Reset.
AUSTRALIA

Digital Platform Regulation Green Paper

April 2024

Reset.
AUSTRALIA

Contents

About this paper

This paper is designed to provide a briefing for public interest organisations around recent movements on, and opportunities, for digital regulation in Australia. It lays out Reset.Tech’s perspectives around what comprehensive, preventative digital regulation should look like. It is intended to be a living document for Reset.Tech, so should be read as documenting a unique moment in policy time in Australia.

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

Reset.
AUSTRALIA

Australian digital regulation: the story so far

Australia has a proud history as a 'first-mover' and innovator on digital platform regulation. Australia was the first country to legislate for online safety and introduce an online safety commissioner,[1] as well as the first to legislate for negotiations between digital platforms and news providers.[2] Analysis from the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry Final Report*[3] continues to influence cutting-edge policy thinking locally and internationally.[4]

Yet in the intervening years, Australia has slipped behind on digital regulation, with digital threats evolving and scaling up in ways that seemed almost unimaginable only a few years ago. New risks, driven by increasingly-powerful algorithms and an explosion of data harvesting, have now surpassed the ability of existing digital regulatory frameworks to effectively manage them. Australia is not alone in facing these risks, but other countries are now making substantial progress, in particular the UK[5] and the EU,[6] with emerging progress in Canada.[7] These jurisdictions have drawn upon the innovations and exemplars of Australian policy innovation but introduced more comprehensive, preventative, and muscular regulatory models. These models encourage platform conduct that ensures user safety and is more commensurate with public expectations for digital regulation more broadly. By contrast, Australia is still largely reliant on a hopeful but outdated desire for industry-led and largely self-regulated processes.

Harm happens as governments wait for self-regulation and co-regulation to fail. Nine years on from the first online safety legislation, and five years on from the 2019 ACCC Inquiry, Australia has a new government and faces new digital challenges. A non-exhaustive list includes:

- Personalised and persistent scam calls, texts, and advertisements, linked to digital advertising business models and causing significant economic harm to Australians;[8]
- Ongoing risks of online harms for children,[9] including online exploitation;[10]
- Increasing cyber abuse directed at adults, especially women[11] and hate speech directed at minorities;[12]

---

[1]Via the *Enhancing Online Safety for Children 2015* Act
https://www.legislation.gov.au/C2015A00024/2017-06-23/text
[2]Via the *News Media and Digital Platforms Mandatory Bargaining Code 2021*
https://www.legislation.gov.au/C2021A00021/asmade/text
[3]Australian Competition and Consumer Commission's *Digital Platforms Inquiry Final Report* 2019
https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report
[4]For example, see UK Parliament 2024 *Digital Markets, Competition and Consumers Bill*
https://bills.parliament.uk/publications/54208/documents/4421 & Government of Canada 2020 *Towards guiding principles — Diversity of content in the digital age*
https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age/towards-guiding-principles.html & Government of Canada 2021 *News Media Canada*
https://ised-isde.canada.ca/site/strategic-policy-sector/en/marketplace-framework-policy/copyright-policy/submissions-consultation-modern-copyright-framework-online-intermediaries/news-media-canada-nmc,
[5]UK 2023 *Online Safety Act 2023* https://www.legislation.gov.uk/ukpga/2023/50/enacted
[6]EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[7]Canada 2024 *Online Harms Bill 2024* https://www.parl.ca/LegisInfo/en/bill/44-1/c-63
[8]National Anti-Scam Centre 2023 *National Anti-Scam Centre in Action Quarterly Update*
https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update/national-anti-scam-centre-quarterly-update-march-2024 & Consumer Policy Research Centre 2024 *Singled Out*
https://cprc.org.au/wp-content/uploads/2024/02/CPRC-Singled-Out-Final-Feb-2024.pdf
[9]Ranging from Ed Tech apps that breach student's privacy (see Human Rights Watch 2022 *"How Dare They Peep into My Private Life?"*
https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments) to algorithms that serve them pro-eating disorder content (Reset.Tech Australia 2024 *Not Just Algorithms*
https://au.reset.tech/news/report-not-just-algorithms/)
[10]eSafety Commissioner 2022 *World-first report shows leading tech companies are not doing enough to tackle online child abuse*
https://www.esafety.gov.au/newsroom/media-releases/world-first-report-shows-leading-tech-companies-are-not-doing-enough-to-tackle-online-child-abuse
[11]eSafety Commissioner 2022 *Women In The Spotlight: How online abuse impacts women in their working lives*
https://www.esafety.gov.au/research/how-online-abuse-impacts-women-working-lives
[12]See for example, the experience of Indigenous Australians during the Voice referendum at Jack Latimore 2023 'Meta rules online racism against Indigenous people meets community standards' *The Sydney Morning Herald*

