

About the Tech Policy Design Institute (TPDi)

TPDi is an independent, non-partisan think tank committed to advancing best practice technology policy in Australia and globally. Based in Canberra, TPDi is registered as a not-for-profit with the Australian Charities and Not-for-Profit Commission. TPDi collaborates with all stakeholders in the tech ecosystem. Our mission is to shape technology for the benefit of humanity. We do this through rigorous research, innovative education, evidence-based public commentary, and community building.

Acknowledgements

We are grateful to all Design Dialogue participants – who contributed their time and expertise to finding common ground and reviewing this report – listed in full in the Appendix. While developed through a collaborative process, the final report, assessment, analysis and all outcomes represent solely the views of TPDi and the authors.

This report was made possible by the generous support of contributors to the Tech Policy Design Fund, including Diamond Sponsor (University of Canberra); Platinum Sponsor (The Minderoo Foundation); Gold Sponsors (Department of Industry, Science and Resources; Digital Transformation Agency; Microsoft; Qoria), and Silver Sponsors (Amazon; Apple; CyberCX; Tata Consultancy Services). These insights were captured at TPDi's annual Tech Futures event, made possible through the generous support of the .au Domain Administration. Our Tech Policy Youth Ambassadors are able to contribute their perspectives to TPDi's activities thanks to generous support from The LEGO Group. TPDi does not represent the views of our funders. In all instances, TPDi retains full independence over our research and complete editorial discretion of outputs.

The TPDi research team reviewed and analysed all the non-attributed content captured at the Design Dialogue. Generative AI tools were used in a limited capacity to assist with summary and editing processes. All arguments, analysis, findings and final content in this report belong to the TPDi research team.

Independence statement

TPDi's independence is our most valuable asset. As a registered not-for-profit, our work is supported by external funding. We only accept funding from entities that agree to be disclosed publicly and commit to respect and promote TPDi's independence. TPDi does not represent the views of any of our funders. All outputs represent solely the views of TPDi and/or the authors.

Authors

Zoe Jay Hawkins, Co-Founder & Deputy Executive Director, TPDi.
Johanna Weaver, Co-Founder & Executive Director, TPDi.

With invaluable contributions from Thomas van der Valk, Meredith Hodgman, Emily Crabb, Paris Borkowski and Helen Portillo-Castro.

Citation

Hawkins ZJ, Weaver J (2026). *Digital duty of care: make tech care*. Tech Policy Design Institute.

ISBN (print) 978-1-7649583-0-1

ISBN (online PDF) 978-1-7646740-9-6

Copyright



This work is licensed under CC BY-NC-ND 4.0.

To view a copy of this licence, visit:

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Contact

Tech Policy Design Institute
www.techpolicy.au

hello@techpolicy.au

ABN: 94 681 576 394

TPDi is registered as a not-for-profit with the Australian Charities and Not-for-Profit Commission.



CONTENTS

FOREWORD	4
TPDi RECOMMENDATIONS.....	5
DESIGN DIALOGUE EXECUTIVE SUMMARY	8
METHOD: TPDi DESIGN DIALOGUE.....	14
COMMON GROUND.....	16
DIVERGENCES	23
APPENDIX: PARTICIPANTS.....	31
ENDNOTES	33

FOREWORD

Online harms are not inevitable consequences of technological progress.

Legislation to introduce a digital duty of care is a rare opportunity for Australia to reshape the online environment and its impact on our lives. Technology has immense positive benefits but realising them requires proactive policy design.

This is Australia's opportunity to implement a duty to make tech care.

A digital duty of care will obligate online services to keep their users safe, prevent serious harms *before* they occur, and anticipate the next generation of harms on the horizon.

When this legislation is introduced into Parliament, every effort should be made – by all stakeholders – to avoid the reform being defined, reduced or derailed by the most polarising fault lines.

Done well, the duty will encourage services to invest in safer design, empower individuals with meaningful choices, and create a framework that endures as technologies and harms evolve.

Done poorly, it could become another layer of regulatory complexity. It could create obligations that look ambitious on paper but cannot be meaningfully enforced. It could miss the moment and fail to create real change.

The concept is simple but the design choices are not.

Good tech policy requires more than good intentions. That is why we convened a TPDi Design Dialogue on the digital duty of care. We brought together leaders from across Parliament, government, industry, civil society and research to move the conversation forward. Collective knowledge and diverse perspectives produce stronger policy.

Drawing on dialogue discussions, this policy spotlight details areas of common ground and areas of divergence, highlighting the key legislative choices that will shape the design of the duty.

This document also sets out **7 TPDi recommendations for policymakers**.

Policy is one of the most powerful tools we have to influence how technology affects people and society. We must wield it with intention, and the digital duty of care is an opportunity to do exactly that.

Passage of well-designed legislation – enshrining a positive overarching duty on tech companies to care – is a beginning, not an end point.

But the future is still ours to shape – and we have a duty to do so.

Johanna Weaver

Johanna Weaver
Co-Founder
Tech Policy Design Institute

Zoe Jay Hawkins

Zoe Jay Hawkins
Co-Founder
Tech Policy Design Institute



TPDi RECOMMENDATIONS

This report summarises key insights from TPDi's multi-stakeholder Design Dialogue on the digital duty of care, hosted on 10 August 2026 at Parliament House, attended by the Minister for Communications and representatives of her department, as well as representatives from civil society, industry, government and academia (listed in the Appendix). This report was prepared prior to the government's release of the exposure draft Online Safety Amendment (Digital Duty of Care) Bill 2026.¹

Drawing on those discussions, this section sets out TPDi's independent recommendations for policymakers as they consider the design of the digital duty of care. We have annotated the recommendations to indicate the extent to which related concepts are reflected in the Exposure Draft.

1. Implement an overarching duty

Partially reflected in exposure draft bill (see s26 – especially 26(c), including its note, and s26A)

The legislation should implement an overarching duty that obligates online services to take reasonable steps to prevent foreseeable serious harm.² This overarching duty is the most important component of the legislation. It future proofs the law, ensuring it captures new technologies, risks and harms as they emerge, without necessitating a new parliamentary process with each technology or harm. Put simply, **the overarching duty is the mechanism to ensure the obligation on services to prevent harm evolves at the same speed as technological innovation.** This approach does not preclude additional specific requirements also being included in the legislation, but these should be supplementary to the overarching duty – they should not replace or dilute it.

2. Extend that duty for all Australians

Reflected in exposure draft bill (see ss 25B and 26 – especially 26(c), including its note), but note comment regarding overarching duty above.

All Australians deserve a safe online environment, regardless of their age, and the duty's scope should reflect that.³ The principle that organisations should take reasonable steps to prevent foreseeable harm is already well established in Australian law, including in the common law doctrine of negligence, as well as in legislation including civil liability, workplace health and safety (WHS), and consumer protection. Establishing a specific *digital* duty of care makes it unambiguous that the 'duty to care' extends to online services, while adding greater specificity as to what that duty entails (in the same way that WHS legislation extends the common law doctrine of negligence to the workplace, while adding specificity to the obligations of employers).

There has been some suggestion that the duty could or should be limited in application to children only.⁴ TPDi does not recommend narrowing the duty in this way. Serious online harms are experienced by adults as well as children and experienced more acutely by vulnerable groups – for example, through tech-facilitated gender-based violence and online racism. Restricting the duty to children risks creating an arbitrary 'age cliff' where protections disappear at adulthood despite the evidence of the serious online harms affecting adults. **If political realities require, the legislation should impose a duty to all Australians with a phased implementation pathway that prioritises implementation for**

children, while allowing time to resolve the policy questions surrounding implementation of a duty for adults.

3. Address service design not just content – and fix our feeds

Reflected in the exposure draft bill (see proposed ss 25F, 26(3)(a), 26(4)–(6) and 26A(2)(a)(iii)–(iv))

The duty should address the systems, features and design choices that create or amplify harm, not just the content and conduct that is shared on a service. **Australia's approach should cover recommender systems, hyper-personalised targeting, addictive product design, AI sycophancy and other features that shape user behaviour and increase risk of harm.**⁵ Obligating services to prevent harm caused by their own service features and functions is a way of mandating 'safety by design'.⁶ **This should include, but not be limited to, a specific requirement for content recommendation algorithms to be opt-in.**⁷

4. Enable enforcement: establish mechanisms to fund the regulators and for users to seek direct redress

Not reflected in exposure draft bill but expanded powers (see ss 26D, 26F–26G, 192C–192N and 199–205)

The impact of any duty will ultimately depend on its enforcement. As policymakers determine the scope of the duty, they should also consider the regulator powers, funding and structures required to supervise and enforce this next phase of regulation. **The legislation should evolve the Office of the eSafety Commissioner into a multi-Commissioner model commensurate with the regulator's expanding responsibilities.**⁸ It should also provide a mechanism to fund increased regulatory responsibilities, including but not limited to, by eSafety and the Office of the Australian Information Commissioner (for example, by introducing a levy – building on Australia's precedent in the telecommunications sector,⁹ or the Irish precedent for online platforms).¹⁰ Enforcement should, however, not remain the sole domain of regulators. **The legislation should also establish a private right of action** (allowing for individual/class actions – a method which has proven effective in the United States)¹¹ **and appropriate pathways for user redress** (Ombudsman).¹²

5. Incentivise services to compete on safety

No exemption framework in exposure draft bill but general ministerial exemption power (see s25A(3)(a))

This reform should make safety investments commercially attractive by building in targeted exemptions from specific obligations for services that can demonstrate their effective risk mitigations. While exemptions from the overarching duty should not be available, this is an opportunity to introduce the debated social media age restriction exemption framework (initially proposed in South Australia) that would accommodate access for under 16-year-olds to social media services that demonstrate harm minimisation.¹³ This approach is being considered in Canada.¹⁴ Instead of only relying exclusively on fines for failure, Australia's online safety framework should build in design features that create commercial incentives for a race to the top.



