Submission to the Digital Technology Taskforce

on the Issues Paper

'Positioning Australia as a leader in digital economy regulation - Automated Decision Making and AI Regulation'

22 April 2022

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for privacy, democracy, fairness & freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[1]

[1] Learn more about our work on our website: https://digitalrightswatch.org.au/

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Digital Technology Taskforce regarding the Issues Paper on 'Positioning Australia as a leader in digital economy regulation - Automated Decision Making and AI Regulation' as part of Australia's Digital Economy Strategy.

Overall, we are concerned that the priorities and framing of the Issues Paper represent an approach which focuses heavily on reducing regulatory barriers for economic gain, without due regard to the ways that artificial intelligence (AI) and automated decision making (ADM) will impact the rights, safety and wellbeing of individuals and communities in Australia. We appreciate that this is the first step in the public consultation process, and look forward to seeing the Taskforce develop a balanced approach over the coming months.

For reference, DRW has been an active participant in other public consultations related to Australia's digital economy, including the:

- News Media Bargaining Code,[2]
- Online Safety Act,[3]
- Privacy Act Review Discussion Paper,[4]
- Data Availability and Transparency Act,[5] and
- Trusted Digital Identity Framework.[6]

We welcome the opportunity to participate in further discussion with the Digital Technology Taskforce throughout the process of developing the Discussion Paper in the latter half of 2022, as well as in development of the overarching Digital Age Policy Framework.

---

[2] Digital Rights Watch, Submission to the Economics Legislation Committee on the proposed Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020, 18 January 2021, available at: https://digitalrightswatch.org.au/2021/01/28/submission-news-media-bargaining-code/

[3] Digital Rights Watch, Submission to the Department of Infrastructure, Transport, Regional Development and Communication on the proposed Online Safety Bill 2020, 14 February 2021, available at: https://digitalrightswatch.org.au/2021/02/18/submission-the-online-safety-bill/

[4] Digital Rights Watch, Submission to the Attorney-General on the Discussion Paper regarding the Review of the Privacy Act 1988, 10 January 2022. Available at: https://digitalrightswatch.org.au/2022/01/11/submission-privacy-act-review-discussion-paper/

[5] Digital Rights Watch, Submission to the Office of the National Data Commissioner on the Data Availability and Transparency Bill 2020, 6 November 2020, available at: https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/

[6] Digital Rights Watch, Submission to the Digital Transformation Agency on the Digital Identity Exposure Draft, 27 October 2021, available at: https://digitalrightswatch.org.au/2021/10/28/submission-digital-identity-exposure-draft/

General remarks

While we appreciate that this Issues Paper sits within a broader Digital Economy Strategy and therefore a focus on the potential economic and productivity gains is to be expected, we are concerned that not enough consideration has been given to the impact that AI and ADM has upon the rights, safety and wellbeing of individuals and communities.

DRW understands the allure of, and genuine interest in, the possible economic benefits promised by AI and ADM. There are also many areas where AI and ADM may offer immense public good, for example, in medical sciences and early detection of diseases. Robust regulation that places human rights and safety at the centre is not a threat to this kind of technological innovation.

However, these technologies also present significant risks to privacy and digital security, and can result in biased, discriminatory or other harmful outcomes. This is of particular concern should an algorithmic system result in individuals or groups being unable to access essential government, health or financial support and services, or where AI or ADM is used in disciplinary, judicial or policing contexts. We need only look back to the recent disastrous Online Compliance Intervention, more commonly referred to as "Robodebt", to get a glimpse of the kind of harms that can arise when algorithmic technologies are implemented without appropriate rules, risk assessments and safeguards.[7]

There is a wealth of recent examples documenting ways that AI and ADM technologies can result in significant harm, such as:

- individual harm caused by facial recognition used by law enforcement resulting in wrongful arrest,[8]
- collective harm as a result of racial profiling through predictive policing,[9]
- harms of allocation arising from discriminatory allotment of, or unequal access to, products or resources,[10]
- harms of representation which reinforce existing discrimination, disadvantage or stigma, often by using historical datasets which contain biased, incomplete or outdated data.[11]

---

[7] See, for example, 'Robodebt responsible for $1.5bn unlawful debts in 'very sorry chapter' court hears,' The Guardian, May 2021, https://www.theguardian.com/australia-news/2021/may/07/robodebt-responsible-for-15bn-unlawful-debts-in-very-sorry-chapter-court-hears

[8] This has occurred at least three times, see for example: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[9] See, for example: 'Technology can't predict crime, it can only weaponise proximity to policing,' Electronic Frontiers Foundation, September 2020, https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing

