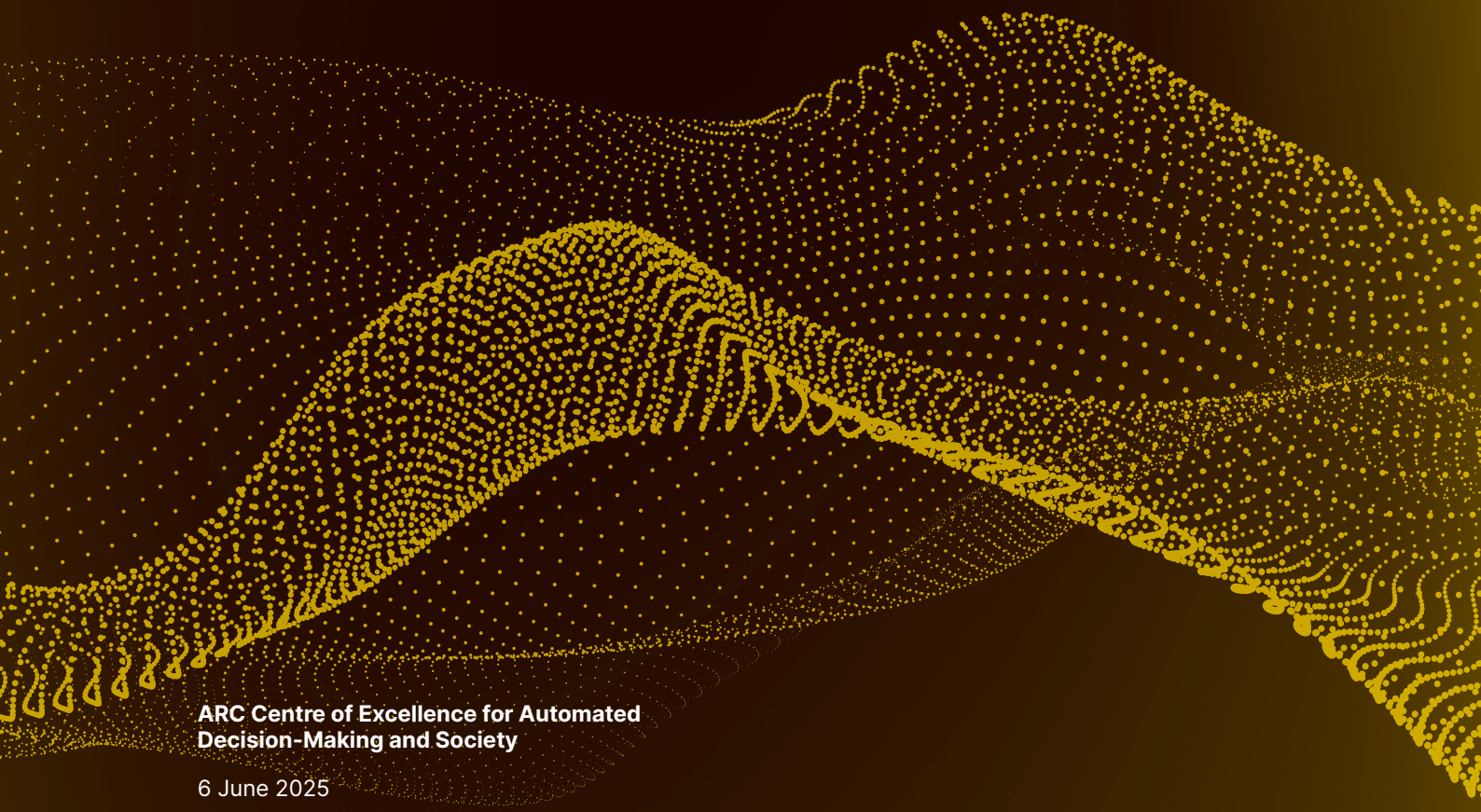
ADM+S

ARC Centre of Excellence for **Automated Decision-Making and Society**

ADM+S SUBMISSION

Productivity Commission Pillar 3: Harnessing data and digital technology

Authors
Jacky Zeng, Kimberlee Weatherall, Christine Parker,
Lina Przhedetsky, Madeleine Stirling, Henry Fraser, Julian Thomas



ARC Centre of Excellence for Automated Decision-Making and Society

6 June 2025

Acknowledgement of Country

In the spirit of reconciliation, we acknowledge the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Suggested citation

J. Zeng, K. Weatherall, C. Parker, L. Przhedetsy, M. Stirling, H. Fraser, J. Thomas. (2025) Submission to the Productivity Commission, *Pillar 3: Harnessing data and digital technology*. ARC Centre of Excellence for Automated Decision-Making and Society. DOI: 10.60836/1fr1-1c60

ARC Acknowledgement

This research was conducted by the ARC Centre of Excellence for Automated Decision-Making and Society (CE200100005), and funded partially by the Australian Government through the Australian Research Council

Australian Government
Australian Research Council

About ADM+S

The ADM+S is pleased to have this opportunity to engage with the Productivity Commission. The ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) is a cross-disciplinary, national research centre established and supported by the Australian Research Council to create the knowledge and strategies necessary for responsible, ethical, and inclusive automated decision-making (ADM). More information about ADM+S and its research may be found on our website, www.admscentre.org.au.