6. Protect public-interest research into platform harms

Reflected in exposure draft legislation (see ss 205B-205L)

The duty should provide legal protections for legitimate public-interest research into online services, expanding on those provided by the EU Digital Services Act by vetted researchers.¹⁵ **This should include protections for researchers investigating platform harms, including where research involves accounts or methods that may otherwise breach platform terms (for example, safe harbor for creation of fake accounts (often called ‘sock puppet’ accounts) to test algorithmic features).** Any access framework should include clear privacy, security and ethical safeguards. This would position Australia as a global leader in the public-interest research needed to drive ongoing systemic change.

7. Approach as a cross-partisan national priority

Debates about online safety regulation can quickly become polarised, simplified or drawn into entrenched disputes about censorship, privacy, and the role of government. As legislation is introduced, there will be important debates around scope, proportionality, accountability and oversight. But the focus should remain on identifying common ground and practical mechanisms for improving the safety of Australians in a rights respecting manner. Every effort should be made – by all stakeholders – to avoid the reform being defined, reduced or derailed by the most polarising fault lines.

Australia’s Digital duty of care is a nationally significant, fundamental reform in the interests of all Australians. Online services are shaping Australia’s community wellbeing, social cohesion and trust in democracy. Online safety should therefore be treated as a long-term cross-partisan national priority, rather than a short-term political contest.

DESIGN DIALOGUE EXECUTIVE SUMMARY

The digital duty of care is one of the most consequential reforms to be considered by the Australian Parliament this year. At its core the Digital duty of care is about making tech care.

Online services, from social media to devices and artificial intelligence systems, shape how Australians access information, participate in civic life, build relationships and engage with institutions. The central societal role these services play means their design and governance increasingly shape outcomes far beyond online spaces: individual wellbeing, public safety, economic participation, social cohesion and democratic resilience.

Australia is widely regarded as a global leader in online safety with a sophisticated regulatory regime, overseen by the world's first independent online safety regulator. Over the past decade, successive Australian Parliaments have progressively expanded the online safety framework through the *Online Safety Act 2021* (Cth), Codes and Standards, plus social media minimum age (SMMA) restrictions.

A digital duty of care has the potential to simplify and future proof the regime to deliver systemic change. Rather than addressing specific harms, technologies or products individually, the government's proposed duty would impose an overarching obligation for all online services to take reasonable steps to mitigate foreseeable serious harms. **It represents a transition to a more systemic, risk-based and future-focused approach to online safety.**

Australia is not alone. Around the world, governments and courts are increasingly examining how online services are designed, how algorithms and AI-based systems shape behaviour, and whether the incentives built into digital products contribute to harm. Yet while the direction of travel is becoming clearer, many important design questions are yet to be tested in Parliament.

Online safety policy is inherently challenging: it combines highly personal and emotionally charged issues with powerful commercial interests, rapidly evolving technologies and politically contentious debates about speech, accountability and the role of government.

To support Australia's consideration of this reform, the Tech Policy Design Institute (TPDi) convened a multistakeholder Design Dialogue at Australian Parliament House in August 2026. The purpose was to identify areas of common ground, surface meaningful differences and clarify the policy decisions still facing policymakers.

This report was prepared before the government's release of the exposure draft Digital Duty of Care Bill 2026.¹⁶



Convergence

The Dialogue revealed considerably more convergence than many participants anticipated.

There was common ground support for:

1. **implementing a proactive and preventative duty** – participants supported a duty that places greater responsibility on services to anticipate and mitigate foreseeable harms
2. **implementing an overarching and enduring duty** – participants broadly favoured a technology-neutral and harm-agnostic duty capable of adapting to evolving technologies, products and risks over time
3. **addressing systems and product design, not just content** – participants agreed the duty should focus on how services are designed, including features, recommender systems and other mechanisms that can create or amplify harm
4. **sharing responsibility across the tech ecosystem** – participants agreed responsibility should not sit solely with social media services but should be distributed across the wider digital ecosystem, while remaining proportionate to risk and control
5. **retaining existing protections and capabilities** – participants broadly agreed that reform should build upon, not weaken, the protections and regulatory powers and already present in Australia's online safety framework
6. **aligning commercial incentives with safer outcomes** – participants found that the duty should be designed in a way to incentivise corporate investments in safety as a competitive advantage, as opposed to only a cost centre
7. **enhancing transparency and independent scrutiny** – participants agreed that an effective duty requires independent scrutiny beyond regulator reporting and platform self-assessment, including appropriate researcher access, auditing and transparency mechanisms
8. **coordinating a coherent regulatory system** – participants agreed that the duty must operate coherently alongside privacy, consumer, competition and existing online safety regulation, with strong coordination across regulators
9. **matching ambition with regulatory capability** – participants agreed that the success of the duty will depend on regulators having the powers, expertise and funding necessary to supervise and enforce it effectively
10. **cultivating public legitimacy and political feasibility** – participants agreed that reform will require a clear articulation of success, effective public communication and broad political support.

Divergence

The divergences concern the scope and ambition of the duty.

1. **How to balance rights for safety?** How to reconcile human rights to freedom of expression and privacy when they are in tension with safety policy objectives and other rights.
2. **Children or all Australians?** While there was strong support that the duty should establish baseline protections owed to all Australians, some participants questioned whether it could operate as a child safety regime.
3. **Illegal, serious, precursor, cumulative and/or systemic harms?** Participants differed on how far the duty should extend beyond illegal harms to include financial harms, harmful but lawful content and conduct, precursor harms, cumulative harms and broader systemic harms.
4. **Risk-based or outcomes-based duty?** Participants differed on whether the duty should focus primarily on reducing risks and preventing harms or also require services to promote positive outcomes for users and society.
5. **Universal safeguards or personalised protections?** Participants differed on whether safer online environments are best achieved through broadly consistent safeguards for all users or protections tailored to particular users, vulnerabilities and contexts.
6. **How prescriptive?** Participants differed on how much certainty should be embedded into the duty, and how much flexibility should be left to regulators, delegated rule-making processes and the evolution of common law over time.
7. **Bold or incremental reform?** Participants differed on if the duty should be used to secure comprehensive reform now or establish a more limited foundation to be expanded over time.

AREA	CONVERGENCE	DIVERGENCE
Scope	C1. Proactive and preventative duty C2. Overarching and enduring duty C3. Address systems and product design, not just content C4. Share responsibility across the tech ecosystem	D2. Children or all Australians? D3. What harms should the duty address? D4. Risk-based or outcomes-based?
Design	C5. Retain existing protections and capabilities C6. Align commercial incentives with safer outcomes C7. Bold or incremental reform?	D1. How to balance rights for safety? D5. Universal safeguards or personalised protections? D6. How prescriptive?
Implementation	C8. Coordinate a coherent regulatory system C9. Match ambition with regulator capability C10. Cultivate public legitimacy and political feasibility	D7. Bold or incremental reform?



Cautious optimism, not complacency

It would be easy to focus only on the areas of divergence represented throughout this report, which are significant. Yet one of the strongest observations from the dialogue was how much common ground existed across a diverse and often unlikely group of participants. There was genuine optimism in the room that a digital duty of care can move beyond familiar divisions and deliver practical change.

Many participants arrived expecting more polarisation than they encountered. Several commented they were struck by the broad support for preventative approaches and the willingness of participants to engage constructively with competing perspectives.

This was not born of naivety. Significant design choices are being considered, and participants were realistic about the scale of the task ahead. One participant described the coming years as a ‘tsunami’ of work, while others emphasised that designing and implementing an effective duty will be difficult, resource intensive and politically challenging.

That risk is already beginning to emerge in the political debate. As the duty moves from principle to legislative design and debate, there are signs that the conversation could harden into familiar arguments about censorship, government overreach and individual responsibility. If that happens, the reform risks being defined by polarised positions rather than by the core design principles of making tech care and establishing a mechanism to hold them accountable if they don’t. The role of civil society and independent researchers will become more important when legislation is introduced into Parliament and the public debate intensifies. It is incumbent on all of us to help ensure the conversation is informed by evidence, lived experience and focused on the practical end goal of the reform: safer online environments, and responsibility and accountability of the digital platforms and services that shape our world.

The task now is to build on the constructive foundation revealed in the dialogue, resist unnecessary politicisation, and help shape a public debate focused on meaningful protections for Australians.

The independent statutory review of the *Online Safety Act 2021*, conducted by Delia Rickard PSM, identified this limitation and recommended an overarching statutory digital duty of care (the duty).¹⁷ Rickard’s proposed duty would evolve Australia’s online safety approach by creating a single overarching obligation for services to systematically identify, assess and mitigate all foreseeable serious harms across the online ecosystem.

The Australian Government has committed to introducing a digital duty of care. It published an issues paper in May 2026 proposing all services regulated under the *Online Safety Act 2021* must take ‘reasonable steps to maintain effective systems and processes’ that ‘prevent reasonably foreseeable serious harms’ in order to ‘provide a safe online environment for Australians’.¹⁸ This policy intention has now been reflected in exposure draft legislation.¹⁹

Changing expectations around the world

Other jurisdictions have already started moving in the direction of pushing the onus onto online services to prevent harm from occurring, both by anticipating risks and considering product design.

The European Union’s 2022 Digital Services Act imposes ‘due diligence’ obligations on online intermediary services. It also requires very large online platforms and search engines to assess and mitigate system risks associated with their services, including risks to fundamental rights, civic discourse, public health and democratic processes.²⁰ Its implementation is also increasingly testing design features

rather than content alone. The European Commission has issued preliminary findings concerning platform features including addictive design.²¹

The United Kingdom's *Online Safety Act 2023* imposes a series of statutory duties on online services to assess, manage and mitigate online safety risks.²² While the UK's 2019 white paper proposed an overarching duty of care,²³ this was ultimately not included in the legislation. The Act includes specific duties regarding illegal content, content harmful to children, and transparency and accountability for categorised services.²⁴ The Act does not include a single overarching duty and does not include an obligation to prevent 'lawful but awful' harms to adults.