- Vast and invasive data breaches, exacerbated by Australia's weak privacy and data protection laws, widening existing holes in national security and personal security;[13]
- Implementation challenges over the *News Media Bargaining Code*, with Meta's exit from the deals threatening a loss of over $100m to the Australian news market;[14]
- A deteriorating information environment, with upticks in 'fringe' and palpably false content, including a rise in AI-generated content with unclear provenance;[15]
- Governance challenges to DIGI's *Australian Code of Practice on Misinformation and Disinformation*, with X (formerly known as Twitter) exiting the Code after routine failures to respond to independent reports of serious breaches;[16]
- Deepening national security threats of ideologically motivated extremism,[17] with intensifying links to content recommender systems (or algorithms).[18]

Over the last decade, governments at home and around the world have also learned that:

- Voluntary or at best co-regulatory schemes do not produce high quality protections for Australians,[19] and can simply be ignored by platforms. They rely on creating 'reputational risks' where platforms violate them and there are limits the 'reputational risk' approach;[20]
- Even legislation and fine regimes are vulnerable to dismissal by very large platforms, if they are not considered significant enough;[21]

---

https://www.smh.com.au/national/meta-rules-online-racism-against-indigenous-people-meets-community-standards-20230815-p5dwqt.html

[13]Office of the Australian Information Commissioner 2024 *Notifiable data breaches report* https://www.oaic.gov.au/__data/assets/pdf_file/0021/156531/Notifiable-data-breaches-report-July-to-December-2023.pdf & Reset.Tech Australia 2023 *Australians for Sale Targeted Advertising, Data Brokering, and Consumer Manipulation* https://au.reset.tech/news/coming-soon-australians-for-sale-report/

[14]The Hon Michelle Rowland MP, Minister for Communications 2024 *Press Conference* https://minister.infrastructure.gov.au/rowland/interview/transcript-press-conference-sydney-0 & Rod Sims 2022 'Australia's News Media Bargaining Code led the world. It's time to finish what we started' *The Conversation* https://theconversation.com/australias-news-media-bargaining-code-led-the-world-its-time-to-finish-what-we-started-188586

[15]Tom Rogers 2023 ''Highest level of mis-and-disinformation we've seen online': AEC' *Australian Broadcasting Corporation* https://www.abc.net.au/listen/programs/radionational-breakfast/aec-on-referendum-education-campaign-and-misinformation-/102758190; Pranshu Verma 2023 'The rise of AI fake news is creating a 'misinformation superspreader' *The Washington Post* https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation/

[16]Digital Industry Group Inc. 2023 *Media Statement* https://digi.org.au/category/media-statement/

[17]Australian Security Intelligence Organisation 2022 *Director General's Annual Threat Assessment* https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2022 & Australian Security Intelligence Organisation 2023 *Director General's Annual Threat Assessment* https://www.asio.gov.au/director-generals-annual-threat-assessment-2023 & Australian Security Intelligence Organisation 2024 *Director General's Annual Threat Assessment* https://www.oni.gov.au/asio-annual-threat-assessment-2024

[18]Reset.Tech Australia 2022 *Algorithms as a weapon against women: How YouTube lures boys and young men into the 'Manosphere'* https://au.reset.tech/news/algorithms-as-a-weapon-against-women-how-youtube-lures-boys-and-young-men-into-the-manosphere/ & Manoel H Ribeiro *et al.* 2019 *Auditing Radicalization Pathways on YouTube* https://www.researchgate.net/publication/335337464_Auditing_Radicalization_Pathways_on_YouTube

[19]Reset.Tech Australia 2022 *How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot* https://au.reset.tech/uploads/report_-co-regulation-fails-young-people-final-151222.pdf