[10] For example, in 2019 Apple was accused of discrimination after offering a lower credit limit to a woman compared to a man with a similar credit rating. See: 'Apple Card Investigated after gender discrimination complaints,' The New York Times, November 2019. See: https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

[11] For example, Microsoft found gender bias arose in models based on data that contained gendered stereotypes. See 'Man is to computer programmer as woman is to homemaker? Debiasing word embeddings,' Microsoft, 2016. https://www.microsoft.com/en-us/research/publication/quantifying-reducing-stereotypes-word-embeddings/

Perhaps one of the most egregious and well-known examples of harm caused by an algorithmic system is the commercially-available risk assessment tool called COMPAS, used to predict recidivism and to assess a criminal defendant's likelihood of committing a crime. This algorithmic tool was found to be racially biased—predicting inaccurately that Black defendants were twice as likely to reoffend than white defendants—and notably, *no more accurate* or fair than predictions made by people with little to no criminal justice experience.[12]

If Australia is seeking to be a leader in digital economy regulation and earn public trust and confidence regarding the use of these technologies, especially in the public sector, it is essential that the approach to regulation take seriously – and learn from – these and other examples of AI and ADM creating or exacerbating harm.

Recommendation 1
Any regulation of AI and ADM should centre the human rights, safety and wellbeing of individuals and communities as a first priority.

Protecting personal information

Not all uses of AI and ADM will handle personal information or raise privacy issues. However, those that do process personal information, make predictions or decisions based on personal information as data inputs, or are designed to interact directly with individuals will likely raise some privacy considerations.

Many of the harms that arise from AI and ADM stem from inappropriate collection and use of personal information. As such, robust privacy regulation can go a long way toward mitigating privacy-related harms.

For instance, it is not uncommon for the data inputs to algorithmic systems to be a secondary use of personal information, or for that data to have been collected in ways that may not have been reasonably expected or understood by individuals.[13] In some cases models will make inferences about individuals which may constitute collection of personal or sensitive information, or possibly discriminate based on “proxy variables” which may not readily appear to be personal information, but can still lead to unfair or discriminatory outcomes.[14] Privacy law can, and should, be employed to mitigate these issues and more.

Reforming privacy regulation in Australia is an essential step toward building a fair digital economy and for AI and ADM to be developed and deployed for the public good. Beyond

---

[12] ‘The accuracy, fairness, and limits of predicting recidivism,’ Julia Dressel and Hany Farid, Science Advances, Volume 4, Number 1, January 2018. https://advances.sciencemag.org/content/4/1/eaao5580; ‘Machine Bias,’ ProPublica, May 2016. See https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[13] ‘Algorithms, AI, and Automated Decision — A guide for privacy professionals,’ Salinger Privacy, 2021. Available at: https://www.salingerprivacy.com.au/downloads/algorithms-guide/

[14] ‘Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias,’ Australian Human Rights Commission, 2020, page 11. Available here: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing

that, we believe that **recognising the right to privacy at the federal level is critical to protecting the privacy and safety of all Australians.** Enshrining a federal right to privacy would create a rights-based relationship with the way Australians' data and privacy is treated, as opposed to an economic or value-driven model which has been the case so far.[15]

We also wish to urge the Taskforce not to fall subject to a belief that "data doesn't lie". We note that the Issues Paper states that "automation has the potential to reduce bias and discrimination, as a machine can only reflect the inputs provided by human users. However, it has long been recognised that algorithms can reflect the bias of their programmers".[16] This does not account for issues of historical or representation bias, which can occur within the datasets used as inputs. As highlighted by Lizzie O'Shea, "the data on which we train technology uncritically ingests yesterday's mistakes."[17] We urge the Taskforce to consider the significant and growing amount of research into bias and fairness in machine learning and deep learning to ensure that the risks and realities of the technology are sufficiently considered when developing any proposals for regulation.[18]

Recommendation 2
Introduce a federal-level right to privacy in order to effectively empower all Australians in the digital age and protect them against privacy violations by public and private entities.

Recommendation 3
Consider the potential to regulate aspects of AI and ADM through the regulation of information privacy. By placing robust limitations on what can and cannot be done with individuals' personal information, many of the downstream harms resulting from AI and ADM can be mitigated.