A plethora of litigation in the United States has similarly brought attention to claims concerning services responsibility for allegedly addictive platform design and features, including infinite scroll, notifications and recommendation systems.²⁵

The legal context and implications of each of these developments differ, but together they illustrate a broader change in the policy conversation. Governments, regulators and courts are increasingly examining how a service is designed, how it influences behaviour, and how its systems distribute risks.

New day, new harms

Emerging technologies add urgency to getting Australia's online safety policy settings right. Deepfakes created with generative AI inflict harm, particularly on women.²⁶ Anthropomorphised AI companion systems raise questions about emotional attachment and the effects of highly personalised attention on relationship expectations.²⁷ Connected devices and wearable technologies such as smart glasses create new pathways for surveillance and technology-facilitated abuse.²⁸

These developments reinforce the challenge of regulating for every new technology. Legislators face the task of designing frameworks that can stand the test of time. A digital duty of care could provide an overarching framework capable of holding services accountable even as technologies and harms evolve.

A consequential design choice

The question before Australia is how to hold online services responsible for the environments they create. There are also related but separate reform discussions underway across privacy, competition and scams policy that intersect with this conversation.²⁹ It was in this context that TPDi convened the Digital Duty of Care Design Dialogue. This report captures the discussion as a practical contribution to the next stage of Australia's reform.



Figure 1: Messages from Design Dialogue participants to the Minister for Communications



METHOD: TPDi DESIGN DIALOGUE

TPDi's work is grounded in a simple belief: technology does not determine our future, people's decisions about technology do – through the institutions we build, the policies we implement, the way we relate, and the choices we make about how technology is designed, developed, deployed and governed.

This belief underpins TPDi's Design Dialogue method.

TPDi's Design Dialogue method

Technology policy challenges are often characterised by competing interests, polarised public debate and fragmented expertise. Yet effective governance requires policymakers to understand diverse perspectives and thread the needle of complex trade-offs.

TPDi Design Dialogues are curated, structured, facilitated forums that support this task.

We convene leaders from across Parliament, government, industry, civil society and research in trusted, neutral forums designed to move the conversation forward. Participants are asked to listen actively, test their assumptions and engage meaningfully with competing viewpoints.

TPDi Design Dialogues create the conditions for productive discomfort, helping stakeholders move beyond adversarial positions towards a shared understanding of complex policy problems and a pragmatic commitment to designing solutions. Through this process, areas of common ground emerge and, in some cases, are created. This common ground is where workable tech policy solutions exist.

The objective is not to eliminate disagreement and manufacture consensus on all things. Rather, TPDi's Design Dialogues build bridges. They humanise complex debates, cross-fertilise expertise, and strengthen trust across stakeholder groups.

The value of a Design Dialogue extends beyond any single report. By strengthening understanding across stakeholder groups and building relationships capable of sustaining future engagement, the process contributes to a more constructive technology policy ecosystem.

The method forms part of TPDi's broader theory of change, helping raise the bar by enabling informed debate and improving policy and governance.³⁰

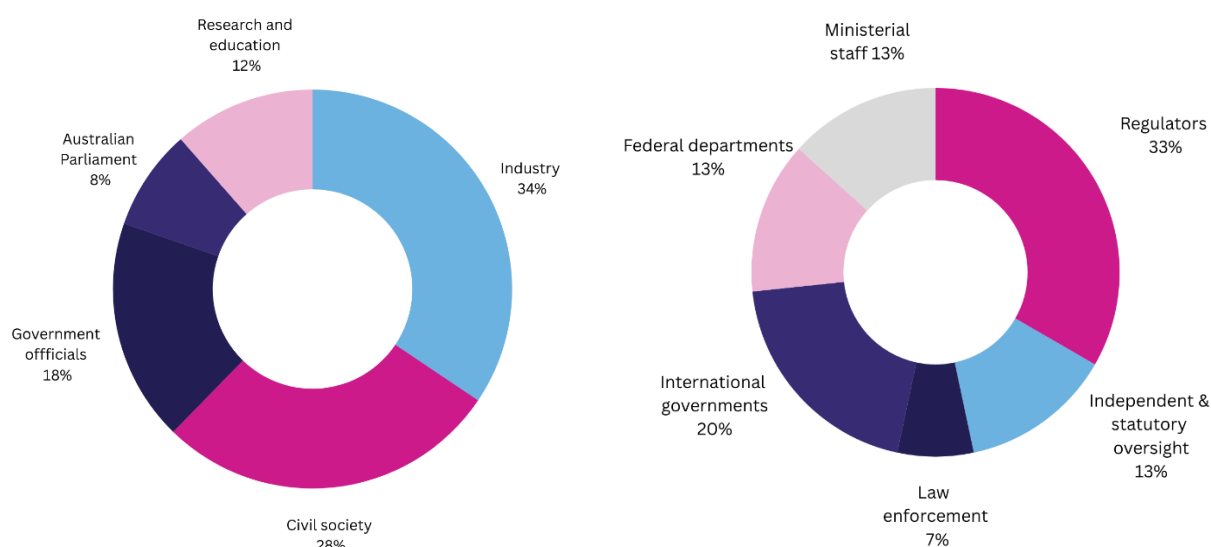
Digital Duty of Care Design Dialogue

TPDi convened the Digital Duty of Care Design Dialogue at Australian Parliament House on 10 August 2026 to support Australia's consideration of this significant online safety legislative reform.

The consultation brought together 61 participants from 51 organisations and institutions. Participants came from civil society (28%), government (18%), Australian Parliament (8%), industry (34%), and research and education (12%). The cohort included parliamentarians, rights advocates, major technology companies and digital platforms, Australian safety-tech businesses, regulators and statutory bodies, government departments, philanthropic organisations, universities and research institutions, youth representatives, civil society organisations and international governments. Figure 2 shows a breakdown of stakeholder representation.



Figure 2: Breakdown of participants by stakeholder group and government representation



Women comprised 66% of participants.³¹ The consultation also included organisations with direct expertise in the experiences of children and young people, human and digital rights, digital inclusion, consent and gender-based harm. These included the Alannah & Madeline Foundation, the ARC Centre of Excellence for the Digital Child, UNICEF Australia, Teach Us Consent, Movember, Digital Rights Watch and Good Things Foundation Australia.

Young people also participated directly alongside parliamentarians and senior stakeholders, enabling genuine intergenerational discussion, with 3 TPDi Youth Ambassadors contributing their perspectives to the consultation. First Nations perspectives were contributed to the Dialogue through the First Nations Digital Inclusion Advisory Group.

Together, this mix of participants provided a broad cross-section of perspectives from organisations developing and operating technology, researching digital harms, representing affected communities, regulating online services, and shaping public policy.

The full-day discussions were conducted on a non-attributable basis to encourage candid engagement and constructive challenge.

The purpose of the dialogue was not to produce a single agreed position. Instead, it identified areas of common ground, surfaced points of divergence and clarified the key design choices that government will ultimately need to resolve.

Discussions focused on 3 questions:

1. What should the duty require, and of whom?
2. What can Australia learn from international experience?
3. How should the duty be enforced and implemented?

All participants were invited to complete a 'policy postcard' capturing their 'one key takeaway' from the dialogue for delivery to the Minister for Communications.

The findings that follow are organised around areas of convergence and divergence that emerged through the dialogue. Together, they provide a practical map of the policy common ground and design choices facing the Parliament in the consideration of a digital duty of care for Australia.

COMMON GROUND

Framing

Convergence 1: Proactive and preventative duty

There was strong common ground on the overarching purpose and ambition of the digital duty of care (duty): to move Australia's online safety framework towards a clear obligation to prevent harm.

Participants broadly agreed that the increasing speed, scale and complexity of online services mean a reactive, 'whack-a-mole' approach is not sufficient to address emerging harms at scale. **There was support for imposing an obligation on service providers to develop, deploy and monitor their services in a way that keeps their users safe *before* harm occurs (known as an 'ex ante' obligation).** Participants agreed that a duty was also a way to operationalise the 'Safety by Design' principles into practice.

'If we can get in front of the threat, we can stop the harms before they occur.'

It was recognised that the principles of taking 'reasonable steps' to prevent 'foreseeable harm' are well established across Australian common law and state and territory civil liability frameworks. Likewise, 'chain of causation' is a well-established common law principle that bestows significant legal precedent in apportioning responsibility and accountability in complex circumstances. Embedding these legal terms of art in the duty will help deliver both clarity and certainty.

That said, adopting an overarching duty was not taken to imply a 'zero-risk' approach. Participants acknowledged that some harms will still occur, but this paradigm shift would drive important change and materially 'turn the volume down' on the harms occurring. Doing this effectively, and soon, was seen as important to sustain Australians' confidence in online services.

'Overarching principles are important to create future-proof legislation. We need to be proactive and adaptive.'

Convergence 2: Overarching and enduring duty

Participants also agreed on the value of Australia moving to a more technology- and harm-agnostic approach to harm-prevention obligations. **The statutory review's recommendation that Australia adopt a single overarching duty, rather than multiple duties relating to specific harms or technologies, was an area of common ground.**³²

An overarching, principles-based obligation was seen to provide important baseline protection, particularly in the absence of a comprehensive human rights framework. Participants noted that numerous specific duties – like those adopted in the UK – may inadvertently restrict the value of the duty.³³ Participants favoured a more overarching, principles-based approach would future proof the duty to capture new and evolving technologies and risks

'My one key takeaway is that the duty be designed to endure without the need for constant updates, either via Parliament or the minister.'



without requiring primary legislation to be continually amended. For example, the duty should account for the outputs, activities and operation of AI agents without needing to explicitly itemise that rapidly evolving technology.