This submission is a product of The Regulatory Project, a signature project of ADM+S.

Authors: Jacky Zeng,[1] Kimberlee Weatherall,[2] Christine Parker,[3] Lina Przhedetsky,[4] Madeleine Stirling,[5] Henry Fraser,[6] Julian Thomas.[7]

This submission

This submission addresses **three of the four policy reform areas** in the Productivity Commission's inquiry into Pillar 3: Harnessing data and digital technology:

- Support safe data access and handling through an outcomes-based approach to privacy
- Unlock the benefits of consumer data through effective access rights and controls; and
- Enable AI's productivity potential.

The submission is the product of a collaborative process involving direct contributions from the above researchers from ADM+S. ADM+S researchers come from many different institutions, disciplines and perspectives. It should not be assumed that every contributing author, or every member of the Centre subscribes to every comment or recommendation made below. The submission represents our best effort to consolidate research and thinking in a way that can be useful to the Productivity Commission more generally. We would be very happy to engage further with the Commission into future stages of this important inquiry.

[1] Affiliate, ARC Centre of Excellence on Automated Decision-Making and Society (ADM+S) and Senior Research Assistant, the University of Sydney.
[2] Professor of Law, The University of Sydney and Chief Investigator, ADM+S.
[3] Professor of Law, The University of Melbourne and Chief Investigator, ADM+S.
[4] Research Fellow, The University of Melbourne Law School and ADM+S.
[5] Research Assistant, Melbourne Law School, The University of Melbourne.
[6] Lecturer, Queensland University of Technology Law School and Associate Investigator, ADM+S.
[7] Distinguished Professor, School of Media and Communication at RMIT University and Director, ADM+S.

Executive Summary

- Australia needs a regulatory framework that will build public confidence in data and technology and make it easier to unlock the benefits offered by new technology and AI. The right regulatory framework is not the only factor that will enable Australia to harness the potential of data and digital technology, but it is an important part of the picture.
- We endorse a shift in approach to digital regulation that is more outcomes-based and positively framed across all areas of digital reform.

Our current approach isn't working

- Australia's existing digital regulatory framework is the product of a fragmented patchwork of reforms resulting in laws that do not meet the expectations of the average Australian.
- Australia's piecemeal approach obstructs, rather than facilitates, the realisation of opportunities offered by new technology because it:
    - **inadequately protects consumers** from the broader risks of the algorithmic models that power these digital transformations. Consumers' trust that they are protected is an important driver of broader adoption;
    - **imposes unnecessary burdens on businesses** by multiplying regulatory complexity;
    - **puts too much reliance on policymakers** to update multiple laws, **and regulators** to monitor and enforce a growing web of bespoke rules; and
    - **significantly challenges civil society** to provide well-informed consumer representation.

What would work better?

- The government should make a shift towards a more outcomes-based, principles-based, and positively framed regulatory framework. This could mean:
    - In **privacy law**, 'returning to' and updating the *Privacy Act 1988* (Cth) (Privacy Act) as a priority measure. The government should action the principle-based proposals which have been accepted, but not yet legislated. These include: fair and reasonable processing, right to erasure, and a modernised conception of consent (without endless specification and detail).
    - In **content regulation**, a digital duty of care (drawing influence from the UK's Online Safety Act), or a due diligence approach (inspired by the EU Digital Services Act) that avoids legislating separate rules for each individual kind of content.
- AI regulation is a space where issues of fragmentation and incoherence are amplified. Different parts of government are producing multiple 'guidance documents' and there remains a distinct lack of clarity from government on what the road ahead may look like. Timely action is needed. We are happy to discuss further with the Commission what clarity could look like in the area of AI governance.

Our response

Regulatory certainty and consumer trust are key conditions for Australia to harness the opportunities of digital technology and AI, while avoiding or mitigating the risks of inappropriate adoption. Incoherent, overcomplicated regulatory frameworks risk chilling innovation and disincentivising Australian businesses, especially small and medium-sized enterprises (SMEs), from pursuing digital opportunities.

Australia's current regulatory approach to digital technology regulation is a fragmented patchwork of reforms. **We endorse a shift towards a more outcomes-based and positively framed regulatory framework that extends across all areas of digital reform.** This includes the Commission's consideration of regulatory reform in data protection (privacy) and artificial intelligence (AI), as well as other areas such as platform and content regulation.

Australia's focus on a series of specific issues (which it has dealt with by drafting detailed rules for those specific issues), has come at the cost of updating general, underlying data and consumer frameworks. This is creating regulatory complexity and burdens, without increased effectiveness. This submission discusses what outcomes-based and positively framed regulation could look like across privacy, AI, and platform regulation.

Australia's current approach is not working

Developments in digital technology – fuelled by data and epitomised by the current rise of Generative AI – are transformative forces that require thoughtful, strategic policy approaches. They affect every part of the economy. Without a focus on underlying common, general legal frameworks, there is a risk of proliferation of rules in different sectors, addressing slightly different issues in slightly different ways.

