



Summary of key themes - feedback on the Exposure Draft of the Online Safety Amendment (Digital Duty of Care) Bill 2026

September 2026

A total of 225 substantive submissions were received from industry (including major platforms, the broader tech industry and small business groups), civil society (including health and community services and advocacy groups), academics and researchers (including legal and tech policy experts), and government-affiliated organisations, as well as individuals. The department received 5,101 emails during the consultation process, including a high volume of campaign driven emails opposing the Bill. The following is a summary of key themes arising from substantive submissions only.

Objects of the Act

Civil society groups suggested that the promotion and protection of the 'best interests of the child' be incorporated into the Objects of the Act. Others suggested broader references to vulnerable groups in the community in relation to online harms, including women and First Nations people. Some industry and civil society groups suggested broader framing of the Objects around freedoms and rights such as freedom of speech, access to information and privacy.

Construction of the Duty

Safe online environment

Some stakeholders were concerned about the broad construction of the Duty in the Bill, especially the requirement to ensure a safe online environment, and the descriptions of certain listed harms (such as hostile attitudes to women or gender equality) which were considered too broad. Some suggested the combination of broadly defined obligations, regulatory discretion for the eSafety Commissioner and significant penalties may incentivise over removal of lawful speech.

Some stakeholders called for the Duty to focus more explicitly on ‘systems and processes’ instead of the requirement on services to ensure a safe online environment, as defined in the legislation.

Some child safety advocates suggested the obligation under the Duty to provide a safe online environment explicitly include non-resident victims of CSEAM perpetrated, facilitated or shared by Australians, rather than being tied exclusively to persons or children ‘in Australia’.

Reasonably practicable

A number of civil society stakeholders sought clearer recognition of competing rights and interests in determining what measures are ‘reasonably practicable’ under the Duty. Academic, civil society and religious stakeholders variously called for greater consideration of freedom of expression, privacy, freedom of religion and access to lawful information, with some advocating an explicit human rights framework or statutory protections. Some specified that the grossly disproportionate threshold when balancing factors (such as impact on privacy) should be lowered.

Several industry stakeholders, including small website owners and sections of industry associated with infrastructure, asserted that the threshold for ensuring a safe online environment should reflect a provider’s ability to minimise risk to the extent possible.

Rulemaking and delegation to rules

Several industry, academic and civil society stakeholders raised concerns about the breadth of Ministerial and Commissioner rule-making powers, particularly the ability to expand categories of harm, with a significant number considering that certain Ministerial rulemaking powers should be removed or substantially narrowed such that significant policy settings should instead be settled in primary legislation. A smaller group supported delegated instruments and guidance as providing flexibility to respond to technological and regulatory change.

Across these positions, stakeholders commonly sought stronger safeguards around rulemaking, including: legislative requirements for consultation; transparent and evidence-based decision-making; clearer statutory criteria; human rights impact assessments; enhanced parliamentary scrutiny; and sunset and periodic review requirements detailed in the legislation. Different stakeholder groups advocated for specific interests to be recognised or protected in the legislative framework to bind future decision making over subsequent rulemaking powers including the rights of the child, freedom of speech and expression, and access to legitimate public-health and harm-reduction information.

Services captured by the Duty

AI coverage

Several stakeholders, including civil society and academics, sought broader coverage of conversational, companion and generative AI services under the Duty or clarification they were included.

Broad capture

Some academic and civil society stakeholders supported broad, technology-neutral coverage across the technology stack as a means of protecting against emerging risks and future-proofing the framework. Other stakeholders across several sectors emphasised that obligations should reflect the functions and risk profile of different services, and the level of control over content and experience exercised, rather than applying uniformly. Some industry stakeholders were concerned that the broad capture of services could diffuse responsibility and cause confusion.