There was also discussion that an overarching duty could be supported by more detailed mechanisms underneath it, including rules, codes and regulatory guidance. Participants noted that regulatory guidance can play a valuable role to provide clarity about what compliance might look like in particular circumstances, but there is a balance to strike between providing clarity versus being overly prescriptive.

See Divergence 6: How prescriptive?

Scope

Convergence 3: Address systems and product design not just content

Participants agreed that the duty should focus not just on individual pieces of content but also address the features, systems and product design that can create or amplify harm. Participants referred to the '4Cs' of online risk – content, conduct, contact and compulsion – as illustrating the breadth of risks that a systems-based duty should address.³⁴

Recommender algorithms and hyper-personalised targeting were identified as important enablers and amplifiers of risk – described by one participant as the 'special sauce' that can cause harm. Participants considered it important that the duty also capture addictive product design that encourage prolonged or compulsive use.

'This is our best shot of getting hold of the algorithm. Regardless of breadth, the duty needs to have depth.'

'Fix our Feeds (please) :)'

Participants pointed to the broader international trend towards scrutinising product features and design choices as sources of harm in their own right. In August 2026, a landmark trial was settled, involving a bipartisan coalition of 47 states against Meta,³⁵ with lead states seeking changes to features including screen time limitation and the option for a non-personalised feed.³⁶ Thousands of separate claims concerning allegedly addictive design by Meta and other major platforms are also progressing through US courts.³⁷ Similarly, participants noted that the European Commission has issued preliminary findings that TikTok and Meta have respectively breached the Digital Service Act (EU DSA) through addictive design, including infinite scroll, autoplay, push notifications and highly personalised recommender systems.³⁸

Looking ahead, participants identified anthropomorphised AI chatbots, and the potential for users to develop emotional attachment or dependency, as an emerging frontier for these kinds of design-related dark patterns. This reinforced the importance of a duty capable of addressing how services interact with and influence users, rather than only the content they distribute and conduct they facilitate.

Participants also converged around the idea that focusing on system-level interventions may provide a pathway to reducing harm that is less susceptible to the polarising free-speech debates associated with moderating individual categories of content.

'Most frustrations I hear with young Australians is about the inability to control the algorithms, their addictions, notifications, bot accounts, anonymity. We would love a redesign of the features.'

'Ensure that safety by design is mandatory and not optional.'

Convergence 4: Share responsibility across the tech ecosystem

There was common ground that the duty should apply broadly to all products and services across the complex tech ecosystem. Participants pointed to the diversity of services and products through which harms can arise – including social media, AI agents, games, app stores, connected toys, chatbots, and wearables such as smart glasses. A layer cake of services across the tech ecosystem may be involved in the occurrence of an online harm, including internet service providers, hosting services, and devices, reinforcing the importance of the duty including a way to clearly distribute responsibility across the ecosystem (for example: by importing the well-established common law principle of *chain of causation*).

Participants agreed that the breadth of the duty should not mean uniform responsibility.

Participants raised the merit of specifically distinguishing the different obligations of different categories of service. Example was drawn from the EU DSA, which categorises services in terms of size where large platforms have greater requirements over smaller ones which also have a duty to assess risk. Concerns were raised, however, that size is an imperfect measure for harm prevention. Small niche platforms can cause significant harm.

Overall, there convergence that what is 'reasonable' should reflect the nature and risk profile of a service, and its opportunity to mitigate harm. For example, there would be reasonably higher expectations of a service designed for or commonly used by children, than of an enterprise software service.

Participants noted this will be captured through defining 'reasonable steps' to take into account the factors listed above, and/or in risk assessment processes tailored to the unique profile of each service. This concept of graduated service-level responsibility was distinct from a separate discussion of whether protections within a service should also vary between different users, age groups or risk profiles (Divergence 5: universal safeguards or tailored protections?).

Participants recognised the value of clarifying and simplifying the definitional categories used in the *Online Safety Act 2021*, but the consensus was that retaining this breadth of scope through a whole-of-ecosystem approach is important to driving change. It was also noted that fully distributing responsibility across the tech ecosystem also involves grappling with the important role of device-level parental controls.

There was clear consensus that, to future proof the duty, its scope needs to be sufficiently broad to capture products and services not yet in common use.



Design

Convergence 5: Retain existing protections and capabilities

There was common ground that the duty should not result in any regression from the protections, regulatory capabilities or technical sophistication already in place under the existing framework. This did not mean retaining the current architecture unchanged but treating it as a baseline from which the new, streamlined framework should build.

Participants pointed to the sophistication of the existing codes and standards, which contain more than 330 risk-based measures spanning the online ecosystem, alongside a regulatory toolkit that includes 66 investigative powers. There was discussion of the considerable effort and contestation that had gone into specifying age-assurance requirements through the Phase 2 codes and standards, including for Class 2 material.³⁹ Removing the codes without preserving this work could leave services without sufficient clarity about what they are expected to do. **Participants characterised the importance of the codes ‘setting the floor, not the ceiling’ – the duty should close any gaps and elevate the ambition, while ensuring the existing baseline is not lost.**

See Divergence 6: How prescriptive?

Similarly, participants considered that existing transparency mechanisms under the Basic Online Safety Expectations (BOSE), and established investigative and enforcement capabilities, should be preserved or strengthened.

Convergence 6: Align commercial incentives with safer outcomes

Participants recognised that some online harms are closely linked to the business models that underpin certain large digital platforms’ design and operation. Features such as recommender algorithms, personalised targeting and engagement-driven design present a tension: they create commercial value but can also amplify risk and lead to harm. Through this prism, safety interventions are often seen by companies as cost centres that detract from the bottom line. An effective duty will need to disrupt this incentive structure head on.

‘Incentive based engagement can align private interest where penalties previously haven’t worked.’

There was an interest in the potential of harnessing, rather than resisting, this profit motive. Participants discussed the opportunity to use the duty to make safety investments commercially attractive – rewarding companies that innovate and compete on the quality of their protections. The objective would be to create a market in which better safety performance creates commercial advantage, alongside credible penalties when services fail to meet their obligations.

International examples illustrate how well-designed regulation can reshape these incentives. Under Canada’s proposed Digital Safety Act. For example, if the Digital Safety Commission of Canada is satisfied that a social media service provides adequate safeguards for children, it could *exempt* the provider from needing to prevent under 16-year-olds from accessing their service.⁴⁰ Australia’s social media minimum age restriction framework also considered an exemption, as was proposed in South Australia, but it was not included in the final legislation.⁴¹ Exemptions like these create incentives for services to pursue demonstrably safer design. **The aim of the duty should not only be to make unsafe services expensive to operate (‘sticks’), but to make safer services commercially competitive (‘carrots’).**

Convergence 7: Enhance transparency and independent scrutiny

Participants agreed that an effective duty requires independent capability to observe, test and scrutinise how online services operate. Regulator reporting and service risk assessments are important, but should not be the only source of evidence about whether risks are emerging or mitigations are working. Participants emphasised the importance of empowering the research community in Australia to undertake ongoing research, auditing and testing – summarised by one participant as ‘no accountability without multistakeholder observability’.

Participants suggested that Australia’s online safety regime should consider a mechanism for research access to data, and protections that enable researchers to provide independent scrutiny of big tech platforms in the public interest.

There was broad agreement that appropriately governed researcher access to platform data would be an important component of a successful digital duty of care regime. Participants noted that independent researchers play a critical role in identifying systemic risks, evaluating the effectiveness of mitigations and providing evidence to inform regulatory decision-making. Several international approaches were highlighted in the discussion. Participants highlighted Article 40 of the EU DSA, which requires very large online platforms and search engines to provide vetted researchers with access to data for the purposes of researching systemic risks.⁴²

‘There is no accountability without observability. With observability we can ensure digital platforms and services meet their duty of care to us all.’

There was common ground around the importance of providing greater certainty for researchers undertaking legitimate public-interest research. Participants noted that researchers can face legal, contractual and practical barriers and risks when investigating online platforms, including risks

associated with breaching platform terms of service. Concern was raised that, in Australia, it is not legal to create sock puppet accounts, as it is in Europe.

‘The regulator needs the support from private industry to actually map digital providers and where their risks are, e.g. external auditors.’

Participants also noted the limitations of relying solely on publicly observable information or sock puppet research accounts. While such methods can help identify harmful content, they offer only a limited window into how recommender systems and other platform features operate in practice. It was discussed that understanding system-level risks often requires access to underlying platform data and evidence about how services function for diverse, real users. Access to sequence data and other forms of operational data were highlighted as potentially important for understanding the pathways through which users are exposed to content and risks.

Participants emphasised that researcher access is not simply a matter of making more data available. Any access regime would need to balance transparency and accountability objectives with privacy, security, ethical and commercial considerations. Participants pointed to the contested implementation of the EU’s DSA Article 40 as a reminder that data-sharing arrangements require well-designed governance, clear safeguards and robust oversight.

With so few jurisdictions currently providing legal protections for researchers, by embedding these protections in the duty, Australia has a significant opportunity to become a global hub for world-leading research capable of driving long-term systemic change.



Implementation

Convergence 8: Coordinate a coherent regulatory system

Participants recognised the duty will sit within a much wider, increasingly complex and interconnected regulatory system, that includes existing online safety regulations as well other privacy, consumer protection and competition frameworks. Some overlap between these schemes was noted as inevitable and appropriate, but participants shared a concern regarding the risk of regulatory incoherence. There was agreement over the importance of clarity about respective regulatory roles, effective consultation across portfolios where responsibilities intersect, and mechanisms that enable regulatory to work collectively on emerging and cross-cutting issues.