To the average Australian, digital regulation likely doesn't feel like it's "working": we see rising data breaches;[8] increasing concern about and significant losses from technologically-facilitated scams,[9] spreading adoption of privacy invasive technologies like facial recognition despite privacy commissioner and public concerns,[10] a large and concentrated data broking market where consumers have 'no meaningful control' over use of their data,[11] and AI-generated political advertising often unmoored from any relationship with truth.[12] Levels of trust in AI are low (and lower than elsewhere in the world);[13] concerns about privacy and data use are high.[14]

[8] OAIC, 'OAIC Stats Show Record Year for Data Breaches', *OAIC* (13 May 2025). Data breaches reported in 2024 rose by 25% compared to the previous year.

[9] G. Atta, 'How AI is being used to create sophisticated scams that leave even experts second-guessing', *ABC News*; National Anti-Scam Centre, 'Australians Better Protected as Reported Scam Losses Fell by Almost 26 per Cent' (Text, 11 March 2025). Although losses from scams were falling, the reported losses in 2024 were still $2B.

[10] 'Melbourne Council Wants Facial Recognition', *Information Age.*

[11] Australian Competition and Consumer Commission, *Digital Platform Services Inquiry 8th Interim Report - March 2024* (No 8, Australian Competition and Consumer Commission, 21 May 2024).

[12] S. Grantham, 'The AEC wants to stop AI and misinformation. But it's up against a problem that is deep and dark', *The Conversations*.

[13] N. Gillespie et al, *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025* (KPMG and The University of Melbourne, April 2025).

[14] OAIC, *Australian Community Attitudes to Privacy Survey 2023* (Office of the Australian Information Commissioner, 8 August 2023); See also, T. Northcott, et al, 'Unhealthy food advertising on social media: policy lessons from the Australian

Australia's approach is piecemeal

The incremental, piecemeal nature of Australia's approach to digital reform is a significant contributor to these issues. There has been no shortage of legislative action in response to high-profile issues, especially issues with high political valence, such as online child safety. But this approach, while active, lacks coherence and does not facilitate productive digital innovation. In some areas, legislative action has been too slow to make a difference; in other areas, rushed responses have resulted in incoherent laws and an over-reliance on consumers acting to try to protect themselves.

Government seems to have focused on legislative reforms targeting very specific harms, or types of data, across the fields of privacy/data, consumer protection, online safety, and copyright/content industries. Again and again, the government has sought to tackle a *specific* harm within a *specific* regime (see Appendix A for further detail). The picture is mixed, but overall, there *is* a pattern. Policymakers have failed to act to update core parts of the data and consumer frameworks with basic approaches that could make some of these detailed regimes needless, or at least, less complex.

For example, specific privacy (data) protections have popped up across multiple domains:

- The *Data Availability and Transparency Act 2022* (Cth) (DATA), which enables sharing of government data across government and with universities for government service delivery and research;
- The Consumer Data Right (CDR) (introduced 2019): an open banking regime designed to enable consumers to request service providers to share their data with other firms;[15]
- The *Digital ID Act 2024* (Cth): legislation for verification of identity without handover of copies of credentials; and
- The *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth), which involves age assurance for all social media users to limit some social media platform accounts to people over the age of 16.

In each case, concerns about data use and privacy arose in Parliamentary debate. In each case, rather than deal with privacy *generally* by updating the *Privacy Act,* new, specific, stronger privacy standards were written in and inserted into individual pieces of legislation. In many cases, similar or related reforms have been proposed as part of the general *Privacy Act Review*. Appendix B illustrates this point, juxtaposing specific additional protections with general reforms proposed by the recent *Privacy Act Review.* It shows how each act addresses the same issues separately, and differently – creating unnecessary proliferation and complication of rules. If, instead, the government had prioritised a more strategic, principled and overarching reform agenda for the Privacy Act, at least some of these specific rules would have been unnecessary.

Ad Observatory', *Health Promotion International*, Volume 40, Issue 2, April 2025; Hayden, Lauren, Newton, Giselle, Carah, Nicholas, Tran, Dang Khuong, Brownbill, Aimee, Obeid, Abdul, and Irving, Rohann (2024). How alcohol and gambling companies target people most at risk with marketing for addictive products on Facebook. Canberra, ACT, Australia: Foundation for Alcohol Research and Education.

[15] Competition and Consumer Act 2010 (Cth), Pt IVD Div 5.

Impacts: the complexity problem and its costs

The result of the lack of commitment to a coherent digital regulatory strategy is a patchwork of inconsistent legislative protections that see Australia's regulatory regime lagging behind that of similar nations. This causes problems for *everyone*.

A failure of protection for consumers

The current approach to digital regulation fails to adequately protect the consumer from the broader risks of algorithmic models that power Australia's digital transformations. Legislation such as the *Online Safety Act 2021* (Cth) attempt to address specific (and oftentimes extreme) risks – misinformation, abuse, hate speech, terrorism – while ignoring the pervasive everyday targeting of harmful products like alcohol, gambling, and risky financial services to vulnerable populations, including children.[16] Similarly, we can see both the CDR and Digital ID as highly specialised regimes within privacy that do little to address the common privacy concerns faced by individuals today such as the overcollection of personal information online and a lack of control over their personal information (beyond the scope of banking). [17] Australians still, across the economy, have no general legal right to complain of unfair commercial practices or unfair processing of their personal data, no right to require deletion of their personal data, no ability to withdraw their consent to businesses retaining their data.

