Submission to the Treasury

regarding the

Review of AI and Australian Consumer Law 2024

24 November 2024

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/

Who we are

Digital Rights Watch is a charity organisation founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness and freedom. Digital Rights Watch educates, campaigns and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website:

www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Elizabeth O'Shea | Chair | lizzie@digitalrightswatch.org.au

Kate Bower | Digital Rights Advocate | kate.bower@digitalrightswatch.org.au

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Treasury regarding the AI and Australian Consumer Law Review 2024. We support the Australian government's commitment to developing a regulatory environment that builds community trust and promotes AI adoption.

As Australia's leading digital rights organisation, DRW is primarily concerned with the implications of AI and automated decision making (ADM) systems for the human rights, safety and wellbeing of individuals and communities. We actively participate in public consultations regarding the development of legislation and policy in relation to technology and human rights. Our recent submissions relevant to AI regulation and governance include:

- Submission to the Department of Industry, Science and Resources Proposals Paper introducing mandatory guardrails for AI in high-risk settings[2]
- Submission to the Select Committee on Adopting Artificial Intelligence regarding the inquiry into the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia[3]
- Submission to the Department of Industry, Science and Resources in response to the Safe and Responsible AI issues paper[4]
- Submission to the Digital Technology Taskforce in response to 'Positioning Australia as a leader in digital economy regulation - Automated Decision Making and AI Regulation' Issues Paper[5]
- Submission to the Senate Economics Committee Inquiry into the influence of international digital platforms[6]

---

[2] See Appendix 1

[3] Digital Rights Watch Submission to the Select Committee on Adopting Artificial Intelligence regarding the inquiry into the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia, 17 May 2024, Available at: https://digitalrightswatch.org.au/2024/10/07/submission-the-opportunities-and-impacts-for-australia-arising-out-of-the-uptake-of-ai-technologies/

[4] Digital Rights Watch Submission to the Department of Industry, Science and Resources in response to the Safe and Responsible AI issues paper, 14 August 2023, Available at: https://digitalrightswatch.org.au/2023/08/14/safe-responsible-ai/

[5] Digital Rights Watch 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, Available at: https://digitalrightswatch.org.au/2022/04/22/submission-regulating-ai-and-automated-decision-making-in-australia/

[6] Digital Rights Watch Submission to the Senate Economics Committee inquiry into the influence of international digital platforms, 14 March 2023. Available at: https://digitalrightswatch.org.au/2023/04/26/democratising-digital-economies/

DRW welcomes the opportunity to participate in public hearings or further consultations and to provide comment and feedback on future specific proposals.

General remarks

As noted in the Discussion Paper, AI-enabled goods and services are now commonplace in the Australian market and people interact with AI-enabled products in their daily lives. These products range from entirely online digital products, such as subscription streaming services for entertainment and customer service chatbots, to internet-connected physical goods such as digital assistants in smart phones and smart speakers, to internet-of-things goods that have little to no human interactivity, such as robot vacuums.

In general, we regard the ACL as robust principles-based legislation that protects consumers from a broad range of harms and poor business practices. However, AI-enabled products present unique challenges to consumers' ability to participate fairly and safely in the market and enact their consumer rights using the Australian Consumer Law (ACL). The largest challenge is the opacity of AI and algorithms, making it difficult for individuals to assess whether a good or service meets the consumer guarantees of acceptable quality and fitness for purpose. Consumers understand there is a problem when a toaster doesn't toast, however it's near impossible for everyday people to assess the quality and efficacy of AI-enabled products, making it equally impossible to seek remedy using the ACL.

In the broader context of digital markets, in which AI-enabled products exist, practices of deceptive design, unfairness and manipulation should be addressed through economy-wide provisions. As such, DRW supports the introduction of a prohibition on unfair trading and refer to the work of consumer groups such as CHOICE and Consumer Policy Research Centre for further elucidation of the benefits of an unfair trading ban.

Privacy regulation as a form of AI regulation

As noted in our previous submissions, many of the harms that arise from AI and automated decision making stem from inappropriate collection and use of personal information. As such, robust privacy regulation can go a long way toward mitigating privacy-related harms caused by AI.

We welcome the recently tabled *Privacy and Other Legislation Amendment Bill 2024*. The reforms contained in this bill are essential. However we note that there is no timeframe for the many dozens of other reforms that the government agreed must be made to the Privacy Act. Specifically, this includes reforms to the definition of personal information (which sets the scope of the act), the concept of consent, a proposed 'fair and reasonable' test, as well as the removal of certain exemptions.

