Positioning Australia as a Leader in Digital Economy Regulation

Issues Paper on Automated Decision Making and AI Regulation

University of Melbourne submission

Department of Prime Minister and Cabinet

April 2022

1. Overview

The University of Melbourne welcomes the opportunity to respond to the Department of Prime Minister and Cabinet's Issues Paper, *Automated Decision Making and AI Regulation* (the Issues Paper).

New Artificial Intelligence (AI) and Automated Decision Making (ADM) technologies have the potential to deliver major benefits to Australia's society and economy. Realising these benefits will depend upon a regulatory framework that allows for innovation while managing the considerable risks associated with the development and the use of new AI/ADM technologies. We commend the Government for adopting a consultative approach to the design of AI/ADM regulations.

About this consultation

The Digital Technology Taskforce was established in 2019 and is overseeing the implementation of Australian's Digital Economy Strategy, released in 2021. The Issues Paper addresses the role of AI (Artificial Intelligence) and ADM (Automated Decision Making) technologies in Australia's social and economic future, and identifies the aim for Australia to become a top 10 digital economy and society by 2030. It emphasises the importance of flexible legislation, placing great importance on ensuring "policies, regulation and standards are fit for purpose" and "agile as technology develops." By changing legislation when necessary, in order to promote the maximum growth and adoption of new technologies, the Government hopes to position Australia as a leader in digital economy regulation. The Digital Technology Taskforce also considers the potential risks of these technologies and acknowledges the need for the development of unbiased and ethical AI and ADM. Referencing the Artificial Intelligence Ethics Framework, the OECD AI Principles and other AI principle frameworks, the paper foregrounds the importance of concepts such fairness, transparency, reviewability (contestability) and accountability.

About this submission

This submission was prepared by the University of Melbourne's Centre for Artificial Intelligence and Digital Ethics (CAIDE). The Centre facilitates cross-disciplinary research, teaching and leadership, bringing together expertise from the Melbourne Law School, the Melbourne School of Engineering, the Faculty of Engineering and Information Technology, the Faculty of Arts and the Faculty of Science at the University of Melbourne.

The submission addresses the key regulatory challenges associated with emerging AI/ADM technologies, and provides an outline of the different approaches to responding to these challenges (the use of existing Law, a focus on data harms and privacy regulation, and the development of law and regulation specific to AI). We also discuss the potential for using Government procurement to drive the ethical development of AI/ADM, and the importance of Australia's skills system in supporting upskilling of regulators. The submission also offers responses to each of the ten consultation questions included in the Issues Paper.

The University would welcome the opportunity to continue working with the Government on the development of regulations relevant to AI/ADM.

For further information, or to discuss the submission, Professor Jeannie Paterson, Centre for AI and Digital Ethics Co-Director can be contacted at jeanniep@unimelb.edu.au.

2. Reflections on regulating AI

AI and ADM have the potential to make markets and government deployment of resources more efficient, effective and safe. However, these technologies also raise social and legal challenges in terms of the harms they may occasion, contractual complexity, privacy, data protection, cyber security, the blurring of public/private responsibility, and the risk of amplifying the disadvantage and discrimination already experienced by vulnerable populations.

The focus of the Automated Decision Making and AI Regulation paper is on regulation, namely 'how our regulatory settings and systems can maximise opportunities to enable and better facilitate the responsible use of new technologies' (p 2). There is an ongoing debate in Australia and internationally about how best to regulate AI: what kinds of regulatory systems are needed to facilitate beneficial uses of AI/ADM while providing incentives for those designing and deploying the technologies to do so in a responsible manner.

Our preference is for applying existing law, upskilling regulators, and using targeted regulation, including soft law options, to address specific high-risk concerns about the use of AI/ADM. Additionally, we suggest a focus on procurement by governments and firms, which is critical to ensuring the preconditions to responsible AI. We begin by emphasising the case for regulation.

2.1 Why regulate?

It is sometimes assumed that regulation acts in opposition to innovation and the adoption of technology. The concern is a pertinent in the sense that over-regulation may give rise to duplication, overlap and incoherence.[1] It may also lead to gaps in the regulatory regime and regulatory arbitrage whereby firms design their products to avoid regulation, and use very precise statutory definitions to obtain an unfair advantage over regulated products.