Existing regulatory arrangements emphasise individualised harms. For instance, the dominant paradigm in the Privacy Act is of 'privacy self-management'.[18] The Act overwhelmingly focuses on the harms associated with collection and disclosure of information that could *identify* an individual. It attempts to mitigate these harms by providing transparency to individuals about how data is used, and requiring consent for many uses. However, this approach places an overwhelming burden on users navigating countless platforms. It also does not address the fundamental challenge now posed by algorithmic data processing. Algorithmic systems now make targeting inferences from aggregated datasets and behavioural patterns that don't require individual personal data collection, or the identification of individuals.

In the context of online safety, enforceable rules have been implemented to deal mostly with the removal of individualised harmful content – rather than creating general expectations on platforms to take steps to ensure positive online environments: like a digital duty of care, or due diligence (i.e. impact assessment and mitigation) obligation.

There is a disconnect, in other words, between the closed silos of our digital regulations and the systemics harms that consumers are experiencing every day.

[16] See e.g. Christine Parker et al, 'Addressing the accountability gap: gambling advertising and social media platform responsibilities' (2024) 32(4) *Addiction Research & Theory* 312 https://doi.org/10.1080/16066359.2023.2269852.
[17] Above n 14, 23-25.
[18] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126(6) *Harvard Law Review* 1880.

Unnecessary complexity for business

Secondly, this fragmentation leads to complexity, creating unnecessary regulatory burdens for businesses and organisations.

The burden of complexity is real, but it is important to think about how this plays out in debates. Australian policymakers are oftentimes faced with a significant paradox – industry stakeholders demand both regulatory certainty and flexibility for innovation. They criticise principles-based laws as too vague, while simultaneously condemning detailed rules as rigid red tape.[19] Australian policymakers have, understandably been more responsive to the demand for certainty: writing more rules that seek to address concerns raised during consultations; rules that are more detailed, but harder to apply.[20]

An example is the Government's response to the proposal to remove the small business exemption from the Privacy Act.[21] The proposed exemption would modify privacy rules for small business due to concerns about the regulatory burden posed by complex privacy law.[22] However, this would introduce a *different* kind of complexity: working out *which* rules apply, and when there is a shift from one set of rules to another. In fact, many small businesses are already bound by the Privacy Act obligations e.g. those involved in credit reporting and providing health services.[23] Add onto that, the potential for additional provisions of the CDR, Digital ID or DATA means that organisations have to decide when, for example, CDR data ceases to be CDR data and becomes 'regular' personal information. An entity that deals with both regimes might have to apply separate rules, or have separate systems. The proposed modification for small businesses will introduce yet another fragment to this tangle of data protection rules. The burden imposed on business in working out which privacy rules apply to them and dealing with confused consumers trying to enforce inapplicable rules is likely to outweigh any benefit of writing a separate set of rules.

[19] It is easy to be cynical: concluding that the real demand is for less rules and the resulting 'certainty' of an unregulated free-for-all all. Of course, that too would fail in promoting *either* certainty *or* innovation: Australia's creative regulators have responded to legislative stasis by using decades-old consumer protection laws to try to inch shut the gaping data maws of the platforms: *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367. Google was fined $60 million for breaching the statutory prohibitions on misleading and deceptive conduct: *Australian Competition and Consumer Commission v Google LLC (No 4)* [2022] FCA 942. Or see the Privacy Commissioner's use of existing privacy law against retail use of facial recognition: *Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy)* [2024] AICmr 230 (29 October 2024). Rather than be cynical, here we take seriously the expressed concern, but contest what is touted as the *answer* to the concern.

[20] See discussion B. Thom, 'The Curse of Cumulative Impacts', *Australian Coastal Society* (Webpage); R. Nelson, 'Breaking Backs and Boiling Frogs: Warnings From a Dialogue Between Federal Water Law and Environmental Law', (2019) 42(4) UNSW Law Journal 1179; R. Nelson, *Regulating a Thousand Cuts: Global Law and Policy Solutions to Cumulative Environmental Problems*, (2025) Cambridge University Press.

[21] Attorney-General's Department, *Privacy Act Review Report 2022*, (Report, February 2023).

[22] Australian Government, *Government Response Privacy Act Review Report*, (September 2023).

[23] Among many other cases as per *Privacy Act 1988* (Cth) s 6D. The government response to the Privacy Act Review proposes also that companies collecting biometric information and/or using facial recognition should also not be exempt.