Exemptions

A substantial body of industry feedback sought exemptions or reduced obligations for services considered to present lower risks or with less ability to directly address online harms. This included infrastructure, equipment and connectivity providers with limited visibility of, or control over, content; closed enterprise and business-to-business services; schools and closed educational platforms; financial services; and community and health advocacy, and other public-interest services.

Stakeholders from academia and industry sought clear statutory criteria for determining exemptions, with some preferring them to be established in primary legislation (rather than rules) and others seeking timely exemption instruments, wanting to avoid unnecessary compliance costs due to a delayed exemption framework. Academic stakeholder suggestions included enabling providers to apply for exemption, and the ability for the Minister to review, apply conditions or revoke exemptions.

Person responsible

Industry stakeholders sought greater certainty about who is the “person responsible” for a service, particularly within complex corporate arrangements. Feedback generally supported responsibility attaching to persons or entities with substantive control or influence over relevant systems and design, rather than employees, volunteers or those performing routine technical administration.

Harms in scope of the Duty

Stakeholders expressed broad support for the existing scope of the Bill, particularly the serious harm categories. There was also broad support from academics and civil society groups for the capture of harms, beyond content harms, relating to online conduct and system design.

Stakeholders expressed differing views on the harm thresholds for adults and children. Some civil society groups suggested protections against ‘material and conduct that is harmful to children’ should be extended to those aged under 25 while others suggested harms such as exposure to eating disorder material should apply equally to children and adults. A broad range of stakeholders advocated including vilification and hate based on protected characteristics including race, religion, sex, gender identity, sexual orientation, sex characteristics or disability, technology-facilitated gender-based violence, image-based abuse and nudification/deepfake content within the definition of seriously harmful material and conduct. Civil society stakeholders also identified technology-facilitated coercive control, harmful body-image and appearance-related content and features, and harmful health misinformation for inclusion in seriously harmful conduct and material.

Industry stakeholders expressed support for clear harm definitions and parameters to support implementation and regulatory certainty. A range of stakeholders suggested safeguarding of access to political and religious speech, public interest journalism, educational material, news content, health information, classified material and accounts of lived experience. There was strong support for excluding health information, particularly information about voluntary assisted dying and harm reduction services.

Regarding the split of harm responses for children and adults, government-affiliated and other stakeholders noted privacy concerns and the risk to anonymous help-seeking from services, and sought privacy-preserving approaches that minimise data collection.

Obligations on services

Risk assessments

There was substantial feedback on the proposed risk-assessment obligations, including general support for risk assessment as a core component of a preventative Duty alongside calls for proportionality in how the requirements would apply. Industry stakeholders sought tiered or simplified approaches for smaller and lower-risk services, while civil society supported greater assurance or scrutiny for higher-risk or high-reach services. Industry stakeholders also raised concerns about recordkeeping requirements and confining re-assessments of risk to substantive service changes.

Civil society stakeholders proposed a range of matters that risk assessments should consider including cumulative exposure and the combined effects of design features, the needs and varying risks to children and vulnerable users and explicit consideration of children's best interests and child-rights impacts.

Academic and civil society stakeholders recommended prescribing minimum mitigations for certain established harms while allowing flexibility for others. Other feedback emphasised the need to assess potential adverse consequences of any mitigations considered, including on privacy, cybersecurity, participation, freedom of expression, access to information and confidential or anonymous help-seeking.

Complaints and dispute resolution

Civil society, academic and consumer sector stakeholders supported accessible, timely and transparent complaint and dispute-resolution processes, with particular emphasis on arrangements appropriate to children and people experiencing or at heightened risk of harm. There was strong support for minimum complaints standards being established in the primary legislation. Some stakeholders also sought clearer appeal and review rights and greater statutory clarity about the services and decisions to which complaint and dispute-resolution requirements apply. Industry feedback, particularly from infrastructure, small business, telecommunications and finance sector stakeholders, emphasised that complaints and dispute resolution requirements should be proportionate and appropriately aligned with existing sectoral complaints frameworks.