At the same time, the effect of regulation on innovation and markets should not be catastrophised. Properly regulated markets can be innovative, responsible, and trustworthy. In this light, well designed regulation produces better outcomes for all citizens, not merely those driving innovation.

The function of many regulatory regimes is to promote better outcomes for firms and people. Competition and consumer protection law, for example, is premised on creating efficient and fair markets, including by addressing areas of market failure and requiring firms to internalise the costs (or externalities) to society of their harmful conduct.

Indeed, we suggest that there is no benefit in technological innovation that comes at the cost of disproportionate harm to individuals and democratic values. Such an outcome undermines the social license of governments and firms that use AI/ADM. There are also reputational risks that may, in the longer term, harm business and government interests and reduce overall trust in technology. This can result in missed opportunity and harm: the benefits that would have accrued from the technology may fail to materialise due to a lack of caution in the drive to innovate and adopt.

2.2 How to regulate?

Given acceptance of the role of regulation in this context, what then are the possible strategies for regulation of AI/ADM? We suggest they involve choice between relying on existing law, data law, and and new AI focused law.

Existing law

A primary approach to the law and regulation of AI/ADM is to apply pre-existing law. On this view, the

[1] See generally, Australian Law Reform Commission, *Review of the Legislative Framework for Corporations and Financial Services Regulation* (Report No 137, November 2021).

legal response to disputes and harms around the Internet of Things (IoT) should be focused on the human actors' conduct and the outcomes of that conduct. In other words, humans design, implement and govern these systems. The systems in law are like any other tool or process used by individuals, business or government, and the law applicable to these fields should apply. There is much to be said for this approach. It is technologically neutral, and moreover in the past has accommodated new technologies (including email and electronic signatures).

There is much to be said for this approach. Existing law has in the past accommodated new technologies (including email and electronic signatures). Moreover, it relies on specialist regulators with expertise and understanding of the underlying policy imperatives driving the relevant regulatory regimes. On this approach the principles of responsibility would be familiar ones; based in private law, public law, and statutory regimes.

Data harms and privacy regulation?

A second, intermediate approach, to regulating AI/ADM focuses on the use of data that underlies these technologies. Some AI/ADM will rely almost entirely on data which is not personal. However, some AI/ADM do use personal data, and the harms that arise from processing personal data are unique, and go beyond traditional legal concepts of property, rights, and harms. Personal data once collected can be repeatedly repurposed and reused, as well as recombined and re-identified. Data may even be sold to other organisations. Misuse has impacts on privacy, and can lead to more concrete harms including identify theft and discrimination.

Concerns about untrammelled data use and its impact on personal privacy underly the EU General Data Protection Regulation (GDPR), which puts obligations on those who collect and process data as well as giving rights to the subjects of data processing.[2] They also have led to the currently ongoing review and reform of the Australian Privacy Act 1988.

However, while important, data protections can only ever be a partial response to the regulation of AI/ADM. Often they are premised on consent, which is easily obtained, even where individuals have much to lose by misuse. Privacy Law does not address concerns about quality of service and the resilience of devices to cyber attacks.

Moreover, evidence suggests that individuals' attitudes to data sharing vary according to the proposed use. Individuals are more supportive of public interest uses of (deidentified) data for health research, than the use of such data for commercial outcomes. This again supports a risk-based approach to regulation.

Cyber rules

A complementary approach to regulating AI/ADM also focuses on harms, this time harms resulting from cyber breaches. Recently there has been considerable focus on the risks of cyber attacks that arise from the interconnected character of IoT devices, and the potential for hacking, stalking and identity theft. While these issues affect individuals, there is also a concern about the flow on effects to essential infrastructure where networked devices are hacked.

Governments in the US, UK, EU and Australia have been exploring the possibility of specific cyber safety standards for IoT devices.[3] Proposed initiatives range from soft law guidance, mandatory codes,

[2] Council Regulation (EU) 2016/678 of 27 April 2016 on the protection of natural persons with regard to the processing of data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

[3] See the Australian Government Department of Home Affairs *Securing the Internet of Things for Consumers*

prescribed warnings and an extended approach to product safety requirements.[4]

Again, these initiatives are probably justified as a specific response to a unique problem. But it would be desirable from a perspective of coherence to wrap cyber responsibilities into existing sector specific law. This will allow an informed and scaled approach to cyber risk. It would also allow regulatory enforcement strategies to leverage the existing expertise of regulators, without unduly increasing the burden on firms that would arise from contradictory or poorly coordinated regimes.