Complexity and specificity hampers regulators

This piecemeal approach also excessively burdens policymakers and regulators to enact, maintain and enforce a growing web of reforms. The opacity of digital platforms raises serious hurdles to the monitoring and enforcement within each specific digital regulatory regime. Notably, the recent Tranche 1 Privacy Act reforms have introduced new enforcement powers for the Office of the Information Commissioner (OAIC) – such as coercive powers in relation to investigations, and the ability to undertake public inquires. While such developments are welcome, the OAIC is but one of many regulators who act in the broader remit of Australia's digital landscape. This means that each specific regime would potentially have to be reformed to provide specific powers of monitoring and enforcement for regulatory authorities, as has been proposed for the Australian Communications and Media Authority (ACMA), and canvassed for the Australian Competition and Consumer Commission (ACCC) and the Australian Securities and Investments Commission (ASIC). This is a process that places a heavy burden on policymakers not simply to create specific provisions reacting to particular substantive harms, but also to grant regulators powers for every new harm. Notwithstanding, such reforms may not even be effective. They do not provide a consistent and clear framework for the public and relevant authorities to understand and respond to predictive consumer modelling and targeting.[24]

Fragmentation significantly challenges civil society

Lastly, we note that another set of actors face significant challenges from this fragmentation and complexity: civil society. The volume of work, the complexity of the policy/regulatory issues and the fragmentation of consumer interests all present barriers to well-informed consumer representation in this area. This is a problem exacerbated by the fact that unlike other significant domains (such as telecommunications and energy), there is no consumer organisation funded to address consumer issues relating to the digital platforms. This makes the case for consideration of how consumer representation can be better funded – for example through an industry levy – while simultaneously arguing against the current piecemeal approach to reform.

What should we do?

In light of the discussion above, we **endorse a shift in digital regulatory reform, towards a more holistic and outcomes-based approach**. Importantly, we think that reforms should be made to introduce a positively framed regulatory framework which shifts the onus away from customers and regulators, and towards the organisations who collect and handle the data; and who are almost always in the best position to mitigate related harms.

In **privacy** this shift means 'returning to' and updating the Privacy Act as an urgent regulatory priority. We are in favour of the principle-based proposals – such as modernising the concepts of personal information and consent; the introduction of the right of erasure and enhanced access and transparency rights – which the

[24] N. Carah & S. Brodmerkel (2021), Alcohol Marketing in the Era of Digital Media Platforms, *Journal of Studies on Alcohol and Drugs*, *82*(1), 18–27.

Government have agreed in-principle but were not enacted in Tranche 1.[25] The most promising of these proposals in the introduction of a 'fair and reasonable' test which places a positive onus on businesses to ensure that their use and handling of personal information is fair and reasonable in the circumstances. This directly addresses several impracticalities of our current framework, which requires individuals to largely self-manage their privacy in a world of increasingly complex data processing activities (e.g. screen scraping and AI) and 'dark patterns' which may nudge users towards consenting to more privacy intrusive practices.[26] Fairness and reasonableness are both concepts that are broadly understood; capable of being flexible over time; and well-grounded in Australian legal frameworks.[27] A holistic focus on the core issues underlying privacy should enable streamlining of other regimes (CDR, Digital ID etc.) further down the line.

In the sphere of **content regulation**, we have seen promising announcements from the federal government to enact a digital duty of care,[28] a measure recommended by both the Joint Select Committee on Social Media and Australian Society[29] and the review of the Online Safety Act.[30] It is expected that the duty would require companies to conduct regular risk assessments to proactively identify harmful content and take reasonable steps to avoid or mitigate against harm.[31] Broadly, the measure has been praised for its unified approach with the UK's Online Safety Act and the EU's Digital Services Act – which offer two similar but distinct approaches: [32]

- **UK's Online Safety Act** – introduces a pluralistic **digital duty of care** – prescribing different obligations for different types of services: user-to-user platforms; search engines and messaging services. [33]
- **EU Digital Services Act** – introduces a **due diligence approach** that is broader than the UK's duty of care model and emphasises not only risk assessment and mitigation but also overall platform transparency, accountability, and the protection of human rights in the digital space. [34]

Critics of the UK's pluralistic duty of care model have argued for Australia to enact a singular duty of care, which would take a systems-first approach over a content-first approach, encouraging platforms to safeguard their systems before harm even occurs. [35] Consistent with the argument in this submission, we agree.

---

[25] Above n 22.
[26] Ibid.
[27] See e.g. Firms providing certain financial services, for example, are subject to a requirement to act 'efficiently, honestly, and fairly' in the provision of those services to consumers. See K. Weatherall et al., *Submission to the Privacy Act Review Discussion Paper*, (January 2022). See also Henry Fraser and José-Miguel Bello y Villarino, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough' (2024) 15 *European Journal of Risk Regulation* 431 http://dx.doi.org/10.1017/err.2023.57.
[28] M. Rowland MP, 'The governance of digital platforms', *The Sydney Institute* (Speech, 13 Nov 2024).
[29] Commonwealth of Australia, 'Social media: the good, the bad, and the ugly', *Joint Select Committee on Social Media and Australian Society* (Final Report, November 2024).
[30] eSafety Commissioner, 'eSafety Statement on the Online Safety Amendment (Social Media Minimum Age) Act 2024' (Media Release, December 2024).
[31] Above n 28.
[32] L. Given., 'Australia will impose a 'digital duty of care' on tech companies to reduce online harm. It's a good idea – if it can be enforced', *The Conversation* (Article, November 2024).
[33] *The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025* (UK).
[34] European Commission, *The Digital Services Act*, (Website) and P. Leerssen, 'Counting the days: what to expect from risk assessments and audits under the DSA–and when?' (2023).
[35] Reset.Tech Australia, The Victorian Bar and the Law Society of NSW each argued for this approach in their submissions to Delia Rickard's review of the Online Safety Act 2021.

