



Zen Dodd

POLICY AND PUBLIC SUBMISSIONS

26 OCTOBER 2026

Submission on the Online Safety Amendment (Digital Duty of Care) Bill 2026

Environment and Communications Legislation Committee

steadytao.com/s/d8361f5d

Executive Summary

Bluntly. This Bill should not pass.

The Online Safety Amendment (Digital Duty of Care) Bill 2026 does not create a narrow duty for large social-media companies. It establishes a general obligation to ensure a “safe online environment” across carriage, hosting, search, app distribution, artificial-intelligence generation and even the supply, maintenance and installation of communications equipment. It regulates lawful material and product design, forbids consideration of compliance cost and attaches civil penalties reaching the Government’s advertised A\$109.2 million corporate maximum.^{[1][2]}

The harms used to promote the Bill are real. Child sexual exploitation, grooming, threats, fraud and non-consensual intimate imagery require effective laws and usable remedies. Parents and guardians should remain primarily responsible for the lawful material, services and devices their children use while government addresses conduct that another person cannot reasonably prevent or remedy. Those responsibilities do not justify one statutory architecture through which government, the eSafety Commissioner and risk-averse providers decide which lawful material, communications, features and users are permitted online.

The Bill must be judged as permanent state infrastructure rather than by the present Minister’s intentions. Its categories include material said to encourage hostile attitudes towards women or gender equality and anything else that may cause serious harm to children. It declares broad classes of product feature to have negative behavioural impacts and permits further features to be prescribed. It also authorises false-identity observation and testing. Parliament should ask whether each power remains acceptable when exercised by a future government hostile to a political movement, religion, sexual or gender minority, health service, journalist, researcher or technology.

The Government’s public account does not match the introduced text. Minister Wells has described reasonable steps, regulation of Big Tech, parliamentary control of new harms, no covert surveillance and a low-risk self-assessment pathway. The Bill uses a different compliance standard, reaches much further, retains open-ended categories, permits ministerial expansion and contains no statutory low-risk certification pathway.^{[3][4][1]} The public then received approximately two weeks and a five-page limit to comment on the exposure draft. Material provisions changed before introduction and the published impact analysis does not assess the Bill now before Parliament.^{[5][6][7]}

Australia already has targeted offences, removal powers, industry codes, Commissioner-made standards and a forthcoming Children’s Online Privacy Code. They can be corrected where evidence shows a defect. The new Code already addresses many of the data and design practices used to justify this Bill without requiring every user to be identified or placing lawful online activity under one general safety duty.^[8]

The committee should recommend that the Bill not be passed. Targeted measures in Schedule 1 should be considered separately, Schedule 1 Part 5’s retrospective validation should be removed unless fully justified and the existing codes and standards should remain until Parliament receives a measure-level transition map. Any replacement proposal should follow completion of the Children’s Online Privacy Code, a new impact analysis and a genuine public exposure process. PM&C’s standard timetable assumes four weeks and says consultation should generally not be shorter than one month; a proposal of this breadth warrants longer.^[9]

Contents

1. Position and scope	3
2. Parents, children, providers and the state	3
3. The hostile-government test	4
4. Public claims and the introduced Bill	4
5. Scope, control and compliance	6
6. Lawful content and product design	7
7. Child privacy and age assurance	8
8. Private communications and encryption	9
9. Existing codes and transition	10
10. Enforcement, remedies and research	11
11. Consultation and impact analysis	12
12. Targeted measures	13
13. Questions for the Government	14
14. Recommendations	15
15. Closing	15

1. Position and scope

I make this submission in my personal capacity. The views are my own and should not be attributed to an employer, client, project or other party with which I am associated. I work with software, infrastructure and security evidence. My concern is how this Bill would operate once broad legal concepts become content systems, age checks, account restrictions, risk assessments, regulatory notices, investigations and decisions about who may participate online.

I have inspected the introduced first-reading Bill, its explanatory memorandum, the Minister's second-reading speech, the Parliamentary Library Bills Digest, the September exposure draft, official policy and impact-analysis material, released consultation records and relevant public statements by Minister Wells. The Bill was introduced on 15 October 2026 and remains before the House of Representatives. The committee is due to report on 20 November 2026.^[10]

Online harms are real and current safeguards are imperfect. Child sexual exploitation, grooming, non-consensual intimate imagery, threats, fraud, stalking and serious harassment require effective responses. Recommendation systems, profiling and engagement incentives can also shape what people encounter.

The question is whether this Bill provides a necessary, precise and proportionate response. It does not. It uses serious cases to justify an architecture which reaches lawful speech, private communication, identity, product design, infrastructure and ordinary adult access. It gives substantial powers to future office-holders while leaving essential limits to later instruments, guidance, exemptions and enforcement judgement. Targeted provisions can be considered separately; the general duty should be rejected.