An AI Law?

A third category of response to regulating AI/ADM focuses on the technology itself. The argument here is that AI is not just another tool or product, but generates its own unique regulatory challenges. These arise from the character of AI as being opaque, adaptive, and to many people incomprehensible.

In the EU, this approach has motivated proposals for an AI Act. The draft EU AI Act uses a risk-based model that premises the regulatory response as proportionate to the risk to safety and human rights posed by any application of AI technology.[5] Different obligations are placed on AI systems that create an unacceptable risk, a high-risk, and a low or minimal risk. It includes *ex ante* compliance procedures for market entry, certification and ongoing monitoring, and reporting for high-risk AI applications, with the overall aim of promoting trustworthy AI or, in other words, AI that is fair, safe, reliable, and accountable.

Most of the focus of the AI Act is on public facing uses of AI, such as the ubiquitous surveillance that may result from smart cities without proper oversight. For example, the use of 'real-time' biometric identification systems in public (including facial recognition). The draft AI Act has been criticised as on the one hand too onerous and on the other as insufficiently nuanced to issues of human rights and consumer protection.

2.3 A risk-based approach

One way through this dilemma of regulatory design is to focus on a risk-based approach to regulation, but without trying to develop an omnibus AI Act.

A risk-based model is already used in areas such as product safety and financial services regulation. Such an approach would consider the risks of harm that regulation is seeking to address (with an emphasis on human rights), and the benefits that may be generated by the relevant technology. It would aim for a proportionate response having regard to these factors.

For example, a starting point might be to apply existing regulatory regimes to new and emerging technologies such as ADM and AI. However, it should be recognised that there may be specific features of AI that generate an increased risk of harm, and which may justify more targeted regulatory responses.

For example, we might be highly concerned about accuracy and less about discrimination in uses of AI in plant agriculture. AI products in this space may be addressed for example by the Australian Consumer Law, and in particular the consumer guarantee regime in part 3-2. However, concerns have

[4] Strengthening Australia's Cyber Security Regulations and Incentives (2021). https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice. See also 'Government Response to the Call for Views on Consumer Connected Product Cyber Security Legislation' (*Department for Digital, Culture, Media & Sport*, April 2021) www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response

[5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206 (April 2022)

been raised about the ability of farmers to access data in new generation machinery, essential to running their farms and to repairing goods.[6] Specific regulation has been proposed and might be justified as a response to the new reliance on data in emerging technologies.

Conversely, human rights issues and concern about discrimination are raised by the use of 'one to many' facial recognition technologies. Robust and strong protections in the form of rights to contestability, human rights assessments, auditing for bias and error, should be considered before such technologies are rolled out (if used at all).

An approach that seeks to articulate the specific elements that an AI/ADM system must possess to meet regulatory standards is likely to quickly go out of date. An alternative is to identify the outcomes or performance expected of the technology. For example, consumer-based products, whether using AI or not, are expected to be safe, durable and fit-for-purpose. Consumer credit must not be unsuitable for the borrower – meaning it must not be likely to cause financial hardship. Under the design and distribution regime in the *Corporations Act*, responsibility is placed on developers of financial products to ensure such products are suitable for the target audience.

Different, more onerous obligations might apply to government decision making. This insight leads us to insights for accountable AI.

2.4 Human rights assessments for government, and high impact decisions

A principles-based approach may be particularly suitable for ADM and AI systems developed or deployed in the public sector. This would be similar to the approach to that found in Human Rights law, which requires that:

a) the system's purpose/aim must be legitimate,

b) the system must be likely to achieve that purpose or further that aim (or is necessary to do so in a stronger formulation), and

c) there is no less intrusive, less-biased, or less rights-infringing alternative to achieve those aims or purpose.

This third of these requirements is important. The introduction of technology for its own sake – treating it as a desirable end rather than a means to an end – is problematic, particularly when public funds have been expended on it and when those who provide the funds (taxpayers) are negatively impacted. The Australian Human Rights Commission (AHRC) recommended such an approach for government decisions impacting individuals and also recommended it be adopted by comparable business decisions. For this sort of approach to flourish, however, there needs to be a high degree of transparency around the use of ADM.