AI regulation

AI regulation is a space where these issues are amplified. Although we have no clear rules of the road ahead, multiple 'guidance documents' are being produced by different parts of government: a detailed, but entirely voluntary AI Safety Standard is offered (which the government itself is not following);[36] a National AI Assurance Framework regarding use of AI in government, based on Australia's 8 AI Ethics Principles[37] has been released for the public sector which is inspired by the NSW AI Assessment Framework which applies separately to the NSW public sector.[38] In 2024 the Australian government have consulted on a set of 10 Mandatory AI Guardrails for high-risk uses of AI that loosely overlaps, but are not clearly aligned with the aforementioned 8 AI Ethics Principles.[39] There remains a distinct lack of clarity from government about what approach it intends to take. It is entirely unclear whether Australia's AI regulation will be furthered through the use of AI Ethics Principles, a general risk-based approach, or domain-specific rules.

Consistent with the argument in this submission, we think it is a mistake to develop out detailed, domain specific rules, rather than paying attention to underlying general frameworks. An outcomes-based and positive framework would look more like the mandatory guardrails: requiring firms implementing AI to identify high-risk use cases and systems, take steps to mitigate the risks, and conduct ongoing monitoring. We are happy to discuss further.

We appreciate that policymakers face difficult questions in relation to determining the substance, form and scope of AI regulation; effective monitoring and enforcement mechanisms and how it should interact with our existing laws. However, the fragmented state of Australia's current AI regulation is insufficient to address emerging risks; perpetuates regulatory ambiguity that impedes business planning, and could undermine competitive advantages in the global AI economy. Timely action is needed.

[36] Department of Industry, Science and Resources, *Voluntary AI Safety Standard*, (Paper, September 2024).
[37] Department of Industry, Science and Resources, *Australia's AI Ethics Principles*, (Publication, 2019); Australian Government et al., *National framework for the assurance of artificial intelligence in government*, (2024)
[38] NSW Government, *NSW Artificial Intelligence Assessment Framework*, (
[39] Department of Industry, Science and Resources, *Proposals Paper for Introducing Mandatory Guardrails for AI in High-Risk Setting*, (2024).

Appendix A – Unfinished business in digital regulatory reform

Actioned	Proposed or canvassed but unactioned
Specific privacy reforms: • Children's Privacy Code (drafting underway) • Individual right of action for intentional or reckless serious invasions of privacy; • Anti-doxxing: criminal offence for menacing or harassing online communication of personal information of individuals or racial/religious and other groups • More enforcement powers for OAIC; making it easier for OAIC to pursue civil penalties. • Consumer Data Right (Open Banking) • The Digital ID Act.	General 'Tranche 2' privacy reforms, including:[40] • Expanding the general **scope of application** by expanding the definition of personal information and removing the small business exemption • Expanding basic obligations from fairness in *collection* to require that *use and disclosure* be 'fair and reasonable in the circumstances' (not just 'relevant to what the business does') • Baseline security requirements • Privacy impact assessments for activities with high privacy risks.
Specific consumer protections: • Scams Prevention Framework Act: principles-based obligations for intermediaries to detect, disrupt, prevent, report scams; information sharing. No liability. • Expansion of the unfair contract terms regime - including expanding contracts treated as 'standard'; expansion of offences; more businesses can complain.	General consumer protection reforms: • Unfair trading practices including provisions against dark patterns • Consumer-oriented competition prohibitions (e.g. anti-tying; anti-preferencing) Consumer guarantees (product safety provisions), including mechanisms for allocating liability for faulty AI-enabled goods.[41]

[40] The dot points here are limited: the *Privacy Act Review* made 116 proposals (some with multiple parts); the government agreed to 38 and agreed in principle to 68. These points highlight certain substantive, general proposals expected to be enacted in some form.

[41] Department of the Treasury, *Review of AI and the Australian Consumer Law* (Discussion Paper, Treasury, 12 December 2024) <https://treasury.gov.au/consultation/c2024-584560>.

	Digital competition regime.[42]

Online safety reforms:
• Takedown of individual examples of material that breaches communications standards (crime, terrorism, extremism, and R+ type material) or targets individuals (cyberbullying, intimate image abuse etc).
• (non-enforceable) Basic Online Safety Expectations (BOSE)[43]
• Kid's Social Media Ban
	General online safety reforms:
	• Platform duty of care[44]
	• Mis/disinformation – 2024 abandoned reforms: requiring platforms to:
	  ○ Address seriously harmful content with measures addressing algorithms, bots, fake accounts, malicious deep fakes, advertising and monetisation;
	  ○ Publish risk assessments, policies, reports; data access for researchers;
	  ○ Provide complaints and dispute procedures for content moderation
	  ○ Give ACMA power to develop/register codes of practice

Some specific AI reforms: • Obligation to explain how data is used in ADM systems in privacy policies (Privacy Act reform) • Federal government only: binding policy obligation for departments/agencies to publish general statement on use of AI and identify an accountable official.	General regulation of Artificial Intelligence and automated decision-making systems: • Mandatory guardrails addressing general standards for development, deployment

[42] The Treasury, *Digital platforms – a proposed new digital competition regime*, (Consultation paper, December 2024).