[20]Tess Bennett 2024 'Social media giants 'no longer fear reputation risks' *AFR* https://www.afr.com/technology/social-media-giants-no-longer-fear-reputation-risks-20240422-p5flls

[21]eSafety Commissioner 2023 *eSafety demands answers from Twitter about how it's tackling online hate* https://www.esafety.gov.au/newsroom/media-releases/esafety-demands-answers-from-twitter-about-how-its-tackling-online-hate

- Meaningful platform transparency requires significant legislative incentives, such as prescriptive reporting requirements[22] and data-enabled avenues for independent, external scrutiny of platform systems;[23]
- The threat of significant fines does shift platform behaviour, such as prompting cautionary investments in 'trust and safety' personnel.[24]

The common thread between these regulatory challenges is the need for a systemic focus, and for transparency and accountability. To meet best-practice digital platform regulation Australia needs to 'write in' a systemic focus with transparency and accountability mechanisms. This need not require massive new packages. Rather, there are timely and achievable opportunities taking place in live policy processes, including, coalescing opportunities within the domain of online safety and misinformation and disinformation policy, with linkages into privacy and data protection.

The purpose of this paper is to provide a timely thought-piece. It identifies some emerging opportunities in the digital regulatory space, although it is not intended to be a total review of the Australian policy landscape. It also identifies some emerging thinking from Reset.Tech about a potential direction of travel for these policy discussions. These are presented here as 'food for thought' to encourage discussion as these rapid policy discussions emerge.

[22]Otherwise, transparency reports become "vague". (See for example Uri Gal 2022 'Transparency reports' from tech giants are vague on how they're combating misinformation. It's time for legislation' *The Conversation* https://theconversation.com/transparency-reports-from-tech-giants-are-vague-on-how-theyre-combating-misinformation-its-time-for-legislation-184476), The EU and UK have requirements for specific types of information to prevent this (see Recital 65, EU 2022 *Digital Services Act* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065 & Section 20, UK 2023 *Online Safety Ac*t https://www.legislation.gov.uk/ukpga/2023/50/enacted)

[23] See for example John Albert 2022 'A guide to the EU's new rules for researcher access to platform data' *Algorithm Watch* https://algorithmwatch.org/en/dsa-data-access-explained/, which explains researcher access requirements as laid out in article 40, EU 2022 *Digital Services Act* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065, In the UK, Chapter 7 Section 162 of the Online Safety Act describes how the UK is developing its researcher access scheme (UK 2023 Online Safety Act https://www.legislation.gov.uk/ukpga/2023/50/enacted)

[24] European Commission 2023 *The impact of the Digital Services Act on digital platforms* https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

Current policy dynamics

Years of digital platform regulation preparation and review across a range of policy domains could 'come to a head' very soon. Significant policy processes, including the long-awaited *Privacy Act* Review, the Amendment Determination of the *Basic Online Safety Expectations*, and the expedited review of the *Online Safety Act* are overlapping and opening a window for genuine harmonisation across typically fragmented policy areas.

The present regulation gap for misinformation and disinformation may be filled by the *Combatting Misinformation and Disinformation Bill*, and the latest setback regarding Meta's cooperation under the *News Media Bargaining Code* may prompt the government to legislate for more robust platform engagement on issues of digital content and value exchange. A non-exhaustive list of policy movements and consultation is presented in Figure 1.