2.5 Regulatory preconditions of accountable AI

Responsible or trustworthy AI requires mechanisms for accountability when processes go wrong and for contestability for those adversely affected by decisions or processes.[7] AI/ADM has unique features that may impede the possibility of these processes working effectively. These technologies tend to be opaque and adaptive, and are often subject to commercial in confidence agreements. For accountable AI, mechanisms for ensuring transparency are crucial, including providing explanations of AI decisions where humans are impacted. Transparency is a key element of most AI ethics frameworks, as noted in the Issues paper. It means clarity in when AI/ADM systems are being used and the kinds of systems

[6] Australian Government Productivity Commission *Right to Repair* (Report No 92, October 2021)

[7] Henrietta Lyons, Dr Eduardo Velloso and Professor Tim Miller, 'Challenging Decisions Made By Algorithm' *Pursuit* (24 Nov 2021) https://pursuit.unimelb.edu.au/articles/challenging-decisions-made-by-algorithm

in place. Explanations do mean providing sufficient clarity around the decision or outcome, such that those affected by and responsible for the decision can understand the factors that led to the result. Sometimes explanations can be better facilitated by using simpler AI models. Like regulation of risk in AI/ADM, what is required from transparency and explainable AI can be scaled. Considerable research in explainable AI is being undertaken at universities, including the University of Melbourne.[8] What is key is to ensure high levels of transparency and good explanations in ADM affecting the fundamental rights and essential services and entitlements (indeed if it is used at all). These mechanisms are not sufficient on their own but should be seen as the preconditions to strong regulatory oversight and accessible mechanisms for contesting adverse decisions.

2.6 Procurement

Proper procurement process standards provide an opportunity for minimising risks. Throughout the process of procurement, mechanisms for oversight and accountability can be undermined. Firms developing technology are reportedly protecting the operational detail and insights from collected data through commercial in confidence clauses in the relevant contracts. With more robust procurement standards, the firms and government departments buying AI/ADM could ensure that the software they are procuring is not only designed to be transparent and to include accountability frameworks, but also that mechanisms are put in place to address risks and issues as they arise.[9]

Additionally, lawyers are a key stakeholder in ensuring ethical AI through the delivery of timely and informed advice on issues of AI, ADM, Cyber Security and the procurement of technologies for business operations both internally and for their clients. Their upskilling in ethical AI, cyber risks and the preconditions for effective oversight and auditing would allow for better compliance and outcomes generally.

2.7 Upskilling Regulators

While there concerns that current regulators lag behind in understanding technological innovation, this is not always the case. The ACCC[10] and ASIC[11] have been very active in responding to issues of technological change in their domains. Nonetheless, if technological experience is found lacking, then regulators should be provided with training and capacity building opportunities. Universities might be utilised for this task. Indeed, the Centre for AI and Digital Ethics already runs general and bespoke masterclasses on 'Demystifying AI Ethics and Regulation'[12].

[8] See https://www.unimelb.edu.au/caide/research/autonomy-and-ai

[9] Bush G, and Paterson J. "Governments as Regulators and Consumers of Ethical AI." *Turkish Policy Quarterly,* March 2022.

[10] See Liam Harding, Jeannie Paterson and Elise Bant, 'ACCC vs Big Tech: Round 10 and Counting' *Pursuit* (online, 24 March 2022) https://pursuit.unimelb.edu.au/articles/accc-vs-big-tech-round-10-and-counting; ACCC, *Digital Platforms Inquiry* (Final Report, June 2019).

[11] See the ASIC 'Enhanced Regulatory Sandbox' https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/, which allows legal persons to test novel financial services products or credit activities without first needing to obtain a credit license.

[12] https://www.unimelb.edu.au/caide/study/2022-demystifying-ai-ethics-masterclass (Accessed April 2022)

3. Questions from the Digital Technology Taskforce

1. What are the most significant regulatory barriers to achieving the potential offered by AI and ADM? How can those barriers be overcome?