This underscores the importance of effective coordination as a feature of the regulatory architecture.⁴³ Existing mechanisms such as the Digital Platform Regulators Forum (DP-REG) – which brings together eSafety, Australian Competition and Consumer Commission, Australian Communications and Media Authority and the Office of the Australian Information Commissioner – provide a solid foundation for this collaboration.⁴⁴ **The introduction of a duty creates the opportunity to consider how regulatory coherence is maintained as Australia's tech policy landscape becomes more complex** (capability 6.1.2 in TPD's AI Agency Tool).⁴⁵

Convergence 9: Match ambition with regulator capability

There was convergence that the ambition of the duty needs to be matched by sufficient regulatory capacity to monitor, supervise and enforce it effectively. The breadth of the proposed regime – including oversight of service providers' risk assessments – will create significant new demands on regulators, particularly eSafety, and participants cautioned against establishing an ambitious duty without the regulator powers and resources needed to give it practical effect.

'The big thing is the need for the regulator to be properly funded and resourced with consistent powers to make it work.'

There was support for exploring whether eSafety's information-gathering, investigative and enforcement toolkit remains fit for purpose for a systemic regulatory role, including by comparison to other Australian regulators. Some participants pointed to the document production and investigatory powers available to ACCC (section 155 powers) as relevant comparators.⁴⁶ A bill to expand the eSafety Commissioner's information gathering powers and increased penalties for non-compliance has since passed the Parliament on 10 September 2026.⁴⁷

Sufficient and sustainable funding was also agreed to be an important part of successful regulatory implementation. **Ireland's cost-recovery model under the *Digital Services (Levy) Act 2024*, which empowers the regulator to charge a levy on service providers to fund enforcement and regulatory functions, was raised as a model Australia should consider.**⁴⁸ This was noted as particularly important if the scope of harms being regulated by eSafety is expanded. Regardless, there was a sense that public expectations for what the regulators can deliver overnight would need to be managed.

'We desperately need a digital duty of care with a well-funded eSafety Commission.'

Participants also discussed emerging international approaches to user redress, including the Appeals Centre Europe, which provides an independent avenue in the EU for resolving disputes between users and platforms.⁴⁹

Convergence 10: Cultivate public legitimacy and political feasibility

Participants emphasised that the success of the duty will depend not only on sound regulatory design, but also on clarity of purpose and sufficient public and political support. There was a shared view that, despite the prominent public conversation about online harms, the concept of a duty of care is not widely understood. **Participants agreed that clarifying the policy intent of ‘what success looks like’ and being able to communicate that in clear public messaging, is essential to success.** One participant suggested the slogan, which we have adopted as the report title – **Digital duty of care: make tech care.**⁵⁰

There was common ground around the importance of preserving the political feasibility of the duty. Participants noted that the public debate on online safety can quickly devolve into entrenched positions, and the successful design, debate and implementation of the duty will require navigating a contentious and highly politicised context.

A duty that is technically sound but unable to secure broad support risks becoming stalled, weakened or overtaken by political tensions. Participants agreed that a durable reform will require careful management of expectations, early cross-partisan engagement where possible, and a focus on outcomes that are understandable and meaningful to Australians.

‘Any new duty of care must also come with a broad community-based learning campaign.’

A recurring theme was the uneven evidence base regarding Australians’ expectations of online safety regulation. Participants referred to ‘the harms Australians care about’ and community views on appropriate online protections. Yet there was also a recognition that policymakers currently have only a partial understanding of what responsibilities Australians expect online services to take on and what trade-offs they are prepared to accept in pursuit of safety.

‘This is a very important reform and it’s critical that we get this right!’

There was support for developing a stronger evidence base regarding Australians’ expectations of online safety regulation. This could include nationally representative research into the harms Australians view as most significant, the responsibilities they believe services should bear, the outcomes they expect a digital duty of care to achieve, and the trade-offs they consider reasonable. Particular attention should also be given to engaging directly with vulnerable groups, such as First Nations Australians, and young people, who are frequently at the centre of these debates but often under-represented within them.



DIVERGENCES

Divergence 1: How to balance rights for safety?

A fundamental tension permeates all online safety debates and underpins most of the following divergences on the Digital Duty of Care: how to reconcile the pursuit of safety while reconciling the range of human rights associated with Australians' online lives?

Participants observed that interventions designed to reduce one category of harm can create new risks or constrain human rights.

It was pointed out that these issues are not merely theoretical. One participant captured this tension through the example of encryption. This same technology that helps a victim-survivor of domestic violence communicate safely and privately can also make it more difficult to detect and prevent the production and distribution of child sexual abuse material.

Another participant noted that Australia's existing online safety framework (including the Online Safety Codes and Standards), have the objective of increasing user safety but also impose age assurance obligations – which, for many, enlivens human rights concerns such as privacy.

Concerns were raised that a strong duty of care may activate public concerns around censorship and curtailing freedom of speech. Others observed that maintaining online spaces where Australians can safely and meaningfully participate is also an important enabler to other rights – such as the right to health, taking part in public affairs, protection from exploitation, violence and abuse, and of equality and non-discrimination.⁵¹

These examples demonstrate that policymakers are increasingly being required to balance respect for multiple different human rights when considering how to make online spaces safe.

It was noted that the doctrine of proportionality in human rights law is specifically designed to address tensions between legitimate public objectives and rights limitations. This doctrine asks, in effect, if a measure pursues an important objective – such as safety or protection from harm – does it limit rights only to the extent that is justified, necessary and proportionate? This provides a useful framework for assessing a digital duty of care, particularly where efforts to advance online safety may affect rights such as freedom of expression, privacy, participation or access to information.

Despite the differences above, participants broadly agreed on the need to take a comprehensive view of harm, including to recognise that interventions to address one harm may create other harms or limit rights.

The key divergence was *how* a digital duty of care should balance human rights and safety where those objectives come into tension. Participants repeatedly returned to proportionality as the framework for navigating these trade-offs, while recognising that reasonable disagreement remains about where the balance should fall.

Divergence 2: Children or all Australians?

A central policy question raised throughout the dialogue was whether the duty should establish baseline protections owed to all Australians (as proposed in the government's issues paper on a digital duty of care)⁵² or primarily operate as a child-safety regime. While there was strong convergence that protecting children should be a central purpose of the duty, grounded in the well-established principle of the best interests of the child,⁵³ participants diverged on whether the obligation to take reasonable steps to prevent foreseeable serious harms should extend more broadly to adults.

'Broad categories of risk that provides protection for everyone – not just children.'

Most participants argued that the duty should be primarily **focused on children and young people**. For some, this was a principled position: children have distinct legal rights, development vulnerabilities and capacities for decision-making that justify strong protections.⁵⁴ Others arrived at a similar conclusion for more pragmatic reasons. They considered a child-focused duty easier to define, and less likely to become entangled in difficult debates about balancing adult safety, freedom of expression and adults' right to assume their own risk.⁵⁵

'Harms present for children in many ways – from content to addiction – and we need to solve for them all.'

Others argued that the duty should apply as a minimum **protection for all Australians, not only children**. Participants observed that many serious online harms, such as technology-facilitated abuse, are regularly experienced by adults. Some participants also noted that some of the broader protections currently being considered or implemented for children, such as the Children's Online Privacy Code, may also be desirable for adults. From this perspective, limiting protections to children risks creating an unmanaged 'safety cliff' at the point a person turns 18 years old.

Australia's lack of a comprehensive statutory human rights framework emerged as a clear point of discussion. Some participants considered this context means it is more pragmatic to start with children. Others argued the reverse: the absence of broader rights protections make it more important for extending baseline online safety protections to adults as well.

Divergence 3: What harms should the duty address?

Another decision facing policymakers is where the boundary of the duty should be drawn. In addition to agreeing that the duty should apply to service design (Convergence 3), **participants broadly agreed that services should take reasonable steps to prevent illegal activity occurring through their services**. However, views diverged on how far the duty should extend beyond clearly unlawful conduct into harms that are lawful, cumulative or systemic in nature.

'We must make clear what is unacceptable and scope our harms around this!'



The harms listed below were discussed at the Design Dialogue starting with narrow and becoming more expansive:

- There was strong common ground on a duty to prevent **illegal harms** (Class 1 under the *Online Safety Act 2021*). Examples raised include child sexual exploitation and abuse, terrorist and violent extremist content, image-based abuse, criminal harassment, hate offences and other unlawful conduct. While there was discussion about enforcement and implementation, there was little disagreement that providers should take reasonable steps to prevent these harms from occurring on their services.
- Beyond these comparatively established categories, participants diverged on whether the duty should address **financial harms**. Scams were repeatedly noted as a major and growing source of harm experienced by Australians online. Some participants argued that scams, gambling related harms, unlawful advertising practices and other financially harmful activities should fall within scope because they are foreseeable harms facilitated through online services. Participants noted the UK's approach of including scams within the online safety framework,⁵⁶ but also noted Australia's separate Scam Prevention Framework legislated in 2025.⁵⁷
- Participants also discussed the category of **harmful but lawful** content and conduct. Examples include suicide and self-harm material, age-inappropriate sexual content, extreme violence and other harms currently addressed through Australia's Class 2 Online Safety Codes and Standards.⁵⁸ There was broad agreement that these harms should be prevented for child users; however, views diverged on whether the same expectation should apply for adults. This question is closely linked to Divergence 2 (Children or all Australians?) and underpins TPD's phased implementation recommendation (Recommendation 2).
- Participants considered what could be called '**precursor harms**': content and conduct that falls below a legal threshold but may be a slippery slope to later, more serious harms. Participants noted that radicalisation pathways towards terrorism, violent extremism and other criminal conduct often emerge well before content becomes unlawful or reaches a threshold of serious harm. Similar arguments were raised in relation to grooming, coercive behaviours and other forms of escalation. Some participants argued that focusing only on conduct that has already crossed a legal or seriously harmful threshold misses important opportunities for upstream prevention. From this perspective, a duty intended to prevent foreseeable harm should allow/require intervention earlier in the pathway. Others raised concerns about drawing such boundaries upstream and the implications on proportionality and free speech.
- Discussion also extended to **cumulative harms**, where no individual exposure may be sufficiently harmful on its own, but repeated exposure compounds into serious harm over time. Examples included misogynistic content ecosystems, harmful influencer cultures and other recommendation-driven experiences that can shape attitudes, behaviours and relationships through repeated exposure. Participants used the example of emotional dependency or attachment arising through interactions with increasingly sophisticated, personalised and anthropomorphised AI chatbots. Unlike pathway harms, which are concerning because they may

'The law should be expansive enough to cover not just illegal behaviour but "lawful and awful". This policy needs comprehensive gender analysis.'

lead to a future harmful threshold, cumulative harms arise through the gradual compounding of experiences and exposure.