Process	Potential significance	Status
Amendments to the Basic Online Safety Expectations Determination	Enhanced focus on systems and elements, or features of digital platform design, that create risks, moving further away from a notice and take down approach	Consultation closed in February 2024,[25] awaiting report
Statutory review of the *Online Safety Act*	A potential broadening of systemic responsibilities through the introduction of a Duty of Care, and an opportunity to revising transparency and accountability mechanisms	The terms of reference for the review have been released.[26]Currently awaiting consultation, expected date of final report October 2024
Review of the *Privacy Act*	Better protections for personal data, including metadata, and stronger requirements around fairness and reasonableness to justify data processing, including by digital platforms	Initial proposals were responded to by the Government in September 2023,[27] and we are currently awaiting information regarding implementation
Proposals for a *Combatting Misinformation and Disinformation Bill*	At minimum, providing a regulatory 'backstop' to the industry-led and industry-managed Code of Practice on Misinformation and Disinformation via information-gathering powers for the Australian Communications and Media Authority. Ideally, encouraging a transparency scheme including third-party public interest data access to widen accountability-based interventions on platform conduct.	Consultation closed in August 2023,[28] but there are active discussions about the next steps
Digital Platforms Services Inquiry 2020-2025	Specific amendments to tackle systemic market imbalances, and the potential for specific interim reports addressing 'joined up' and overarching issues that fall outside the scope of specific legislative reviews	Ongoing,[29] final report due in March 2025
Safe and Responsible AI Consultation	Requirements for safeguards for developing or deploying high risk AI systems, and voluntary AI standards for lower-risk and general use AI. There are also suggestions for transparency and accountability measures	The consultation closed in August 2023, and the Government has announced their interim response.[30] Awaiting next steps
Supplementary legislation to the *News Media Bargaining Code*	Amendments or supplements to the legislation could address the enforceability challenges revealed by Meta's recent conduct and also consider new value exchange problems created by large language models	Not announced

Figure 1: A non-exhaustive list of digital policy consultations and dynamics at the time of publication

[25]Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2023 *Online Safety (Basic Online Safety Expectations) Amendment Determination 2023* https://www.infrastructure.gov.au/have-your-say/online-safety-basic-online-safety-expectations-amendment-determination-2023
[26]Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2024 *Terms of Reference – Statutory Review of the Online Safety Act 2021* https://www.infrastructure.gov.au/sites/default/files/documents/tor-statutory-review-online-safety-act-2021-8Feb.pdf
[27]Attorney-General's Department 2023 Government response to the Privacy Act Review Report https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report
[28]Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2023 *New ACMA powers to combat misinformation and disinformation* https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation
[29]Australian Competition and Consumer Commission 2020 *Digital platform services inquiry 2020-25* https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25
[30]Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2024 *The Australian Government's interim response to safe and responsible AI consultation* https://www.industry.gov.au/news/australian-governments-interim-response-safe-and-responsible-ai-consultation

Reset.
AUSTRALIA

Proposals for systemic regulation

While each policy discussion will have its own nuances and paths to follow, at Reset.Tech we have been thinking more broadly about what one approach to comprehensive digital regulation could look like, with a particular focus on online safety and misinformation and disinformation.

Over the page, we propose a '5 Pillars' model to achieve comprehensive safety, transparency, and accountability for digital platforms in Australia (see Figure 2), and note how for children and young people in particular, the introduction of the 'children's best interests' principle across a range of policy reforms could help to start harmonising approaches.

Our focus in the framework is online safety, but we note there are many ways to go about building a comprehensive framework for managing digital risks, including through consumer and competition domains.

5 pillars for addressing systemic risks

There are five key pillars that could be introduced across the regulatory framework.