One significant barrier to the greater effective adoption of AI/ADM systems may lie be an overoptimism displayed by firms, government departments and other users. Currently, ADM systems still have flaws and are not as "smart" as sometimes suggested by proponents of AI. For example, according to a 2019 study by EY, 30 to 50 per cent of robotic process automation projects fail.[13]

When a company deploys a flawed system, this poses significant risk. These risks include:

- The flawed system may cause internal issues such as incorrect processing or delays.
- The system may cause external issues such as customer dissatisfaction and loss of trust by consumers; or in the case of government, harm the social license of the government and erode democratic functions.[14]
- The system may need to be fixed which can be costly, both in time and funds.
- The system intended to streamline and automate processes has to be abandoned entirely and the company must rebuild the processes from scratch.

This is a significant risk for business, as technologies that are supposed to streamline operations can become cumbersome problems and are usually abandoned once they are no longer fit-for-purpose.

Well designed and targeted regulatory strategies may, perhaps surprisingly, assist in overcoming these risks by ensuring fit-for-purpose systems entering the market with strong oversight, quality control and contestability mechanisms that support accountability, built into their design.

2. Are there specific examples of regulatory overlap or duplication that create a barrier to the adoption of AI or ADM? If so, how could that overlap or duplication be addressed?

As discussed above in 2.1-2.2, the key to avoiding inefficient regulatory overlap and duplication lies in understanding the purpose of regulation, in careful consideration on whether to employ technology specific or general (technology neutral regimes) regulations, and in a willingness to utilise the full suite of regulatory tools, while understanding the network effects of these approaches. Regulatory design for responsible AI should itself be treated as space for experimentation and innovation and should be properly monitored as to its costs and effectiveness.

3. What specific regulatory changes could the Commonwealth implement to promote increased adoption of AI and ADM?

See above qu 1. We also refer to our discussion of the importance of robust procurement practices in 2.7. Many of the government departments and firms that utilise AI/ADM do so as purchasers of the technology, not as developers. Regulation for transparent AI and guidance on procurement best practice for responsible and trustworthy AI will benefit these firms in terms of obtaining a fit for purpose product while reducing the reputational risk of poor outcomes.

What are the costs and benefits (in general terms) of any suggested policy change?

Care should be taken in considering who benefits from arguments that regulation imposes undue costs or impedes innovation. There is a considerable market concentration in the firms that deliver

[13] Nitin Bhatt, "Five design principles to help build confidence in RPA implementations" EY, Nov 2019. https://www.ey.com/en_us/consulting/five-design-principles-to-help-build-confidence-in-rpa-implement

[14] Bush, G and Paterson J. "Governments as Regulators and Consumers of Ethical AI." *Turkish Policy Quarterly,* March 2022.

technological solutions, and what these firms purport harms their interests may in fact protect and benefit local business and government who are the purchasers of those technologies.

The costs and benefits of regulatory initiatives should not be determined as a matter of mere impression. They should be scrutinised and crucially assessed. Universities represent an expert and neutral source of expertise of such tasks.

4. Are there specific examples where regulations have limited opportunities to innovate through the adoption of AI or ADM?

Arguments that there is an overly heavy regulatory burden should be treated with a degree of scepticism. While we embrace good regulatory design, we dispute the claim that regulation necessarily impedes innovation. Facebook's business model has been used as a case in point several times[15] endeavouring to illustrate the false assertion that innovation and regulation run counter to one another. Regulation can help ensure that innovation is not antithetical to the public interest. The key to assessing these questions is to consider the purpose of the regulation in question and whether it is proportionate to the risks it is seeking to address.

5. Are there opportunities to make regulation more technology neutral, so that it will more apply more appropriately to AI, ADM and future changes to technology?

See discussion above 2.3. The issue of 'future proofing' regulation is not a new one. Effective regulatory regimes typically rely on a combination of principles-based safety net rules that are flexible enough to adapt to new changes in practice. These can be supported by regulation, soft law, guidelines, and codes that back up the principles in a manner more tailored to particular contexts. However, we suggest that high risk uses of AI/ADM – for instance involving facial recognition technologies, the use of ADM to determine benefits or rights or curtail liberty, particularly of vulnerable or marginalised groups – should be governed by clearly defined law, consistent with human rights perspectives.