- The broadest category discussed was **systemic harms**, where the impact is felt not by an individual user but by communities, institutions or society more broadly. Participants pointed to misinformation and disinformation, public health, civic discourse, media pluralism, electoral integrity and trust in democratic institutions as examples. Several participants referenced the EU DSA, which takes a broader systemic-risk approach and includes considerations of risk to democratic processes and public wellbeing.⁵⁹

'The scope of the digital duty of care is key. It must capture the full range of harms from user content; to AI generated harmful capability uplift (bioweapons), to AI agents autonomously causing harm.'

Across these discussions, participants repeatedly returned to questions of proportionality and practicality. Some argued that the broadest conception of harm is necessary if the duty is to address the full spectrum of harms occurring online. Others cautioned that adopting a broader approach introduces real policy complexity, such as the challenge of establishing a clear causal link between particular platforms and boarder societal outcomes. **Participants observed that the further the duty expands beyond illegal harms towards cumulative or systemic harms, the more complex questions become around causation, evidence and appropriate intervention.**

Participants also noted that expanding the scope too far risks diluting regulatory attention and platform resources, whereas a narrower scope reduced the focus only on the

most serious of harms. There was also acknowledgement that the broader the range of harms in scope, the more fraught the reform's political passage might become.

Divergence 4: Risk-based or outcomes-based duty?

Another design decision is whether the duty is focused on reducing risks and preventing harms or whether it should also require services to promote positive outcomes for users and society.

Participants broadly agreed that online services should be subject to an overarching duty to prevent harm before it occurs (Convergence 1). However, some participants questioned whether focusing solely on risks and harms provides a sufficiently clear vision of what the duty is ultimately designed to achieve.

Some participants supported a **risk-based** approach, framing the duty primarily as a product safety-style obligation. Analogies were drawn with duties that apply in sectors such as pharmaceuticals, consumer products and environmental protection, where organisations are expected to identify, assess and mitigate foreseeable risks before harms occur. Under this model, the principal role of the duty would be to reduce the likelihood and severity of online harms (although participants were not advocating for pursuing a zero harm/risk approach).

'This is actually about giving rights and protections back to our Australian population, not taking them away.'



Others put forward the merit of a more **outcomes-based** approach.⁶⁰ Rather than focusing solely on preventing harm, this approach would require services to actively promote positive outcomes through the design, deployment and governance of their systems. Participants discussed outcomes such as safe, inclusive and healthy online environments, meaningful participation, gender equality, access to information and other public-interest objectives. From this perspective, the purpose of the regulation would be to encourage the conditions under which Australian individuals, and society writ large, can flourish online. Participants pointed to the EU DSA which places greater emphasis on fundamental rights and public interest considerations when assessing platform responsibilities.

However, reservations were raised about an outcomes-based model. A recurring question was how government, regulators and services would agree on what constitutes a desirable outcome in practice. Participants noted that concepts such as wellbeing, participation, democratic engagement or inclusion can be difficult to define, measure and balance against one another. Participants similarly noted that these metrics vary widely from place to place, and that regulators lack data to account for targeted cohorts, such as regional and remote First Nations communities. This challenge was seen as particularly significant in Australia, which lacks a comprehensive statutory human rights framework that could provide a shared normative foundation for such assessments.

Participants also questioned the extent to which services can be held directly accountable for complex societal outcomes. It was argued that while providers may be able to influence risks through product design, recommendation systems, user controls and governance processes, outcomes such as public trust, democratic participation or social cohesion are shaped by many factors beyond the control of any individual service.

'While it needs to be practical, it should be ambitious and take a rights-based approach that not only protects our safety but also our human dignity.'

Despite these differences, the discussion returned to the importance of clearly articulating what success looks like under the duty. Strikingly, there was no clear consensus when one participant challenged the room asking, 'What are we trying to achieve with the digital duty of care?'

Participants noted that the duty will ultimately need to answer not only what harms should be prevented (Divergence 3) but also how Australians will know whether it is working.

Some participants considered a risk-based framing more politically feasible, rather than requiring agreement about broader societal objectives. Others argued that an outcomes-based model offers a more ambitious vision of what well-designed policy can do to create positive public impacts.

The question for policymakers therefore is whether the duty is intended to prevent negative outcomes, promote positive outcomes, or both.

Divergence 5: Universal safeguards or personalised protections?

Another question for policymakers is whether a generally applicable duty should be implemented through broadly consistent safeguards for all users or through protections tailored to particular users, vulnerabilities and contexts.

Participants agreed that a duty should take a proportionate approach to risk. However, they diverged on whether safer online services are best achieved through universal safeguards that apply to everyone, and/or through protections calibrated to individual users or groups.

This question is distinct from whether the duty should protect only children or all Australians (Divergence 2). Even if the duty establishes a baseline obligation towards every user, policymakers must still decide whether services should provide broadly consistent protections or whether they should be expected to provide different levels of protection to different users.

Some participants argued that services should default to a high common standard for all users rather than placing the burden on individuals to find and activate protective settings. From this perspective, services should be safe by default. Participants discussed the importance of user control, including whether high-risk features such as personalised recommender systems should be opt-in rather than opt-out.

Others argued that harms are not experienced evenly across the population and that 'reasonable' protections should reflect this reality. Participants noted that certain harms are disproportionately experienced by particular groups, such as women, First Nations Australians, and people living with disability. Harms are often amplified by highly personalised systems. From this perspective, uniformly applying the same protections to everyone may leave some users under-protected while unnecessarily restricting others.

'Privacy and safety are not a trade-off, but mutually reinforcing.'

How should services identify users who need greater protection?

There was discussion that a tailored approach creates a second policy question: how services should appropriately determine which users require additional protections and safety settings?

Some participants argued that effective risk mitigation could involve protection of vulnerable groups through tailored user experience.⁶¹

However, other participants noted a potential paradox. The personalised systems that can enable more targeted or proportionate protections are often the same systems that have attracted concern for creating or amplifying harm. Providing tailored safeguards may require services to collect, analyse or infer sensitive information about users, and these profiling practices can themselves create privacy and discrimination risks. Participants raised concerns about privacy, participation, anonymity, exclusion and trust in online services.

Divergence 6: How prescriptive?

A recurring question was how much certainty should be embedded into the duty, and how much flexibility should be left to regulators and the courts over time.

'A principles approach is best.'

Participants broadly agreed that the duty should take the form of an overarching and enduring obligation (Convergence 2). However, views diverged on what level of prescription, guidance and rule-making power is needed beneath that overarching framework.

Certainty or flexibility?

Some participants discussed that specific rules would provide greater confidence that services will be held accountable for addressing particular harms. From this perspective, prescribing categories of harm and minimum expectations can create a clear regulatory 'floor' below which services cannot fall. Participants also



noted that additional specificity may provide industry with greater certainty regarding their compliance obligations, particularly in relation to existing arrangements in Australia's Online Safety Codes and Standards. Some participants pointed to the SMMA regulatory uncertainty as a cautionary tale about the importance of clarity.⁶² The discussion extended to whether compliance with codes, standards or other prescribed requirements should provide a service with a form of safe harbour under the duty (creating a 'carrot' for compliance rather than just a stick).

Other participants cautioned that such a specific approach might risk reducing compliance into a box-ticking exercise. They raised concerns it could prevent regulators from acting where a service has technically complied with a code but nonetheless not taken reasonable steps to prevent a foreseeable serious harm. The UK was noted as an example of where safe harbours mean that compliance with Ofcom's Codes of Practice can allow services to be treated as compliant with statutory duties while serious harms remain.

More broadly, participants differed on whether prescribing specific harms and safeguards strengthens or narrows the duty. While some saw prescription as a useful way to lock in minimum standards, others argued that too much specificity risks distracting or diluting efforts to anticipate and mitigate broader, unlisted risks.

Rule-making versus common law and standards pegging

Participants also diverged on how the duty should evolve as technologies, products and harms continue to change and the merit of ministerial and regulatory rule-making powers.

Some argued that delegated rule-making powers will be valuable to keep the framework relevant over time. The ability to introduce requirements, clarify expectations or respond to emerging risks without requiring new primary legislation was viewed as an important way of future-proofing the duty. In this regard there was strong support for such rules to be disallowable instruments (and, therefore, subject to parliamentary scrutiny by exception). Questions were raised about whether additional safeguards, such as mandatory public consultation or stronger scrutiny processes, should accompany any rule-making authority.

In contrast, others questioned whether extensive rule-making powers are necessary if the overarching duty is genuinely principles-based and technology neutral.

Participants argued that 'reasonable steps' is a well-established legal principle that can evolve further through juridical interpretation and case law. Adopting the EU AI Act's reference to standards 'generally acknowledged state of the art' could reinforce this by ensuring the duty is assessed against recognised and developing technical and governance practice. This approach would reduce the need for prescriptive rule-making, while allowing the duty to evolve at the pace of technology.