2. Parents, children, providers and the state

Parents and guardians have primary responsibility for deciding which lawful services, material and devices their children may use. That responsibility includes understanding the child, setting boundaries, providing support, responding to problems and adjusting those decisions as the child develops. A Minister, regulator or platform cannot know every child's needs, family circumstances and maturity from a general statutory category.

Parents cannot inspect a proprietary recommendation system, compel a platform to disclose its data practices or repair an inaccessible complaint process. That limitation supports targeted transparency, privacy, consumer-protection, security and user-control obligations. It does not make government the substitute decision-maker for every lawful exposure or give a provider authority to determine which contested ideas another family may encounter.

Parental responsibility is not unlimited. A child has rights and interests of their own. Some children live in unsafe households or need confidential access to health, identity, belief, support and educational information. A parent cannot authorise another person to exploit, groom or threaten a child. A service should not be free to deceive users, misuse their information or create an avoidable danger merely because a parent clicked accept.

Those limits support precise law. They do not support one general duty to produce a safe online environment. Government should define and enforce unlawful conduct, protect personal information, regulate deceptive and unfair commercial practices, preserve remedies and intervene where an identifiable risk cannot reasonably be addressed by the affected person. It should not become the ordinary parent of every child or the supervisor of every adult using a service which a child might also reach.

The same distinction applies to providers. A service provider should be responsible for conduct and design within its control. A platform which deliberately recommends harmful material, exposes a child to unsolicited adult contact or misrepresents a safety control should answer for those choices. An internet carrier transporting encrypted traffic, a hosting provider storing customer data, an independent software author and a technician installing communications equipment do not exercise the same control. Treating them as participants in one undifferentiated safe-environment obligation obscures rather than allocates responsibility.

A workable law identifies the exact duty, the party able to perform it, the evidence by which compliance is judged and the remedy when it fails. The Bill instead begins with the desired condition then distributes responsibility across a vast technical supply chain.

3. The hostile-government test

The Bill is being promoted through examples which invite trust in present intentions. That is the wrong test for permanent statutory power.

Parliament should assume that every power will eventually be available to an office-holder who interprets safety, public interest, hostile attitudes, harmful design and serious distress differently from the current Government. That person may be hostile to a political movement, religious group, union, gender or sexual minority, health service, journalist, whistleblower or security researcher. They may sincerely believe that suppressing the relevant material protects children or social cohesion.

The Bill would leave such an office-holder with:

- a statutory safe-environment objective covering lawful material and conduct
- a child-harm catch-all for anything which may cause serious harm
- a power to prescribe further design features as having negative behavioural impacts
- powers to classify services as social media for the under-16 design rule
- powers to require user empowerment tools
- broad information and examination powers
- power to issue or publish warnings and give remedial directions
- data-access schemes and false-identity testing
- a service environment where private actors face enormous penalties for guessing the regulator's expectations incorrectly

The likely result is not only direct government action. It is anticipatory compliance by providers. When the legal standard is uncertain and the potential penalty is severe, the cheapest defensible response is often to remove material, restrict features, demand identity, exclude users or leave the market. The resulting decisions may never reach a court.

Rights protections must therefore appear in the operative legislation. Ministerial intent, explanatory text and future guidance **cannot** carry that burden. Parliament should not enact a broad system then rely on later office-holders to use it well.

4. Public claims and the introduced Bill

Minister Wells is entitled to advocate for her legislation. Parliament still needs an exact account of the legal mechanism rather than analogies to toys, cars, food, seatbelts and playground equipment.

Those analogies obscure the regulatory problem. A manufacturer controls the construction of a toy or the brakes installed in a car. An online service can control its own design and conduct but it does not originate every communication, know every user's circumstances or exercise the same control at every layer of internet infrastructure. Physical hazards can often be tested against a defined state. The effect of lawful speech, a private conversation or a recommendation depends on content, context, audience and use. Product-safety language does not decide who should control those judgements.

Claim	Introduced Bill	Consequence
The duty concerns Big Tech	Section 25B covers carriage, hosting, search, app distribution, AI generation and people supplying, maintaining or installing communications equipment	Obligations are not confined to large platforms or services exercising editorial control
Providers must take reasonable steps	Section 26 requires appropriate action to ensure a safe environment while section 26A forbids considering cost	The Bill uses a materially different and less settled standard than the Minister's public description
New harms require parliamentary amendment	Section 25E(f) already captures any other material or conduct that may cause serious harm to children while section 25G(2) lets the Minister prescribe additional design features	Removal of the adult-harms power did not make every material expansion depend on another Act
The Bill is not controlling free speech	Sections 25D to 25F require providers to classify lawful material and public interest under threat of a large penalty	Providers will make speech decisions even where government issues no removal notice
The Bill is about what platforms do rather than what people say	Sections 25D and 25E expressly classify material and conduct including lawful expression	A systems-based enforcement model still changes what people can say, receive and access
The Bill is not conducting covert surveillance	Sections 205H to 205K authorise false identities, observation, downloading, selected user engagement, feature testing and Commissioner generation of material whose production may be an offence	The ordinary-language assurance does not describe the investigative conduct authorised by the Bill
Low-risk providers will self-assess and have minimal obligations	Section 25B(3) says only that the Minister may exempt a service or class by legislative instrument	No statutory certification pathway or guaranteed low-risk treatment exists before such an exemption is made
Existing codes and standards lack parliamentary scrutiny	Industry standards under section 145 of the current Act are legislative instruments tabled in Parliament and capable of disallowance	The public description combines industry codes and Commissioner-made standards despite their different legal status