6. Are there actions that regulators could be taking to facilitate the adoption of AI and ADM?

The Issues Paper identifies transparency, explainability and accountability as core principals of ethical AI in its discuss of the OECD/G20 AI Principles (p.6). See above 2.5 for the importance of these principles.

Ensuring these practices in regulation would be an enabler for businesses and government looking to use AI and ADM as they would avoid the issues of deploying flawed systems. Indeed, given transparent and explainable AI are essential preconditions for accountability and oversight of AI/ADM systems, there may be a case for mandating these requirements by law at least in high-risk contexts.

Yet there are high levels of uncertainty about what is means to operationalise these requirements. Australian standards have a role here but so does soft law guidance provided by regulators.

7. Is there a need for new regulation or guidance to minimise existing and emerging risks of adopting AI and ADM?

As discussed above in 2.7, we consider that in general existing law can prove fit-for-purpose for regulating AI, combined with a commitment to upskilling and capacity building in cognate regulators. However, there are at least two contexts in which AI/ADM specific regulation may be justified:

- High risk uses of AI, as assessed by reference to human rights standards
- In providing for transparent and explainable AI, the preconditions to accountable and contestable AI.

[15] See generally, Johann Hari, *Stolen Focus*, (Bloomsbury Publishing, 2022) ch 6-7

8. Would increased automation of decision making have adverse implications for vulnerable groups? How could any adverse implications be ameliorated?

There is a significant risk that increased use of ADM systems will have adverse implications for vulnerable groups. There are many, now notorious, international examples of this in the last five to ten years:

- COMPAS, in the United States, a tool used to predict recidivism, has been criticised as disproportionately discriminating against persons of colour.[16]
- The OfQual grading algorithm 2020 used to grade students in the UK due to COVID disruptions. [17] The algorithm used the historical data from schools to give students their marks, resulting in students from high performing schools, often private schools being given higher grades than students from low performing schools. This algorithm was widely protested and eventually thrown out, costing the deploying agency significantly in funding and time.
- Self-driving car errors including Uber self-driving car running reds lights[18] and causing the unfortunate death of a pedestrian in 2018.[19]
- IBM 'Watson for oncology' was a supercomputer designed to aid in diagnosis and prescriptions but was plagued with errors including prescribing erroneous and dangerous cancer treatments.[20]
- Amazon's recruitment algorithm that was found to prioritise male candidates over female candidates even without the inclusion of gender in the data.[21]

Australia is not immune from failings in ADM tools which have fallen more heavily on marginalised and disadvantaged people: as illustrated by Robodebt and by overreaching in the garnishing of debts in NSW.[22] Not only were these examples of automation found to be unlawful, even when the flaws in the process were recognised, there were no mechanisms for affected people to effectively contest the outcomes.[23] Significant stress, anxiety and mental harm were inflicted on those subject to wrongful assessments. The erosion of public trust resulting from these episodes is still palpable, and arguably overshadows more welfare enhancing uses of the technology, such as the examples mentioned in the issues paper, of monitoring truck drivers for tiredness or car drivers for using mobile phones.

Many of the issues and concerns around the use of ADM in discretionary decision-making have been illustrated and discussed in the recent report by the NSW Ombudsman, along with recommendations for rigorous testing, oversight and auditing of the use of data driven ADM in government provisions

---

[16] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[17] Coghlan, Simon, Tim Miller and Jeannie Paterson. (2021). Good Proctor or "Big Brother"? Ethics of Online Exam Supervision Technologies. Philosophy and Technology. DOI: https://doi.org/10.1007/s13347-021-00476-1

[18] https://www.theverge.com/2017/2/25/14737374/uber-self-driving-car-red-light-december-contrary-company-claims

[19] https://www.bbc.com/news/technology-54175359

[20] https://www.theverge.com/2018/7/26/17619382/ibms-watson-cancer-ai-healthcare-science

[21] https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine

[22] NSW Ombudsman, *The new machinery of government: using machine technology in administrative decision-making* (Special Report, 29 November 2021).

[23] Tim Miller, Henrietta Lyons and Gabby Bush 'Data Isn't Neutral and Neither are Decision Algorithms', *Pursuit* (online, 15 September 2020) https://pursuit.unimelb.edu.au/articles/data-isn-t-neutral-and-neither-are-decision-algorithms.

of services and enforcement.[24] We commend these recommendations, and also scenarios with a high level of impact on people's lives, to the value of a human rights based approach, as recommended by the AHRC and discussed in 2.5 above.