---

[15] The emphasis on Consumer Data Rights (CDR) is evidence of this, as is the consideration by the Australian Bureau of Statistics to merge privately held datasets into the public census data to improve results and the 'economic contribution' of the census. This value-driven calculation of privacy infringement vs economic benefit fundamentally shifts when we consider a rights-based system.
[16] Page 11, 'Positioning Australia as a leader in digital economy regulation - automated decision making and AI regulation', Issues Paper.
[17] Future Histories: What Ada Lovelace, Tom Paine, and the Paris Commune can teach us about digital technology, Lizzie O'Shea, Verso, 2019, page 53.
[18] See, for example, 'Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias,' Australian Human Rights Commission, November 2020, page 47, Available at: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing; and 'A Framework for Understanding Unintended Consequences of Machine Learning,' Harini Suresh and John Guttag, Cornell University, February 2020. Available at: https://arxiv.org/abs/1901.10002

Automating surveillance and speed-up in the workplace

The Issues Paper states that "digitally powered automation is creating new ways of working that will boost productivity, improve service delivery, create jobs, help solve the real-world problems of today and grow the businesses of tomorrow."[19]

The suggestion that technology will supplement or replace labour and increase productivity is not new. For centuries the prospect of automation technologies has given rise to both fantasies and anxieties regarding the future of work. However, as research is beginning to reveal, many advancements in automation do not reduce or supplement work, but rather augment the role of management.[20] They also often result in the increase of pervasive surveillance and monitoring of workers under the guise of productivity.

RMIT University PhD Candidate and Researcher Lauren Kelly highlights in a recent essay:

> **"**Issues of work speed-up, monitoring and surveillance are closely associated with workplace automation. That is, rather than replace human workers with robots, many are being forced to work *like* robots."[21]

Some of the most sophisticated automation technologies available do not eliminate or reduce physical tasks. Rather, they monitor and track workers through wearable devices and other technologies. Other areas of work such as recruitment, human resources and rostering are being transformed into 'algorithmic management'. Automation in the workplace often functions as a tool of work *intensification* rather than *elimination.* This may indeed result in surface-level efficiency and productivity gains, but it is to the detriment to the rights, health and dignity of workers—causing long term damage to society and the economy.

We note that the issue of workplace surveillance received some acknowledgement in the Privacy Act Review Discussion Paper. However, we are of the view that extending the Privacy Act to include employee records does not get to the heart of the problems associated with workplace privacy issues, surveillance and automation technologies. To that end, DRW strongly suggests that further investigation is undertaken in this area to develop possible legislation and policies to adequately deal with the complexity of changing workplace surveillance and automation practices.

---

[19] Page 3, 'Positioning Australia as a leader in digital economy regulation - automated decision making and AI regulation', Issues Paper.

[20] See, for example: Mateescu, A & Nguyen, A 2019, "Algorithmic management in the workplace," Data & Society Research Institute, no. February, pp. 1–15; Moore, P v, Upchurch, M & Whittaker, X 2018, Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism, Palgrave Macmillan, London.; and Kelly, L 2020, Technology and power: Understanding issues of insecure work and technological change in Australian workplaces, Melbourne.

[21] See Lauren Kelly, 'Automation is changing work—not erasing it', *State of Digital Rights Report: A 2021 Retrospective,* Digital Rights Watch. Available at: https://digitalrightswatch.org.au/2022/03/03/the-state-of-digital-rights-a-2021-retrospective/

Recommendation 4
Further investigate existing workplace automation and surveillance practices across Australia to identify what is needed to adequately protect workers' rights and long term productivity, balancing digital privacy of workers with reasonable monitoring requirements within an employment relationship.

Regulating for algorithmic fairness

We note that a significant proportion of the Issues Paper, including questions 1-4, frame regulation as a barrier to innovation and to realising the potential offered by AI and ADM. We wish to emphasise that robust regulation of AI and ADM is essential to the Taskforce's goal to increase public trust and confidence in these technologies. Appropriate regulation can also help facilitate technological innovation that is in the public interest. As outlined in the previous sections of this submission we have already seen the harmful results of unbridled technological innovation without adequate regulation.

An increasing number of decisions that impact the lives of everyday people are informed by ADM and AI. In the absence of proper regulation there is significant risk of these technologies creating or exacerebating discrimination and other human rights violations.

In other jurisdictions, algorithmic decision making is regulated, or soon will be. For example:

- The right to object to and opt out of ADM is included in the EU General Data Protection Regulation (GDPR). It also gives individuals the right to receive enough information to be able to understand the automated system, as well as a right to review by a human decision maker.
- Canada's proposed Consumer Privacy Protection Act includes similar requirements to the GDPR.[22]
- In April 2021, the European Commission proposed new legislation to regulate the use of Artificial Intelligence in accordance with "EU values and fundamental rights".[23]
- New York City passed legislation in 2021 that requires companies that use algorithmic systems to assist in recruitment processes to audit these systems to ensure they are not discriminatory.[24]