1. A duty of care shaping platforms' actions	2. Requirements for risk assessments	3. Requirements for risk mitigations	4. Requirements for transparency measures	5. Requirements for accountability measures
An overarching duty of care would place broad obligations on platforms to ensure user safety in systemic ways. Specific responsibilities could be enumerated by focusing requirements for risk assessments. The UK OSA[31] introduces duties of care, and draft Canadian legislation[32] introduces duties on services; however, both are pluralised, which reduces the systemic focus. The EU's DSA[33] regulations have similar systemic obligations but are phrased as responsibilities to address particular risks, specifically risks posed by: ● Illegal content ● Negative effects for the exercise of fundamental rights, such as dignity and privacy and political freedoms, as outlined in the European Charter ● Negative effects on civic discourse and electoral processes and public security ● Negative effects on gender-based violence, public health, children's wellbeing and serious negative consequences to people's physical and mental wellbeing.[34]	Requirements for platforms to assess *all their systems and elements* for risks would incentivise systemic change and help platforms realise their duty of care. Risk assessments could be focused on addressing the following: ● Illegal materials (such as class 1A & 1B materials as already included in the *Online Safety Act*) ● Harmful materials (such as image-based abuse, abhorrent violent material, cyberbullying of children and abuse of Australian adults as already included in the *Online Safety Act*) ● Online scams ● Risks to electoral processes and public security ● Risks to human rights, such as political freedoms, hate speech and violence or serious harm to individuals ● Risks to gender-based violence, children's best interests, public health and the environment.. Both the EU's DSA and the UK's OSA require risk assessments.	As a corollary of risk assessments, platforms must be required to implement reasonable steps to mitigate against each risk identified. These measures must be included in the assessments sent to regulators. Both the EU's DSA and the UK's OSA require risk mitigations against risks identified in assessments. Canada's Online Harms Bill also places obligations on platforms to mitigate risks aligning with their duties.	Five different measures could be introduced to enhance public transparency: ● Annual risk assessments ● Annual public transparency reports, which are heavily prescriptive ● Annual independent audits of risk assessments and transparency reports ● Ad repositories. Openly searchable databases of all ads and meta-data about ads rejected ● Researcher access to public interest data and requirements that vetted researchers can access public interest data. These need to exist alongside strong investigative powers for regulators. The EU's DSA requires this sort of public transparency regime.	To meaningfully drive change, regulations need to be enforceable. Specifically, regulators must be empowered and resourced to: ● Compel redress and changes to platforms' systems and elements rather than just compel transparency or take-down ● Issue penalties that match the scale of global profits of digital platforms ● Have powers to 'turn off' services where failures are persistent and all other measures have been exhausted ● Enhance the public-facing complaints mechanism to include complaints from individuals and consumer groups regarding systemic risks and breaches of their duty of care ● Have strong investigative and information-gathering powers ● Effective notice-and-take-down powers. The European Commission, the UK's Ofcom and the new Canadian Digital Safety Commissioner have combinations of these enforcement powers. The UK goes even further and includes criminal sanctions for executives regarding transparency.[35]

Figure 2: Five potential policy pillars to create effective systemic regulation in the digital space

[31]UK 2023 *Online Safety Act 2023* https://www.legislation.gov.uk/ukpga/2023/50/enacted
[32]Canada 2024 *Online Harms Bill 2024* https://www.parl.ca/LegisInfo/en/bill/44-1/c-63
[33]EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[34]Article 34, EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[35]For more information see UK 2024 *Online Safety Act: new criminal offences circular* https://www.gov.uk/government/publications/online-safety-act-new-criminal-offences-circular/online-safety-act-new-criminal-offences-circular

The 'children's best interests' principle

These concurrent reviews also present an opportunity to create an aligned framework to better improve protections for children and to advance their rights. There appears to be an emerging regulatory response by introducing the 'children's best interests' principle into regulation that affects the digital world. For example, proposals for reform to the *Privacy Act*[36] include options such as:

- Requirements to consider children's best interests in deciding if data processings is 'fair and reasonable';
- The introduction of a Children's Privacy Code, which would embeds the best interest principle;
- Requirements prohibiting direct marketing to children under 18 and prohibiting targeting children under 18 except where it is in their best interests.

Likewise, terms of reference for the *Online Safety Act* call for an assessment of whether the framework should include requirements to ensure industry acts in the best interests of the child.[37]

This approach may help to 'join up' privacy and online safety protections for children in particular, and could be extended to other ongoing reviews, such as the ongoing *Digital Platforms Services Inquiry*. We note that determining children's best interests is not always straightforward, and clear guidance around this could be helpful.[38]

[36]Attorney General's Department 2023 *Privacy Act Review Report,* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
[37]Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2021 *Terms of Reference – Statutory Review of the Online Safety Act 2021* https://www.infrastructure.gov.au/sites/default/files/documents/tor-statutory-review-online-safety-act-2021-8Feb.pdf
[38]See for example, a first attempt at what this might look like in the privacy domain at Reset.Tech Australia 2024 *Best Interets and Targeting: Implementing the Privacy Act Review to advance children's rights* https://au.reset.tech/news/best-interests-and-targeting-implementing-the-privacy-act-review-to-advance-children-s-rights/

Public support for systemic regulation

Working with YouGov, in April 2024 we polled 1,514 people to gather their views on these proposals. We found broad support for them.

Firstly, there was a strong recognition that the public felt unsafe online. In total, 81% of Australians occasionally, regularly or always feel unsafe online (see Figure 3).