9. Are there specific circumstances in which AI or ADM are not appropriate?

AI applications that rely on biometric markers to ascertain character, emotion or state of mind are, in the words of former Human Rights Commissioner Ed Santow, 'junk science'.[25] They should not be used in government services, and their use by private corporations should be discouraged, and indeed scrutinised by relevant regulators as very likely giving rise to misleading conduct.[26]

We also question the use of facial recognition and other surveillance technologies in schools and on very young or other people with limited opportunities to object to these technologies, given the inaccuracies associated with the technology, the other options that are available.[27]

10. Are there international policy measures, legal frameworks or proposals on AI or ADM that should be considered for adoption in Australia? Is consistency or interoperability with foreign approaches desirable?

Tech companies are not geographically constrained. There is a benefit to their operations for law across like-minded countries to be consistent and complementary. This also may benefit regulators who can more efficiently work to coordinate enforcement strategies against transgressing companies.[28]

[24] NSW Ombudsman, *The new machinery of government: using machine technology in administrative decision-making* (Special Report, 29 November 2021).

[25] Ed Santow, CAN ARTIFICIAL INTELLIGENCE BE TRUSTED WITH OUR HUMAN RIGHTS?, (2020) Australian Quarterly, 17.

[26] Jeannie Marie Paterson, 'Misleading AI' (forthcoming) 2022 Loyola Chicago Consumer Law Journal.

[27] Simon Coghlan and Jeannie Paterson presented on their paper 'Virtue and Vice in the Design and Deployment of Digital Technologies for Education,' for the Birmingham Centre for Character and Virtue, (December 2020).

[28] Paterson, Jeannie Marie, and Bant, Elise, et al. "Australian Competition and Consumer Commission v Google: Deterring misleading conduct in digital privacy policies". *Communications Law - Journal of Computer, Media and Telecommunications Law*, vol.26,no.3, 2021, pp. 136-148

4. Conclusion

AI and ADM are fledgling technologies that, while possessing potential to realise unprecedented conveniences and efficiencies, should be treated with caution. Many of these technologies (AI in particular) operate in ways that humans are unable to comprehend in detail. Furthermore, AI and ADM can be used in situations, that range from the relatively benign (e.g., pop song recommender systems) to truly high-stakes circumstances (e.g., self-driving cars, welfare allocation). The drive to innovate should therefore be attentive to the nature and circumstances of the use (and abuse) of the technology. For example, the use of AI to inform the decisions of law courts or the issuing of fines needs to be approached with extreme caution. Indeed, the drive to innovate in regard to some uses of AI/ADM—such as in sentencing or parole decisions, in the determination of student grades for entry to universities, or in public surveillance that uses facial recognition—should be tempered by recognition of the possibility that some uses are simply inappropriate. It will require careful thinking to determine when and how AI/ADM should be developed and deployed.

And yet, as we have emphasised in this submission, regulation need not stifle innovation. The goal should be to create a regulatory environment that is accommodating and nurturing of the right kinds of innovation. Australia is fortunate in that it is home to a large community of ambitious, talented, and altruistic individuals who aspire to use their talents in ways that will improve the lives of others. The goal of any changes to regulatory frameworks should therefore be to provide the necessary guidance to materialise these aspirations for genuinely responsible and trustworthy AI.

Contributors

Prepared by:

Prof Jeannie Marie Paterson, Centre for AI and Digital Ethics and the Melbourne Law School

Dr Paul Barry, Policy and Government Relations

Gabby Bush, Centre for AI and Digital Ethics

Dr Simon Coghlan, Centre for AI and Digital Ethics and the School of Computing and Information Systems

Liam Harding, Centre for AI and Digital Ethics and the Melbourne Law School

Professor Tim Miller, Centre for AI and Digital Ethics, and the School of Computing and Information Systems

Alex Paterson, Centre for AI and Digital Ethics

Professor Liz Sonenberg Pro Vice-Chancellor, Systems Innovation

Dr Michael Wildenauer, Centre for AI and Digital Ethics, and the Melbourne Law School