Without these reforms, the personal information being collected and used by industry to train AI models will take place based on an outdated notion of consent that does not align with community expectations. This is a problem not just for public trust in these models, but also it significantly increases the risk of unintended outcomes. This includes serious and significant cybersecurity risks, as AI-enabled consumer products draw on large troves of data, the creation of which increases the risk of criminal hacking. Critically, without proper care and due diligence applied to data sets used to train AI, there are significant risks of discriminatory and harmful outcomes, made all the more dangerous by having the cover of supposedly neutral technology.

For these reasons, privacy law is a fundamental part of AI regulation and must be factored into any regulatory approach. The failure to implement full-scale privacy reform to date undermines our confidence that the guardrails will do the job we expect of them. The government must prioritise the remaining privacy reforms it has committed to implementing.

Privacy is essential to upholding democracy, reining in corporate power, and building a safe and fair digital future.

The bill has been described as a 'first tranche' in the process of reforming the Act.[7] The two central proposals, a statutory tort and the roadmap for a children's online privacy code, together represent a good first step, but Australia's privacy legislation remains decades behind other nations. Delay in pursuing the remaining reforms leaves gaping holes in Australia's legal regime for the protection of personal information.

We are past the time for incremental amendments to the Act. *The Privacy Act Review Report 2022* ("the Report") introduced 116 recommendations that would bring the Act up to an international standard, and they ought to be legislated in their entirety. Australians expect their privacy to be protected now.

If the Attorney-General's office intends on introducing these reforms in 'tranches', as is suggested, we expect to see a detailed roadmap and timeline for the introduction of the remaining tranche(s), else we risk the remaining reforms being delayed indefinitely. We concur with many other civil society organisations in calling on the government to implement the remaining reforms within six months of taking office, should they win the next election. We also call on the opposition to make a similar commitment should they win office.

In addition to urgent Privacy Act reform and the introduction of an unfair trading prohibition, there are several amendments that could be made to the Australian

[7] Second reading speech – Privacy and Other Legislation Amendment Bill 2024, 12 September 2024, Available at: https://ministers.ag.gov.au/media-centre/speeches/second-reading-speech-privacy-and-other-legislation-amendment-bill-2024-12-09-2024

Consumer Law to ensure its fit-for-purpose for AI-enabled products and that people can continue to enjoy the same level of protection under the ACL as with other goods and services.

Recommendation 1: introduction of a new *sui generis* category of 'digital goods'

As suggested in the discussion paper, AI-enabled products are not adequately captured in the descriptions of goods and services in the ACL. In the example of a robot vacuum, the product is both a 'good' ie. a vacuum cleaner but also a 'service' as the AI algorithm is not static but constantly 'learning' and being updated through internet-connected communication to the manufacturer and may be decommissioned (temporarily or permanently) in circumstances outside of the control of the consumer. It makes sense to the ordinary consumer that obligations for adequate quality such as those for the provision of goods under the ACL are as applicable as the requirement for due care and skill as for services in the example of a robot vacuum, and AI-enabled products more broadly.

Further there are aspects of digital goods that require specific protections to ensure their safe functionality within the marketplace, such as interoperability with other goods in the market.

We recommend that a new *sui generis* category of digital goods be created within the ACL that includes the following statutory consumer guarantees:

- Acceptable quality (similar to Section 54, ACL) - suppliers and manufacturers guarantee that digital goods are acceptable quality to a reasonable consumer when sold
- Fit for any specified purpose (similar to section 55, ACL) - digital goods must be suitable for any purpose specified by the supplier or the consumer
- Supplied with due care and skill (similar to section 60, ACL) - suppliers and providers of digital goods should exercise due care and skill in their provision
- Interoperability (new) - digital goods should be capable of working with other products and services as expected
- Minimum duration for software and security updates (new) - consumers should receive software and security updates for a minimum specified period to ensure ongoing product safety and functionality. The minimum period should be determined following consultation with industry and civil society groups but should be a minimum of three years.

Recommendation 2: amend the product safety and liability framework to include 'digital goods'

The Australian Government is currently considering options for mandatory guardrails for AI in high-risk settings. Digital Rights Watch is broadly supportive of

this proposal, despite issues relating to the absence of a regulatory strategy and enforcement, and the need for prohibitions of AI systems that pose an unacceptably high risk to people, as detailed in our submission in Appendix 1.

However, we believe that the Australian Consumer Law could offer basic consumer protections for low and medium risk AI products and services if appropriately adapted to address the unique qualities of digital goods and in particular AI-enabled products.