It was argued that the value of an overarching duty lies precisely in providing a framework for obligations to mature at the speed of innovation. In contrast an overly prescriptive rules-based framework, it was suggested, may inadvertently limit agility by requiring formal updates as technology and harms evolve.

There were also pragmatic concerns. Several participants noted that itemising specific harms or obligations may create particular points of political contention and provide targets for opponents of

'Gender-based violence prevention and tech-facilitated gender-based violence needs to be need to be Codes.'

reform. A more principles-based model was viewed by some as less susceptible to polarised debates about individual categories of content or conduct (Convergence 3).

Overall, there was a shared desire to balance providing industry with certainty and the ability to meaningfully hold services to account as technology rapidly evolves over time.

Divergence 7: Bold or incremental reform?

A final point of divergence concerned the pace and sequencing of reform. Participants differed on whether the proposed duty should be used to secure a comprehensive reform now or establish a starting point that can be expanded over time.

Some participants favoured a more incremental approach. They argued that legislation should ‘not let the perfect be the enemy of the good’. It should focus on securing broad agreement around a basic version of the duty and avoid becoming stalled by attempts to resolve every contested issue at once. From this perspective, compromise is an inevitable feature of public policy and there is value in securing achievable improvements now rather than risking no reform at all. Participants pointed to the practical realities of legislative design and parliamentary negotiation, making the case that a phased approach could allow the regime time to mature over time as evidence, regulatory capability and community understanding develop. This was described as ‘radical incrementalism’.

Others argued that the introduction of the duty represents a rare opportunity for structural reform and that government should avoid being overly cautious. They contended that if a duty is intended to reshape incentives and move Australia towards a more future-proofed model of online safety regulation, the foundational principles should be established from the outset. Some expressed concern that failing to address key design questions now may leave important gaps unresolved and reduce the likelihood of more ambitious reforms being pursued in the future. Once the issue has been addressed by Parliament, the opportunity for significant reform may not re-emerge for some time.

The discussion frequently explored the relationship between ambition and political feasibility. Several participants noted that the broader the scope of the duty, the more likely it is to attract opposition from stakeholders concerned about regulatory overreach or unintended consequences. Some participants pointed to recent policy debates, including the Misinformation and Disinformation Bill, as examples of how ambitious reform can become polarised.⁶³

At the same time, others cautioned against allowing concerns about political controversy to unnecessarily narrow the reform. From this perspective, the existence of difficult debates is not itself a reason to avoid addressing emerging harms or pursuing a more ambitious vision for online safety. Rather, it reinforces the importance of clearly articulating what problem the duty is intended to solve and how success will be measured (Convergence 10).

The question is therefore whether the legislation should be designed as a comprehensive reform package or as the first step in a broader, staged program of reform. That decision will shape how policymakers approach many of the other design choices identified throughout this report, such as the scope of harms, inclusion of adults and level of prescription contained within the regime.



APPENDIX: PARTICIPANTS

TPDi gratefully acknowledges the following organisations and individuals who participated in TPDi's Digital Duty of Care Design Dialogue.

Participation in the Design Dialogue does not indicate endorsement of the findings or recommendations of this report. Affiliations are listed as at the time of consultation.

Civil society

Alannah & Madeline Foundation, Sarah Davies AM
Australian Human Rights Commission, Patrick Hooton
Centre of the Public Square, Peter Lewis
Digital Rights Watch, Tom Sulston
First Nations Digital Inclusion Advisory Group, Lyndon Ormond-Parker
Global Shield Australia, Devon Whittle
Good Things Foundation Australia, Jess Wilson
Independent Reviewer of the Online Safety Act, Delia Rickard PSM
International Justice Mission Australia, David Braga
Minderoo Foundation, Freya Jansens
Movember, Krista Fisher
Reset Tech, Dr Rys Farthing
Scanlon Foundation, Henry Sherrell
Teach Us Consent, Pnina Hagege
TPDi Youth Ambassadors, Eve Carlin, Bianca Kendrick and George Trigenis
UNICEF Australia, John Livingstone

Australian Parliament

The Hon Anika Wells MP; Kate Chaney MP, Zoe McKenzie MP & Senator David Shoebridge
Office of the Minister for Communications, Summer Brady
Office of the Prime Minister, Hannah Frank

Government

Australian Competition and Consumer Commission, David Abkiewicz
Australian Federal Police, Deputy Commissioner Ian McCartney, Ben Lamont
Delegation of the European Union, Dr Oliver Landwehr
Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Sarah Vandenbroek and Andrew Hyles
Office of the Australian Information Commissioner, Liz Tydd and Kate Bower
Office of the eSafety Commissioner, Kathryn King and Ashley Katz
British High Commission Canberra, Laura Giles
US Embassy Canberra, Philip Oh

Industry

Apple, Josh Machin
auDA, Bruce Tonkin, Marina Go, Michael Lewis and Annaliese Williams
Bower Group Asia on behalf of LEGO Group, Michael McNeill
Business Council of Australia, Don Gomez
Commonwealth Bank of Australia, Sabina Streatfeild
CyberCX, Jordan Newnham
Cybernetic Shield, Jessica Sears
DIGI, Dr Jenny Duxbury
First Movers Co, Yasmin London
Google, Melissa Chin
Macquarie University, Dr Danielle Einstein
Meta, Cheryl Seeto
Minister for Government Services' Independent Advisory Board, Leanne Ho
Protostar Strategy, Dr Tobias Feakin
Tata Consultancy Services, Robert Law
TikTok, Jessika Lofstedt
Wotton + Kearney, Claire Thurstans

Research & education

ARC Centre of Excellence for Automated Decision Making and Society, Professor Christine Parker
ARC Centre of Excellence for the Digital Child, Dr Rebecca Ng
Australian Internet Observatory and the University of Queensland, Professor Nicholas Carah
Global Institute for Women's Leadership, Dr Elise Stephenson
Independent Education Union of Australia, Amanda Hioe
Monash University, Professor Rashina Hoda
Protocol, Emma Cooney



ENDNOTES

- ¹ Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCA), *Exposure draft – Online Safety Amendment (Digital Duty of Care) Bill 2026*, Australian Government, Canberra, 8 September, accessed 10 September 2026. <https://www.infrastructure.gov.au/department/media/publications/exposure-draft-online-safety-amendment-digital-duty-care-bill-2026>
- ² All references to 'services' or 'online services' in this report includes all 8 sections of the online industry as defined under section 135 of the *Online Safety Act 2021* (Cth), including 'equipment' (devices).
- ³ As defined in the *Online Safety Act 2021* (Cth), 'Australians' are defined as someone who is 'ordinarily resident in Australia'.
- ⁴ D Speers, 'Opt-out laws for social media algorithms to be introduced to parliament', *ABC News*, accessed 7 September 2026. <https://www.abc.net.au/news/2026-09-06/opt-out-laws-social-media-algorithm-parliament-government/107121192>
- ⁵ R Hoda, *Future-proofing Australia's digital duty of care – recommendations for closing the emerging technologies gap*, Monash University, 2026. <https://doi.org/10.26180/33274431.v3>
- ⁶ eSafety Commissioner, *Safety by Design*, eSafety website, 8 January 2026, accessed 11 September 2026. <https://www.esafety.gov.au/industry/safety-by-design>
- ⁷ Teach Us Consent, *Fix our feeds*, teachusconsent.com, n.d., accessed 7 September 2026. <https://www.teachusconsent.com/fix-our-feeds>
- ⁸ As recommended by D Rickard PSM, *Report of the statutory review of the Online Safety Act 2021*, October 2024, Commonwealth of Australia, chapter 13. https://www.aph.gov.au/Parliamentary_Business/Tabled_Documents/9184
- ⁹ The Telecommunications Industry Levy, established under the *Telecommunications (Industry Levy) Act 2012* (Cth) and administered through the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth), funds public interest telecommunications services and associated administrative costs. More directly, the Annual Carrier Licence Charge, imposed under the *Telecommunications (Carrier Licence Charges) Act 1997* (Cth), recovers certain telecommunications-related regulatory costs, including costs incurred by the Australian Communications and Media Authority, the Australian Competition and Consumer Commission and the responsible department.
- ¹⁰ Ireland's *Digital Services (Levy) Act 2024* provides the statutory basis for industry-funded digital services regulation, including by amending section 21 of the *Broadcasting Act 2009* (Ireland) to extend the Irish media commission's levy powers and, by amending the *Digital Services Act 2024* (Ireland), to give the Irish Competition and Consumer Protection Commission levy powers for specified digital services enforcement functions. See also chapter 13 of Rickard, *Report of the statutory review of the Online Safety Act 2021*.
- ¹¹ State of California Department of Justice, *Attorney General Bonta Secures Transformative \$17 Billion Settlement with Meta, Proposed Settlement Includes Fundamental Changes to Instagram and Facebook* [media release], 26 August 2026, accessed 11 September 2026. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-transformative-17-billion-settlement-meta>; New Mexico Department of Justice, *Court Orders Meta to Pay \$942 Million and Overhaul Protections for Children on Facebook and Instagram in Landmark New Mexico Ruling* [media release], 7 August 2026, accessed 7 September 2026. <https://nm DOJ.gov/press-release/court-orders-meta-to-pay-942-million-and-overhaul-protections-for-children-on-facebook-and-instagram-in-landmark-new-mexico-ruling/>

¹² See recommendation 26 in Rickard, *Report of the statutory review of the Online Safety Act 2021*, chapter 13; see also Consumer Policy Research Centre, *Someone to turn to*, 22 June 2026, accessed 7 September 2026. <https://cprc.org.au/report/someone-to-turn-to>

¹³ The Office of Impact Analysis (OIA), 'Social media age limit', OIA website, 14 November 2024, accessed 10 September 2026. <https://oia.pmc.gov.au/published-impact-analyses-and-reports/social-media-age-limit>; R French AC, *Report of the independent legal examination into banning children's access to social media*, report to the Government of South Australia Department of the Premier and Cabinet, September 2024.