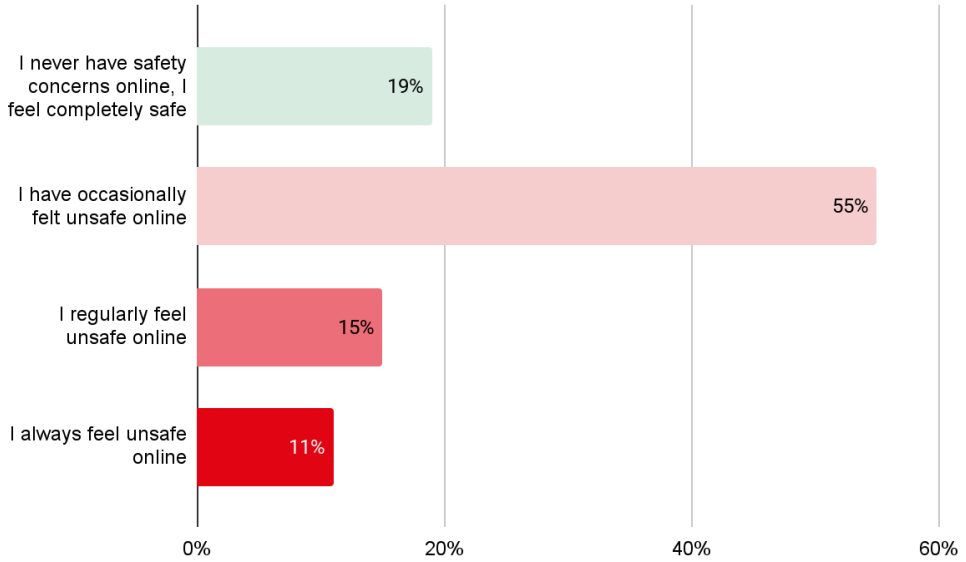

Figure 3: Responses to the question 'Thinking about your experiences using social media platforms, how would you describe your feelings of safety from online risks, such as online scams, deep fakes, data breaches, misinformation and disinformation?' (n=1.514)

When it comes to the type of regulation the public would like to see, there is a strong preference for systemic regulation in conjunction with content focussed regulation (see Figure 4).

Laws that focus on risky content, so that risky content is taken down when it is found	*9%*
Laws that focus on systems, so that platforms are required to build in better and more effective ways to manage risky co	*20%*
Focus on both risky content and systems	*60%*
Neither	*3%*
Don't know	*7%*

Figure 4: Responses to the question 'There are a number of ways that laws can be made to try to improve online safety. Which of these would you prefer?' (n=1.514)

We were also interested in understanding if, in regulating content online, people were concerned about "over-zealous" content moderation. This did not appear to be the case, with only 5% of respondents concerned that platforms were doing too much to address risky content online (see Figure 5).

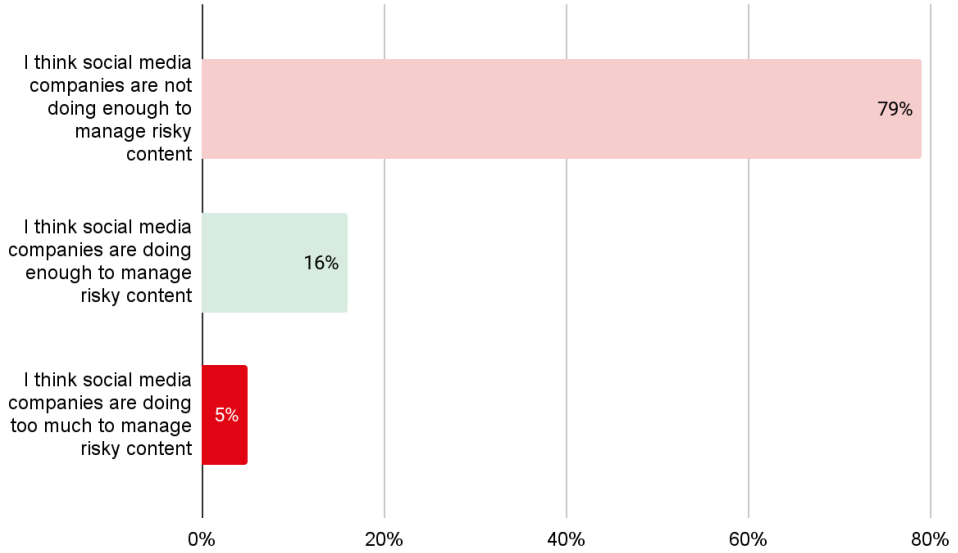

Figure 5: Responses to the question 'Social media companies make lots of decisions about what they do with risky content that breaks their rules. Which of the following best describes how you think social media companies are managing this content' (n=1.514)

We asked about our five pillars approach to digital regulation, starting with a duty of care. We found strong support for a duty of care, with 93% of people agreeing that social media companies should have a duty to take reasonable care of their users (see Figure 6).

