. The following changes should be examined to:

* introduce a law of privacy torts to allow either the Information Commissioner and individuals to sue or take action for egregious and damaging privacy breaches.
* include all small businesses in all privacy legislation (since many small business will have ready access to AI driven data collection and use systems)
* ensure that, where media have knowingly misrepresented individuals using AI generated fakes equivalent to photo-shopping, citizens are able to seek ready redress and instant apologies of equal prominence in subsequent editions. This right should be provided through both defamation, consumer, and privacy law.
* ensure that social media organisations are required to provide a legal right for correction, deletion, and recompense where a citizen’s personal privacy and reputation have been severely damaged.

6.3 Changes to the Crimes Act and Related Crime Legislation and Evidentiary Provisions

This area is likely to be tested significantly be AI generated misinformation and reputational damage to individuals and members of political parties. So, consideration should be given to:

* include a proscription of fraudulent and misleading misrepresentation through the misuse of deep fakes aimed at damaging political opposition, individual reputations, business competitors or any other organisation.
* insist that evidence given in court about AI driven data such as DNA or images is subject to *independent* court based expert analysis (as opposed to the use of “expert” evidence provided by one or other adversaries in a court action)

1. **Glossary of Terms**

Note: There is no definitive agreement about the meaning of AI but the International Standards Organisation does provide a slightly ponderous version. Below is a modified version suitable to the main themes of this paper.

Chat-bot: an automated system to write online information, including opinions.

8

Artificial Intelligence (AI): A system with various levels of automation which can generate predictions with minimal or no explicit programming by humans. Applications of AI can include multi-modal generation of images, speech, text.

Generative AI: Means automated decision making at a higher level of automated activity where there is capacity of machine systems to learn and generate predictions and make decisions.

1. **Contact details.**

Hon Terry Aulich

Chair Aulich & Co

9 Devonshire Square West Hobart TAS 7000

[www.aulich.co](http://www.aulich.co)

aulichterry8@gmail.com