¹⁴ BILL C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts, 1st session, 45th Parl, Canada, 2025-2026 (first reading, 10 June 2026). <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>

¹⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1, Article 40. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>

¹⁶ DITRDCA, *Exposure draft – Online Safety Amendment (Digital Duty of Care) Bill 2026*.

¹⁷ Rickard, *Report of the statutory review of the Online Safety Act 2021*.

¹⁸ DITRDCA, *A digital duty of care for Australia* [issues paper].

¹⁹ DITRDCA, *Exposure draft – Online Safety Amendment (Digital Duty of Care) Bill 2026*.

²⁰ European Commission, *The Digital Services Act*, digital-strategy.ec.europa.eu, n.d., accessed 7 September 2026. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>

²¹ European Commission, *Commission preliminary finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors* [media release], 24 July 2026, accessed 7 September 2026. <https://digital-strategy.ec.europa.eu/en/news/commission-preliminary-finds-tiktok-breach-digital-services-act-failing-ensure-safe-accounts-minors>

²² *Online Safety Act 2023* (UK) c 50. <https://www.legislation.gov.uk/ukpga/2023/50/contents>

²³ UK Department for Digital, Culture, Media and Sport and Home Office, *Online harms white paper*, 8 April 2019, accessed 7 September 2026. <https://www.gov.uk/government/consultations/online-harms-white-paper>

²⁴ UK Government, *Online Safety Act: explainer*, GOV.UK website, 24 April 2025, accessed 7 September 2026. <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>

²⁵ State of California Department of Justice, *Attorney General Bonta Secures Transformative \$17 Billion Settlement with Meta, Proposed Settlement Includes Fundamental Changes to Instagram and Facebook* [media release], 26 August 2026, accessed 11 September 2026. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-transformative-17-billion-settlement-meta>

²⁶ J Inman Grant (eSafety Commissioner), 'Addressing deepfake image-based abuse' [blog], esafety.gov.au, 24 July 2024, accessed 11 September 2026. <https://www.esafety.gov.au/newsroom/blogs/addressing-deepfake-image-based-abuse>

²⁷ eSafety Commissioner, *AI chatbots and companions – risks to children and young people* [online safety advisory], 18 February 2026, accessed 7 September 2026. <https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people>

²⁸ eSafety Commissioner, *From smart cars to tracking devices: technology's increasing role in coercive control and family and domestic violence* [online safety advisory], 30 November 2025, accessed 11 September 2026. <https://www.esafety.gov.au/newsroom/blogs/from-smart-cars-to-tracking-devices-technologys-increasing-role-in-coercive-control-and-family-and-domestic-violence>

²⁹ *Scams Prevention Framework Act 2025* (Cth). <https://www.legislation.gov.au/C2025A00015/asmade/text>; Attorney-General's Department, *Privacy reform – consultation on Exposure Draft legislation*, Attorney-General's website, 31 August 2026, accessed 7 September 2026. <https://consultations.ag.gov.au/rights-and-protections/privacy-reform/>; The Treasury, *Revitalising National Competition Policy*, Treasury website, n.d., accessed 7 September 2026. <https://treasury.gov.au/review/competition-review-2023/ncp>



- ³⁰ Tech Policy Design Institute, *About us*, TPDi website, n.d., accessed 7 September 2026. <https://techpolicy.au/about-us/>
- ³¹ Demographic figures are approximate and based on available self-identification data.
- ³² Rickard, *Report of the statutory review of the Online Safety Act 2021*.
- ³³ UK Government, *Online Safety Act: explainer*.
- ³⁴ Alannah & Madeline Foundation, *Navigating the 4Cs of online safety*, eSmart website, n.d., accessed 7 September 2026. <https://be.esmart.org.au/digital-licence-hub/navigating-the-4cs>
- ³⁵ ABC (Australian Broadcasting Corporation), 'Meta trial that could reshape Facebook and Instagram gets underway in California', *ABC News*, 19 August 2026, accessed 7 September 2026. <https://www.abc.net.au/news/2026-08-19/meta-trial-that-could-reshape-facebook-and-instagram-begins/107052672>
- ³⁶ State of California Department of Justice, *Attorney General Bonta Secures Transformative \$17 Billion Settlement with Meta, Proposed Settlement Includes Fundamental Changes to Instagram and Facebook* [media release], 26 August 2026, accessed 11 September 2026. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-transformative-17-billion-settlement-meta>
- ³⁷ ABC, 'Meta trial that could reshape Facebook and Instagram gets underway in California'.
- ³⁸ European Commission, *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act* [media release]; European Commission, *Commission preliminarily finds the addictive design of Instagram and Facebook in breach of the Digital Services Act* [media release], 10 July 2026, accessed 7 September 2026. <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-addictive-design-instagram-and-facebook-breach-digital-services-act>
- ³⁹ DITRDCSA, *New industry codes to protect children from online pornography* [media release], 2 July 2026, accessed 7 September 2026. <https://minister.infrastructure.gov.au/rowland/media-release/new-industry-codes-protect-children-online-pornography>
- ⁴⁰ BILL C-34 (Canada); French AC, *Report of the independent legal examination into banning children's access to social media*.
- ⁴¹ TPDi, 'Part 2: The politics (Australia v Social Media mini-series)' [podcast], TPDi, 13 November 2025. <https://techpolicy.au/podcast/part-2-the-politics-australia-v-social-media-mini-series/>
- ⁴² *Digital Services Act* (EU).
- ⁴³ Tech Policy Design Centre, *Tending the tech ecosystem*, TPDi website, 2022. <https://techpolicy.au/report-tending-the-tech-ecosystem/>
- ⁴⁴ Digital Platform Regulators Forum, *Regulators strengthen joint oversight of digital platforms* [media release], 17 June 2026, accessed 7 September 2026. <https://dp-reg.gov.au/regulators-strengthen-joint-oversight-digital-platforms>
- ⁴⁵ TPDi, *Expanding AI sovereignty to AI agency*, TPDi website, 2026, accessed 11 September 2026. <https://ai.techpolicy.au>
- ⁴⁶ Australian Competition and Consumer Commission, *ACCC guidelines – use of section 155 powers*, 29 July 2022, accessed 11 September 2026. <https://www.accc.gov.au/about-us/publications/guidelines-on-the-use-of-section-155-powers>
- ⁴⁷ Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill 2026. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r7512
- ⁴⁸ Department of Enterprise, Tourism and Employment, *Minister Calleary welcomes approval of Digital Services (Levy) Bill* [media release], 11 July 2024, accessed 7 September 2026. <https://enterprise.gov.ie/en/news-and-events/departments-news/2024/july/202407112.html>
- ⁴⁹ Appeals Centre Europe website, accessed 7 September 2026. <https://www.appealscentre.eu/>
- ⁵⁰ With consent, we attribute the origin of this slogan to Peter Lewis, host of 'Burning platforms' podcast.

⁵¹ Attorney-General's Department, *Public sector guidance sheets*, Attorney-General's website, n.d., accessed 7 September 2026. <https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets>

⁵² DITRDCA, *A digital duty of care for Australia* [issues paper].

⁵³ Australian Law Reform Commission, 'The best interests principle', *Seen and heard: priority for children in the legal process* [ALRC Report 84], chapter 16, 29 July 2010. <https://www.alrc.gov.au/publication/seen-and-heard-priority-for-children-in-the-legal-process-alrc-report-84/16-childrens-involvement-in-family-law-proceedings/the-best-interests-principle/>

⁵⁴ D Einstein et al., 'Unfiltered access, unseen harms: a developmental and public health critique of digital rights discourse', *International Journal of Environmental Research and Public Health*, 2026, 23(3). <https://www.mdpi.com/1660-4601/23/3/364>

⁵⁵ DITRDCA, *Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2024* [media release], 24 November 2024, accessed 7 September 2026. <https://minister.infrastructure.gov.au/rowland/media-release/communications-legislation-amendment-combating-misinformation-and-disinformation-bill-2024>

⁵⁶ L Woods and A Antoniou, 'Advertising and the Online Safety Act 2023', *Journal of Media Law*, 2025, 17(2):490–520. <https://www.tandfonline.com/doi/full/10.1080/17577632.2025.2606428#abstract>

⁵⁷ *Scams Prevention Framework Act 2025* (Cth). <https://www.legislation.gov.au/C2025A00015/asmade/text>

⁵⁸ S Floreani, *Explainer: the Online Safety Bill*, Digital Rights Watch website, 11 February 2021, accessed 7 September 2026. <https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-bill/>

⁵⁹ *Digital Services Act* (EU).

⁶⁰ C Collins et al., *Digital duty of care policy brief*, ARC Centre of Excellence for Automated Decision-Making and Society, 1 June 2026, p 10. <https://www.admscentre.org.au/digital-duty-of-care-for-online-safety-and-platform-accountability-in-australia/>

⁶¹ Hoda, *Future-proofing Australia's digital duty of care – recommendations for closing the emerging technologies gap*.

⁶² C Armstrong, 'Social media age ban faces High Court challenge as government declares it will not be 'intimidated' by legal threats', *ABC News*, 26 November 2025, accessed 7 September 2026. <https://www.abc.net.au/news/2025-11-26/australia-social-media-ban-faces-legal-challenge/106056528>

⁶³ N Fraser, 'What's next for misinformation regulation?', *Parliamentary Library blog*, 2 July 2025. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Flag_Post/2025/July/Whats_next_for_misinformation_regulation