[43] The *Online Safety Act* also includes "Basic Online Safety Expectations" (BOSE), which outline the Australian Government's expectations that social media, messaging and gaming service providers and other apps and websites will take reasonable steps to keep Australians safe.

[44] It is also worth noting that there are a range of other *specific* harms where consultation about general online safety (or perhaps health and safety) has occurred but not yet been actioned: these include consultations on online gambling marketing reforms (proposed, and strongly supported), and a consultation on laws to prohibit online unhealthy food advertising. ADM+S has undertaken research showing the importance of some of these issues in online environments; consistent with the argument in this paper we would suggest issues of this kind can be brought within a model of a digital platform duty of care or EU-style due diligence approach – where there can be one legal framework guiding positive duties to take proportionate action in relation to a range of harms.

	• A right to meaningful information about substantially automated decisions with legal or similarly significant effect • Response on transparency and regulation of ADM proposals from the Robodebt Royal Commission (Recommendation 17.1, 17.2)
Content generation in news: • News Media Bargaining Code: an attempt to force payment for one specific type of creative content used by platforms (news).	General content generation: • Copyright reform: there have been general noises in the direction of reform in light of AI: albeit no details or proposals as yet.

Appendix B – Fixing the Privacy Act, one kind of data at a time[45]

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
Legislation	*Data Availability and Transparency Act 2022* (Cth)	*Competition and Consumer Act 2010* (Cth) Pt IVD, inserted by *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth)	*Digital ID Act 2024* (Cth)	*Online Safety Act 2021* (Cth) Pt 4A, inserted by *Online Safety Amendment (Social Media Minimum Age) Act* 2024	n/a
What is the Act about?	Accreditation and sharing regime for government-held data between government entities and with universities for delivery of govt services, informing govt policy and programs, and R&D.	Accreditation and sharing scheme for data about consumers and their transactions held by private actors in certain industries (currently banking), to enable consumer to direct sharing with accredited entities to offer services to consumer.	Aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.	To put in place age restrictions for certain social media platforms; provider of such a platform must take 'reasonable steps' to prevent children who have not reached the minimum age from having accounts. Privacy provisions were strengthened in amendments made during Parliamentary consideration.	n/a

[45] There are multiple other Acts with specific privacy provisions – see e.g. legislation relating to My Health Record.

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
Broader definition of personal information		Broader and narrower. Pt IVD applies to 'CDR data', which is data: • Falling within specified types set out in rules • That 'relates to' a CDR consumer, for a CDR action (or information wholly or partly derived from CDR data) (Note also CDR customer can be a corporate entity). At least one person (/CDR consumer) must be reasonably identifiable from the data.	'personal information' extends to 'attributes' of a person (s 35). An 'attribute' is 'information that is associated with the individual, and includes information that is derived from another attribute' (s 10)	The Act is not confined to personal information, but does deal with collection and use of information in the process of age assurance.	**Proposal 4.1** Change the word 'about' in the definition of personal information to 'relates to'.
Special rules for sensitive data and govt identifiers		n/a. On one view CDR data is treated a bit like sensitive data, with additional protections and requirements for consent.	Some sensitive information is prohibited from being collected under scheme: Racial/ethnic origin, political opinions, political memberships, religious beliefs/ affiliations, philosophical beliefs, sexual orientation/ practices (s 44). Others (health, government	Govt identifiers cannot be used to do age verification/ age assurance: s 63DB – unless other options are also available. Digital ID Act methods can only be used if other options are offered.	

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
			identifiers) are treated as 'restricted attributes' (s 11).	Large penalties to guard against platforms using the minimum age obligation to capture large amounts of official government identification from users	
Special rules for biometric data	Biometric data cannot be shared without consent	No	Dealt with in Accreditation Rules. Biometric info can only be collected where entity is accredited to collect biometric data and only used in accordance with Accreditation Rules, and only to verify/authenticate identity (and for testing/ improving tech for doing so) (ss 48-49A). Special rules for govt verification (s 50)	On the contrary: Supplementary EM explicitly calls out 'user interaction or facial age estimations' as 'reasonable methods' for age assurance.	**Proposal 13.2** Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies
Extension to small businesses	Commercial entities can't use scheme.	Use of system requires accreditation.	Small business that is accredited is bound by *PA* (although rules under Digital	Specific prohibitions on collection and use of	**Proposal 6.1** Remove the small business exemption after