We suggest that the most straightforward way to achieve this aim, and retain the usefulness of the ACL would be to amend the product and safety liability framework as detailed in Sections 104 -160 to include digital goods by mention of digital goods in addition to 'goods'.

Further, Treasury should consider:

- Expanding the concept of 'safety defect' in the liability scheme to extend to psychological injury, along with physical or financial harms or loss to cover harms caused by biased, discriminatory or psychologically harmful AI-enabled products. For example, an AI chatbot or character avatar that encourages self-harm of the user [8]
- Mandatory Information Standards for AI-enabled goods that explain what the product claims to do, what it does not do, and the evidence supporting these claims. This transparency is essential for informed consumer choice and trust and to address the transparency problem allowing access to existing remedies under the ACL.
- Removing or amending the evidentiary burden on consumers to take action against a manufacturer of defective or unsafe AI-enabled products, to address the opacity and complexity problems associated with these. This could be done via a presumption of causality principle, as per the AI Liability Directive in the European Union.

Recommendation 3: further review of options for ex-ante obligations for 'digital goods' to ensure they are fit for purpose

Given the unique features of AI-enabled and digital goods - which make it difficult for consumers to assess and identify whether a given product is defective, works as intended or is the cause of injury or loss - it may be appropriate for certain classes of AI-enabled products to undergo pre-market assessments or safety checks. We advocate for further consideration and consultation of options for ex-ante obligations on digital goods in alignment with the Department of

[8] This mom believes Character.Ai is responsible for her son's suicide | CNN Business

Industry, Science and Resources consultation on the mandatory guardrails for high-risk AI systems.

Conclusion

The Australian Consumer Law is pragmatic principles-based legislation that has been protecting consumers for decades. Digital Rights Watch strongly advocates for updating the law to address the specific challenges posed by AI-enabled products so that the ACL can continue to deliver basic consumer protections for decades to come.

Appendix 1

Submission to the Department of Industry, Science and Resources

regarding the

Proposals Paper: Introducing mandatory guardrails for AI in high-risk settings

7 October 2024

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.[9]

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

Who we are

Digital Rights Watch is a charity organisation founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness and freedom. Digital Rights Watch educates, campaigns and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website:

www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Elizabeth O'Shea | Chair | lizzie@digitalrightswatch.org.au

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Department of Industry, Science and Resources regarding the Proposals Paper: Introducing mandatory guardrails for AI in high-risk settings (the Proposals Paper). We support the Australian government's commitment to developing a regulatory environment that builds community trust and promotes AI adoption.

As Australia's leading digital rights organisation, DRW is primarily concerned with the implications of AI and automated decision making (ADM) systems for the human rights, safety and wellbeing of individuals and communities. We actively participate in public consultations regarding the development of legislation and policy in relation to technology and human rights. Our recent submissions relevant to AI regulation and governance include:

- Submission to the Select Committee on Adopting Artificial Intelligence regarding the inquiry into the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia[10]
- Submission to the Department of Industry, Science and Resources in response to the Safe and Responsible AI issues paper[11]
- Submission to the Digital Technology Taskforce in response to 'Positioning Australia as a leader in digital economy regulation - Automated Decision Making and AI Regulation' Issues Paper[12]
- Submission to the Senate Economics Committee Inquiry into the influence of international digital platforms[13]

As previously noted, "AI" can be a slippery concept that has different meanings and purposes depending on who is using it and why. DRW believes the adoption of ISO definitions by the Department is sensible, however we do note that defining technology—especially AI technologies—can often be a point of contention, and may present drafting challenges in the regulatory context. We

[10] Digital Rights Watch Submission to the Select Committee on Adopting Artificial Intelligence regarding the inquiry into the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia, 17 May 2024, Available at: https://digitalrightswatch.org.au/2024/10/07/submission-the-opportunities-and-impacts-for-australia-arising-out-of-the-uptake-of-ai-technologies/

[11] Digital Rights Watch Submission to the Department of Industry, Science and Resources in response to the Safe and Responsible AI issues paper, 14 August 2023, Available at: https://digitalrightswatch.org.au/2023/08/14/safe-responsible-ai/

[12] Digital Rights Watch 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, Available at: https://digitalrightswatch.org.au/2022/04/22/submission-regulating-ai-and-automated-decision-making-in-australia/

[13] Digital Rights Watch Submission to the Senate Economics Committee inquiry into the influence of international digital platforms, 14 March 2023. Available at: https://digitalrightswatch.org.au/2023/04/26/democratising-digital-economies/

recommend that the department take an inclusive approach to its definition of AI, including simpler automated decision-making systems, as these can produce similar outcomes.

