



Digital Duty of Care stakeholder consultation May - June 2026: Key Outcomes

Stakeholder consultation on a proposed Digital Duty of Care model, to be legislated under the *Online Safety Act 2021* (the Act), was conducted in May and June 2026, informed by an [issues paper](#). More than 40 consultation meetings were undertaken in this period, with online services, online safety advocacy groups, child safety groups, organisations representing vulnerable communities, and technology and online safety experts from academia. Key themes captured to date are outlined below.

Theme	Key Findings
Overarching feedback	• There is broad support for introducing a Digital Duty of Care (DDoC) across all stakeholders. • There was general agreement among stakeholders that the DDoC will enable the necessary shift from reactive content moderation to proactive, systems-based safety, addressing service features, which will improve safety outcomes. • Industry believes the DDoC has the potential to reduce regulatory complexity and improve regulatory certainty. • Industry advocated for the regulatory burden under a DDoC to be proportionate to the online safety benefit and, where possible align with regulatory frameworks of international counterparts. • Differing stakeholder priorities highlight the need to strike the right balance between regulatory certainty and ability for the Act to respond to emerging harms and technology changes. • Some stakeholders highlighted the importance of considering impacts on open online discourse, while advancing safety and privacy of Australians.
Focus on features and design	• Online safety advocates and groups representing vulnerable communities strongly endorsed the DDoC moving beyond content-level regulation to system design and platform features. • Key systemic risks identified by online safety advocacy groups and experts included: ○ Addictive design and problematic use ○ Algorithmic amplification and targeting (e.g. outrage monetisation, creation of echo chambers). • These groups also emphasised the importance of: ○ Safety by design ○ Default safety settings (opt-out rather than opt-in).
Algorithmic systems as a central challenge	• Online safety advocates and experts identified algorithms as a major driver of harm (e.g. radicalisation, amplification of extreme views, harmful content loops). • Suggested approaches to mitigate algorithm related harms included: ○ User control (e.g. ability to disable recommender systems) ○ Transparency about metrics used to drive algorithms.

Theme	Key Findings
Emphasis on child safety	- Child safety and online safety groups advocated for reforms to: - Reflect the best interests of the child - Cover all individuals under 18. - These stakeholders highlighted: - Increasing harms impacting young people (e.g. eating disorders, grooming, sextortion) - The need for age-appropriate design and protections.
Scope and definition of harms	- Stakeholders in general called for the legislation to clearly define: - Harms in scope (including illegal, unlawful and harmful to children) - What constitutes 'serious harm' - Systems/features in scope in addition to content-based harms.
Balancing safety, privacy and freedom of expression	- Technology and online safety experts suggested ways to balance DDoC obligations with privacy and freedom of expression including: - Human rights-based framing - Emphasis on systems and processes - Maintaining transparency and accountability safeguards for the regulator.
Risk-based approach to setting obligations	- Industry strongly supports risk-based and proportionate obligations. - There was some concern from industry that small or niche platforms may be overburdened, however it was also acknowledged that size does not equal risk as some smaller services may be higher risk and some larger services may be lower risk.
Regulatory complexity and overlap	- Industry noted the need to prevent overlap of DDoC with existing frameworks (e.g. codes and standards under the Act, privacy laws, National Classification Scheme). - Industry requested: - Alignment with international frameworks (EU, UK)- the UK framework was often preferred as it was said to provide greater regulatory certainty - Recognition of existing compliance efforts - Avoiding cumulative as well as duplicative regulatory burden - Clear guidance on 'reasonable steps' and pre-launch risk assessments to clarify applicable DDoC obligations.
Transparency, accountability and data access	- Technology and online safety experts, advocates for vulnerable communities and online safety advocates strongly support: - Transparency reporting by platforms - Researcher access to platform data – noting Australia lacks a formal scheme. - Industry noted the need to balance transparency with privacy and security risks.
Compliance and enforcement	- Technology and online safety experts, advocates for vulnerable communities and online safety advocates support stronger penalties and fines, potential executive accountability. - Industry supports graduated approach and inclusion of educative/remedial measures in first instance, especially during early implementation.
Ministerial rule making	- Industry expressed concern about being unable to predict the future scope of obligations. - There is broad support for having guardrails on rule-making powers, especially around expanding the scope of harms to be addressed.
Transition arrangements	- Industry expressed a strong preference for: - Gradual or phased transition of the industry codes and standards to the DDoC (rather than abrupt replacement) - Deeming compliance with codes as compliance with DDoC during transition - A transition period of at least 12 months.

Theme	Key Findings
Implementation challenges and capacity needs	• Stakeholders in general acknowledged the complexity in: ○ Designing and enforcing the DDoC ○ Regulating evolving technologies (AI, new platforms). • Stakeholders in general advocated for ongoing consultation and iterative policy design. • Technology and online safety experts noted it would be necessary to continually marshal technical expertise once the DDoC is implemented, to ensure compliance monitoring and enforcement are well informed.