Civil society and other stakeholders also supported escalation options beyond a providers' internal complaint processes. In particular, consumer-sector feedback called for a formalised, independent external dispute resolution pathway, with minimum standards around accessibility, transparency and service coverage, and a legislated external dispute resolution or ombuds framework.

Transparency reporting

Academic and civil society stakeholders and government-affiliated stakeholders called for detailed reporting by online services on online harms and outcomes, including disaggregated reporting on harms affecting particular cohorts, as well as greater transparency concerning recommender systems and behavioural targeting, and disclosure obligations on service providers' risk assessments. Some civil society groups called for transparency where content is removed or downranked in order to comply with the Duty.

Industry stakeholders raised concerns about the scope and proportionality of transparency requirements, advocating that they be proportionate, avoid unnecessary or duplicative reporting burdens, and be accompanied by safeguards to protect confidential and sensitive information, including information that could be used by bad faith actors.

Features and user empowerment

There was broad support for measures providing users with greater choice and control over recommender systems and other design features. Academic and civil society stakeholders emphasised that controls should be prominent, accessible, easily understood and persistent across sessions or service updates, without degrading the experience for users. A significant group considered that safer settings, particularly non-personalised feeds, should operate by default (with an opt-in requirement to algorithmic feeds).

Some stakeholders also recommended that the core policy position under the Government's My Feed, My Way initiative – obligating online service providers to offer end-users a substantive choice between personalised and non-personalised social media feeds – be specified in primary legislation instead of rules.

A substantial body of feedback identified recommender systems, algorithmic amplification and engagement-driven design features as contributing to harmful exposure, including to misogynistic and violent or abusive material, eating-disorder and body dysmorphia content, substance-related material and other harmful content. A recurring view was that these risks are not limited to children under 16, with stakeholders variously supporting extension of design-feature protections to all children under 18, young adults under 25, or all users. However, it was also noted that user empowerment over features should supplement, rather than replace, providers' responsibility to address content and conduct harms through the Duty.

Stakeholders also focused on potential negative behavioural impacts associated with design features, including features that may encourage compulsive or prolonged engagement and sought additional related design features to be expressly captured, including endless scroll, autoplay and reward mechanisms.

Industry stakeholders cautioned that regulation should distinguish harmful engagement or amplification practices from user-directed, accessibility, safety enhancing and other legitimate design features, such as recommender systems on streaming services or retail platforms.

Researcher data access and sock puppets

Researcher access

There was substantial support from civil society groups and academics for independent researcher access to platform data. Academic and research stakeholders emphasised that access should be sufficient to enable meaningful, independent and reproducible research into online harms, with some advocating mechanisms such as searchable content libraries and standardised data-access processes.

A recurring concern was that eligibility for approved researcher access is too narrowly confined to Australian university employees, with stakeholders supporting broader eligibility for appropriately qualified researchers and organisations, such as appropriately governed civil society organisations, subject to equivalent safeguards.

Industry feedback commonly focused on safeguards, particularly in relation to privacy, security, proportionality, and data governance. Stakeholders also considered that safeguards, or a subset of key safeguards, should be included in primary legislation rather than left to delegated rules. Some suggested that access obligations should only apply to larger or higher risk services.

Sock puppet accounts for use by eSafety and approved researchers

A wide range of views were put forward on the provisions enabling the use of fictitious identities to investigate and test services. Some stakeholders supported these powers as important for independent testing, while others supported them only with stronger safeguards around their authorisation, scope, oversight and reporting. A smaller group among industry opposed the powers, raising privacy, security and

surveillance concerns. The online dating industry was particularly concerned about the potential for interactions between users and fake accounts.

eSafety investigative powers

Civil society and other stakeholders emphasised the need for the Commissioner to have sufficient powers to investigate potential non-compliance. Some stakeholders also emphasised the importance of ensuring the Commissioner is sufficiently resourced to exercise its powers effectively.