DRW has previously expressed concern about the priorities and framing of AI regulation in Australia. Specifically, we have raised concerns about the emphasis on the potential to create economic and social well-being at the expense of serious consideration of harm. We are pleased to see the proposed guardrails as part of a broader trend that represents a shift towards meaningfully grappling with risks.

Enforcement and prohibition

We understand that the publication of the guardrails represents the first step in the journey towards potentially comprehensive AI regulation. However, we also note that it remains difficult to assess the utility and value of the guardrails without a fulsome strategy for harm reduction and a clear approach to enforcement.

We appreciate that the guardrails are designed to reduce harm, but an effective approach to harm reduction will also require an assessment at an early stage to consider whether certain tools should be developed and deployed at all (even if they comply with the guardrails as a matter of process). Without such assessments, and a clear path to enforcement capabilities, the guardrails will remain statements that organisations and executives are encouraged to think about, but not much else. The guardrails alone are not sufficient as an AI governance strategy, and are not consistent with a human rights approach, which imposes specific limits and requires enforceability.

We think there is real utility in considering the consequences of non-compliance now, rather than later in the law reform process. That is because there is the potential for some kind of AI to be considered too high-risk and too dangerous such that it should be prohibited. This was envisaged in the European Union AI Act, for example, because the risk categories are attached to consequences. Noting question 4, we think a human rights approach leads to an inevitable conclusion that certain development and applications of AI must be banned, including for example, following the lead of the EU and banning:

- AI use cases that pose a high risk to people's human rights, such as in healthcare, education, and policing;
- AI systems that deploy dark patterns, that is "subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making," or exploit vulnerable people;
- AI systems that infer sensitive characteristics such as someone's political opinions or sexual orientation;

- Real-time facial recognition software in public places; and
- The weaponisation of AI.

Now is the time to think about what kinds of AI technology should be prohibited outright, because the risks posed to human rights are too great. We also think that now is the time to determine the consequences for non-compliance with the guardrails, as well as how the relevant regulator will be able to impose these. Without this strategic thinking, it is difficult to assess the utility of the guardrails as drafted.

Privacy regulation as a form of AI regulation

As noted in our previous submissions, many of the harms that arise from AI and automated decision making stem from inappropriate collection and use of personal information. As such, robust privacy regulation can go a long way toward mitigating privacy-related harms caused by AI.

We welcome the 'first tranche' of privacy reform that was recently tabled by the government in the form of the *Privacy and Other Legislation Amendment Bill 2024*. The reforms contained in this bill are essential. However we note that there is no timeframe for the many dozens of reforms that the government agreed must be made to the Privacy Act. Specifically, this includes reforms to the definition of personal information (which sets the scope of the act), the concept of consent, a proposed 'fair and reasonable' test, as well as the removal of certain exemptions.

Without these reforms, the personal information being collected and used by industry to train AI models will take place based on an outdated notion of consent that does not align with community expectations. This is a problem not just for public trust in these models, but also it significantly increases the risk of unintended outcomes. Without proper care and due diligence applied to data sets used to train AI, there are significant risks of discriminatory and harmful outcomes, made all the more dangerous by having the cover of supposedly neutral technology.

For these reasons, privacy law is a fundamental part of AI regulation and must be factored into any regulatory approach. The failure to implement full-scale privacy reform to date undermines our confidence that the guardrails will do the job we expect of them. The government must prioritise the remaining privacy reforms it has committed to implementing.

Options for regulating the guardrails

As a preliminary matter, we think Option 1 is at risk of being functionally equivalent to inaction. Incorporating the guardrails into existing regulatory regimes - such as privacy, administrative law, online safety, corporations,

intellectual property, competition and consumer protection, and anti-discrimination - is likely to be politically contested and slow. It is an unrealistic approach in circumstances where regulatory action is urgently needed.

In general, we support Option 3, not least because of our comments above about enforcement. We also think that there would be a real benefit in thinking about the powers that an AI regulator might need to be able to promote and monitor compliance with the guardrails. This includes seeking transparency from industry, intervening in the processes used by developers to implement the guidelines as needed, and offering guidance for both developers and deployers. There may also be benefit in a bespoke regulator in serving as a clearing house for complaints, and making policy recommendations that arise as a result.

We think the government should carefully consider the EU proposal to introduce a tort for non-contractual liability.[14] This is the moment to think carefully about how to ensure that those harmed by AI have a meaningful path to redress, to give the public confidence that such technology is trustworthy. This will also allow for such harms to be anticipated and acted upon by those developing and deploying AI, rather than ignored.

[14] Liability Rules for Artificial Intelligence See https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en