Agree	*93%*
Disagree	*5%*

Figure 6: Responses to the question 'Social media companies should have a duty to take reasonable care of their user' (n=1,514)

We also asked about measures for risk assessments and risk mitigations, transparency and accountability, and found strong support for systemic laws that increase accountability and transparency (see Figure 7).

Social media companies should have to make thorough risk assessments to identify major risks on their platforms	*59%*
Social media companies should have to take reasonable steps to manage identified major risks on their platforms	*65%*
Social media companies should have to be transparent with the public and regulators about major risks of their platforms	*63%*
Regulators should have the power to compel social media companies to make reasonable changes to their systems in order to be safer	62%

Figure 7: Responses to the question 'It's not always clear if social media companies are responsible for the harms that happen on their platforms. There are some discussions that laws could be passed that make social media companies more responsible. Which, if any, of these responsibility measures would you support in law (select all you support)' (n=1,514)

We asked for more thoughts about transparency, using the ability to 'understand' how algorithms work as a case study. There was support for a battery of transparency measures (see Figure 8).

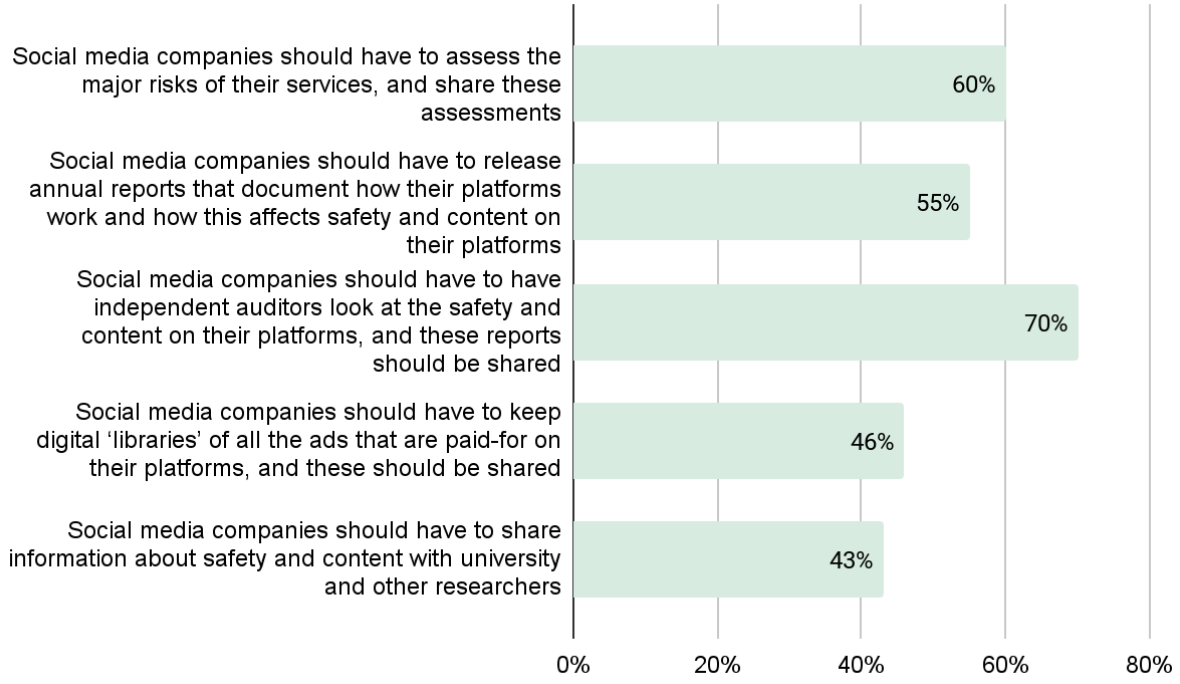

Figure 8: It's not always clear how social media companies build their systems and algorithms. There are some discussions that laws could be passed that make social media companies be more transparent about how platforms work and the consequences of this. Which, if any, of these transparency measures would you support in law? (select all you support)' (n=1,514)

Lastly, we also asked about introducing the children's best interests principle into privacy and safety laws, and found strong support for inclusion in both; 15% of respondents thought the children's best interest principle should be in place to protect the use of children's data (privacy), 12% thought it should be in place when it came to online safety rules and 67% thought it should be in place for both (see Figure 9).