Recommendation 5
Introduce a range of rights with regard to the use of AI and ADM by government agencies:

1. A right to object to and opt-out of automated decision making
2. A right to review and appeal a decision made wholly or partly by automated means,
3. A right to an accessible, plain language explanation about how the system works and/or about how a decision has been made

[22] See https://blog.didomi.io/en/canada-data-privacy-law#three
[23] 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, COM/2021/206 final, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
[24] See https://www.brookings.edu/blog/techtank/2021/12/20/why-new-york-city-is-cracking-down-on-ai-in-hiring/

Reccomendation 6
Introduce a requirement for organisations proposing to use AI or ADM in high risk areas to conduct an algorithmic impact assessment, audit and evaluation. This will increase accountability, transparency, risk assessment and management as part of good due diligence.

Factors used to determine whether an area is "high risk" should include consideration as to whether the system:

- involves a critical sector (such as healthcare, welfare, housing, insurance, employment, education, political processes, the legal system and law enforcement),
- may have a critical impact (such as on people's health, wellbeing and oppotunities; legal or financial impacts),
- makes decisions, predictions or recommendations at a large scale,
- uses data inputs containing protected attributes (as recognised by discrimination law) or sensitive information (under privacy law), or,
- is designed to make decisions or predictions that will adversely impact vulnerable or marginalised groups.[25]

Biometric information and facial recognition

The use of biometric information is not currently specifically regulated in Australia despite the significant risks to privacy and security should it be misused. Rather, it is included under "sensitive information" in the Privacy Act.

The 2021 report produced by the Australian Human Rights Commissioner (AHRC), which is referenced in the discussion paper, suggests "a moratorium on the use of facial recognition and other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement."[26]

The Taskforce may wish to look to international precedents when considering the regulation of facial recognition, including the bans on its use in San Francisco and Maine, as well as significant limitations on it in Virginia, Massachusetts and Washington.[27] With regard to restricting the use of biometric information by the private sector, the Taskforce may consider the Biometric Information Privacy Act (BIPA) passed unanimously in 2008 in Illinois.[28] The BIPA imposes obligations and prohibitions on how private companies can handle biometric information, as well as a private right of action to allow any person aggrieved by a violation to bring an action in court. A specific right of action for misuse of biometric information would be a useful and significant inclusion in any regulation of biometric information.

---

[25] Adapted from 'Algorithms, AI, and Automated Decisions — A guide for privacy professionals,' Salinger Privacy, 2021. See https://www.salingerprivacy.com.au/downloads/algorithms-guide/
[26] See https://tech.humanrights.gov.au/artificial-intelligence/facial-recognition-biometric-tech
[27] See, for example, 'Main passes the strongest state facial recognition ban yet,' The Verge, 2021. Available here: https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law
[28] Illanois General Assembly, Biometric Informaton Privacy Act https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Recommendation 7
Ban the use of facial recognition and other biometric surveillance technologies until there are robust protections in place governing its use, with specific regard to the protection of human rights.

Additional research and resources

In addition to the references included throughout this submission, we wish to raise attention to a few other areas of work relevant to the regulation of AI and ADM which we strongly suggest the Taskforce consider as they progress:

- For a deep dive into the relationship between information privacy law, harm, and risk assessments in relation to AI and ADM, we suggest the Taskforce refer to 'Algorithms, AI, and Automated Decisions — A guide for privacy professionals' from Salinger Privacy.[29]
- For an introduction into the growing field of work being done in data sovereignty and Indigenous AI Protocols we recommend the work being conducted by Australian National University, Old Ways, New, and the Goethe Institue in their Indigenous Protocols // AI Labortatory project,[30] as well as the Position Paper developed by the Indigenous Protocol and Artificial Intelligence Working Group.[31]
- For a look at a public data trust framework and data stewardship, the Taskforce may wish to consider the Data Trust Initative of Cambrige University[32] and research conducted by the Ada Lovelace Institute.[33]

Contact

Samantha Floreani | Program Lead | Digital Rights Watch | samantha@digitalrightswatch.org.au

[29] See https://www.salingerprivacy.com.au/downloads/algorithms-guide/
[30] See https://indigenousprotocols.ai/ and 'Out of the Black Box: Indigenous protocols for AI,' Angie Abdilla, Megan Kelleher, Rick Shaw and Tyson Yunkaporta, 2021. https://static1.squarespace.com/static/5778a8e3e58c62bbf1a639ae/t/61808f1d034eda41942223a9/1635815199890/*Final+Unesco+Paper_Designed.pdf
[31] See https://www.indigenous-ai.net/position-paper/
[32] See https://datatrusts.uk/about
[33] See https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/