Industry stakeholders sought greater safeguards around the exercise of expanded investigative powers including establishing a reasonable excuse defence for provider compliance with remedial directions issued by the Commissioner, and self-incrimination immunity and mechanisms for review or oversight.

Stakeholders also sought stronger protections for an individual's rights or personal information that could be affected by the exercise of investigative and information-gathering powers. Some stakeholders raised concerns about privacy and freedom of expression safeguards, while media stakeholders sought stronger protections for confidential journalistic sources. Industry stakeholders similarly sought protection for commercially sensitive, legally privileged, private and security-sensitive information obtained or disclosed through the exercise of regulatory powers.

Penalties and enforcement

Graduated and proportionate penalties

Industry stakeholders and tech policy experts sought a graduated approach to enforcement and penalties, to be either prescribed in the legislation or set out in related guidance. They emphasised the importance of allowing minor breaches to be rectified following formal warnings while preserving stronger enforcement responses for repeated or significant first-time non-compliance. Industry stakeholders also emphasised that penalties should be attached to sufficiently clear, settled obligations, noting the Ministerial power to extend elements of the scheme, such as the scope of harms.

There were mixed views on the application of remedial directions for breaches of the Duty, with some industry, civil society and academic stakeholders suggesting there should be limits on this power. Proposals included objective thresholds and review mechanisms for remedial directions, reasonable implementation periods and other procedural controls, including requiring the Commissioner to apply to the Administrative Review Tribunal or Federal Court for binding orders.

Substantive penalties

Civil society and some academic stakeholders supported maximum penalties calculated by reference to a provider's turnover or global revenue, rather than relying solely on fixed amounts, with some concerned that fixed maximum penalties may not provide a sufficient deterrent for larger providers. There were also calls for stronger sanctions for serious, repeated or systemic non-compliance, including service disruption measures.

Private right of action

Some stakeholders including academics, civil society and some government affiliated organisations supported a private right of action or direct pathway for individual redress. Stakeholders considered that this could support executive accountability and provide harmed individuals with a clear and direct pathway to legal redress and compensation. Other stakeholders sought clarification about whether the Bill creates a statutory duty capable of giving rise to private legal action. Some industry feedback specifically opposed a private right of action in relation to the Duty.

Transitional arrangements for the Duty

Industry stakeholders particularly emphasised the need for sufficient time to transition to the new framework, including to implement changes required by the Duty, although views differed on the appropriate implementation period. Suggested periods ranged from 12 months to at least 24 months, with some stakeholders seeking that the transition period commence only once relevant instruments and guidance have been finalised. Stakeholders also sought to avoid regulatory gaps during the transition, including by maintaining existing codes and protections until replacement arrangements are in operation.

Nudify powers and operational amendments to existing schemes

Nudify (fake nude) powers

There was general support for the removal powers to enable eSafety to address the availability of products used primarily to generate fake nude material. However, some industry stakeholders suggested that the legislation should more tightly define the fake nude technologies in scope, including by incorporating a stronger predominant use test to prevent capture of multipurpose AI image generation services. Industry also requested that eSafety be required to notify services, before issuing a removal notice, that a notice clearly identify the product for removal and that services be allowed a longer period to comply.

Civil society stakeholders suggested that eSafety powers be expanded from issuing removal notices for apps and websites hosting fake nude technologies to disruption of hosting and infrastructure providers.

Removal notices under complaint schemes

Civil society stakeholders suggested that the requirement for a child to make a report to an online service before lodging a complaint with eSafety be waived at eSafety's discretion, rather than when there is no internal mechanism associated with the service. Civil society stakeholders also advocated removing the six-month time limit on when reposted material could be removed by eSafety without receiving a new complaint.

eSafety disclosure powers

There was some suggestion from industry that safeguards applying to the use, retention or further sharing of information by Commonwealth entities be clarified in the Explanatory Memorandum, particularly with regard to privilege, confidentiality, security and sensitive technical or commercial information.