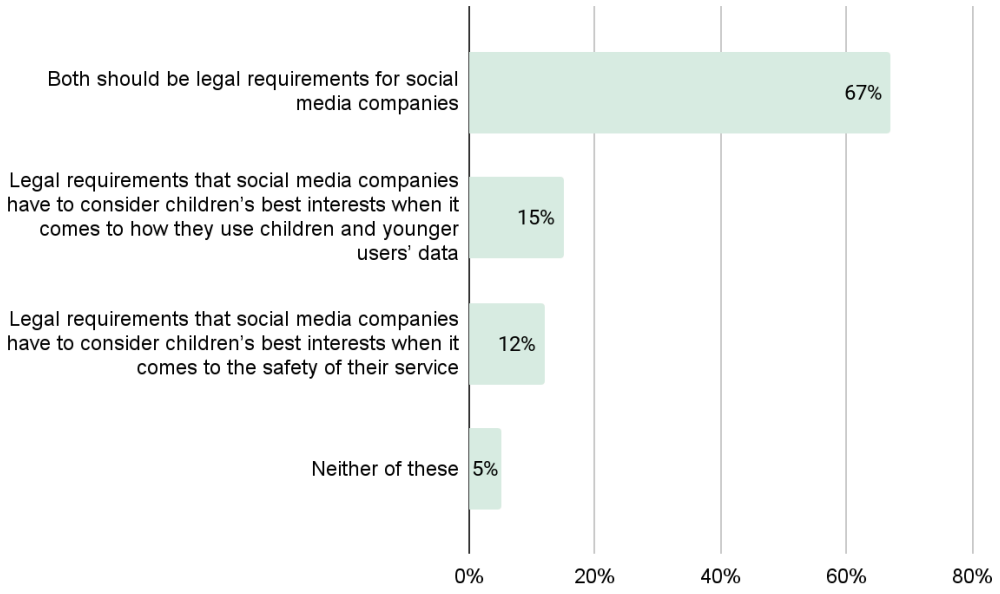

Figure 9: Responses to the question 'It's not always clear if social media companies make their products in ways that are best for children and younger users under 18. There are some discussions that laws could be passed that make social media companies think about children's best interests in the way they work. Which, if any, of these measures would you support in law?' (n=1,514)

Responsibilities

Responsibility for digital platform regulation has spread across a range of Ministerial portfolios. A summary of key activities is below.

Who	Area
Minister for Communications, the Hon Michelle Rowland MP	Misinformation and disinformation, amendments to the Basic Online Safety Expectations, *Online Safety Act* statutory review, including a consideration of potential measures to counter online hate and the introduction of the best interests principle for children, oversight of the Australian Communications and Media Authority and the Office of the eSafety Commissioner
Attorney-General, the Hon Mark Dreyfus KC MP	*Privacy Act* Review, including expedited reforms on vilification, hate speech, privacy and doxxing, a potential children's privacy code, oversight of the Office of the Information Commissioner and Privacy Commissioner
Treasurer, the Hon Jim Chalmers MP	Oversight of the Australian Competition and Consumer Commission
Assistant Treasurer and Minister for Financial Services, the Hon Stephen Jones MP	*News Media Bargaining Code,* National Anti-Scam Centre
Minister for Home Affairs and Cyber Security, the Hon Clare O'Neil MP	Cyber Security Strategy, Strengthening Democracy Taskforce
Minister for Industry and Science, the Hon Ed Husic MP	Safe and Responsible AI Consultation
Assistant Minister for Competition, the Hon Dr Andrew Leigh MP	Review of competition measures, including digital competition

Figure 10: Relevant responsibilities for policy dynamics