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
	Entities engaged in data sharing must be covered by *PA*, or term in the data-sharing agreement that requires compliance with *PA*		ID Act can make modifications) (s 35A). *PA* or equivalent must apply somehow, eg through agreement with Cth (s 36)	personal data apply to any covered entity.	appropriate consultation, and with appropriate support.
Stronger requirements for consent	Not designed for dealing with individuals. Similar to *PA*. Sharing can occur where in public interest without consent.	Yes. Giving of consent occurs under detailed CDR Rules, which have object of ensuring consents are voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn. Rules set out how to achieve these goals. E.g. consents can only last 12 months.	When verifying identity, express consent from individual required for verifying entity to disclose current/former name; address; DOB; phone number; email (s 45). Similar rule for health info; government identifiers (s 46).	Data collected for age assurance cannot be used for another secondary purpose unless with consent, permitted/required by law, or permitted situation under *PA:* s 63F(1) Consent must be voluntary, informed, current, specific and unambiguous: s 63F(2)	**Proposal 11.1** Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous. **Proposal 11.2** The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context.
Withdrawal of consent	n/a	Yes; withdrawal must be possible and there are	Yes, Digital ID must be deactivated on request.	Yes: s 63F(2)(b). Individual must be able	**Proposal 11.3** Expressly recognize the ability to

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
		detailed rules/systems to facilitate this (see rule 4.14)		to withdraw consent in manner that is easily accessible to the individual.	withdraw consent, and to do so in a manner as easily as the provision of consent.
Voluntariness of data-using system	n/a	Yes: system is based on consent.	Yes; alternatives must be offered.	No. Any individual with an account with an applicable system will have to do age assurance.	n/a
Tracking and marketing limits	Commercial entities and purposes are excluded from the scheme. Data-sharing is between government entities, and by universities for research.	CDR data can be used for direct marketing only with specific direct marketing consent.	• Rules limiting disclosure of unique identifiers across different participating entities (s 47). • Prohibition on using or disclosing info about services individual used, how, when (s 53 – 'Data profiling to track online behaviour is prohibited'). • Prohibition on using information for marketing, promotion except	Data collected for age assurance cannot be used for another secondary purpose unless with consent, permitted/required by law, or permitted situation under *PA:* s 63F(1). This excludes usual *PA* rule allowing 'reasonably expected' uses.	Treat IP addresses and device identifiers as personal information; personal information present when a person can be 'individuated' (distinguished from all other individuals). **Proposal 20.2** Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. **Proposal 20.3** Provide individuals with an unqualified right to opt-out of receiving targeted advertising

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
			with express consent (s 55)		**Proposal 20.8** Targeting should be fair and reasonable **Proposal 20.9** Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals
Stronger purpose limitations	Only used for certain purposes: • Govt service delivery • informing govt policy and programs • R&D	Yes: significant additional restrictions in both the Act and the separate CDR rules. Additional safeguards such as having to notify CDR consumers if CDR data is disclosed.	Limits against use in enforcement unless proceedings against the person have started, or with warrant or consent (s 54)	See above – data cannot be used for other purposes unless with consent; stronger definition of consent	
Data minimisation rules	Sharing of personal information in data-sharing – some rules requiring only minimum amount be shared (unless consent or some	Yes. Data Minimisation Principle (CDR Rules Rule 1.8): CDR participant must not collect more CDR data than is reasonably needed; or	Yes. Arguably whole system is a data minimisation exercise: intended to ensure personal information need	Communications Minister can make legislative rules to exclude certain kinds of information being collected by platforms to	Could be seen as related to/overlapping with proposal to require that data collection, use and disclosure be 'fair and

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
	other *PA*-consistent exception)	CDR data that relates to a longer time period than is reasonably needed in order for it, or a relevant CDR representative, to provide the goods or services requested by the CDR consumer	not be collected for identity verification. Also: certain attributes cannot be collected.	do age verification: s 63DA.	reasonable in the circumstances'. Existing collection principle APP3 requires that information be reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
Rules on deletion/erasure	Data-sharing agreements must deal with project duration and what happens to scheme data at end of project (s 19)	Destruction on request of CDR consumer: s 56BAA Obligation to ensure that CDR data no longer needed or able to be used consistent with Division must be de-identified or destroyed. CDR rules specify the steps to be taken (not just 'reasonable steps' per *PA*).	Biometric data collected for verification must be destroyed immediately that purpose is complete (s 51) Identity exchanges must not retain information (s 56)	Personal information must be destroyed after being used for purpose: s 63F(e)	**Proposal 18.3** Introduce a right to erasure so that an individual may seek to exercise the right to erasure. **Proposal 18.8** An APP entity must provide *reasonable assistance* to individuals to assist in the exercise of their rights. **Proposal 18.9** An APP entity must take reasonable steps to respond; refusal of a request should be accompanied by an explanation for the refusal and information

Type of amendment	Data Availability and Transparency Act	Consumer Data Right	Digital ID Act	Social Media Minimum Age Act	Anything similar proposed in Privacy Act Review?
					on how an individual may lodge a complaint regarding the refusal with the OAIC.
Data breaches	Reasonable steps must be taken to prevent or reduce harm from data breach (s 36). Pt IIIC of *PA* applies (s 37)	Brought within *PA:* s 56ES – so data breach provisions apply to CDR entities and CDR data.	Brought within *PA:* s 39 (this does not apply to entities bound by state privacy laws, which must give Digital ID Regulator and OAIC any statement they make to their own authorities)		**Proposal 28** outlines a range of actions on data breaches, including suggesting that the government should consider requiring entities to take reasonable steps to reduce or prevent harm from a data breach (similar to DATA).