The National Press Club address repeatedly presents critics as the "Yeah... but" brigade and concludes through tragic accounts involving children plus a letter from an eight-year-old. Those experiences deserve serious attention. They do not establish that section 25B's scope, section 26A's cost exclusion, section 25E's lawful-content categories, section 27D's age infrastructure or Schedule 3's repeal are necessary or proportionate.^[3]

An anecdote can establish a possible failure and motivate investigation. It cannot prove which intervention would have prevented the event, whether another law already addresses it, which providers controlled the relevant risk or what collateral effects the proposed power would cause. Parliament should require that causal work rather than treating emotional force as legislative evidence.

The Minister also says the Bill reflects consultation. Some significant changes deserve recognition: the power to prescribe additional adult harms was removed and public-interest exclusions were added. Those changes do not validate the rest of the Bill. Consultation is not established merely because a proposal changed. The public record should show what concerns were considered, which were accepted or rejected and why.

In a 22 October interview Minister Wells was asked whether the same duty-of-care principle should apply to government. She distinguished the ethical position and said she was not considering such a duty as Communications Minister, referring instead to electoral consequences. Private providers would face statutory directions and civil penalties while proposed section 25A exempts State and Territory agencies from Part 2 to the extent they provide or control an online service. That different allocation may have a constitutional or policy explanation. The Government should state it rather than present the principle as one which every institution already accepts.^[3]

5. Scope, control and compliance

Proposed section 25B defines nine classes of online service. It reaches far beyond social media, large platforms and services recommending public content. It includes internet carriage services, relevant electronic services, designated internet services, hosting, search, app distribution, services generating material through artificial intelligence and a service which manufactures, supplies, maintains or installs communications equipment for use in Australia.^[1]

The Bill then identifies the provider and, for most classes, the person exercising the greatest degree of day-to-day control as responsible. It does not say that each duty applies only to the risk that party creates or can materially control.

A carrier cannot generally inspect encrypted traffic without defeating the property users rely upon. A hosting provider may have technical custody without knowing the meaning of customer data. An app store can remove an application without controlling conduct inside every service. A model provider, application developer and person operating an AI feature can be separate. An equipment supplier or installer may have no continuing ability to alter a deployed product. Multiple parties can also each exercise control over different risks.

The Minister may exempt services posing little risk. That does not repair the default. An exemption is discretionary, prospective and dependent on an instrument which does not yet exist. The Bill should not impose broad obligations first then require ordinary low-risk services to wait for government relief.

Proposed section 25A also excludes State and Territory authorities or agencies to the extent they provide or control an online service. The Government should explain why a duty promoted as a basic safety standard for ordinary digital services excludes significant public-sector services by default while capturing small private and non-commercial services unless the Minister acts.

The Minister's second-reading speech describes a self-assessment by which providers can certify that they are low risk, followed by minimal obligations determined by eSafety. No such process appears in the Bill. Parliament should not enact the duty on the assumption that a future exemption, guidance document or administrative practice will create a safeguard omitted from the legislation.^[4]

This mismatch is especially serious for small providers, non-commercial communities, open-source authors and Australian services competing with global firms. A fixed maximum penalty and uncertain duty can be existential for them while remaining a manageable cost for the largest companies. Market exit and compliance concentration would leave Australians with fewer choices and strengthen the same dominant platforms invoked to justify the Bill.

The compliance standard ignores practical limits

The September exposure draft required a safe online environment so far as reasonably practicable. Its reasonable-practicability provision included likelihood, degree of harm, available knowledge, available and suitable controls, implementation cost and expected privacy.^[5]

The introduced Bill replaces that structure. Section 26 requires appropriate action to ensure a safe online environment including effective measures against assessed risks. Section 26A asks how far the measure achieves that environment, how it addresses specified material, its effect on service security and whether it is proportionate to likelihood and degree of harm. Subsection 26A(3) then states that cost must not be taken into account.^[1]

The change is not a clarification. It removes technical feasibility, available knowledge, suitability, privacy and cost from the express test while placing greater weight on the outcome. The explanatory memorandum says occurrence of harm alone does not necessarily breach the duty. That limitation should be in the Act if it is essential to construction.^[11]

Cost is not a sufficient reason to continue a serious avoidable danger. It is still necessary when selecting among controls, deciding whether a measure is technically possible, assessing the effect on service viability and allocating finite resources between risks. Even work health and safety models invoked by the Government use reasonable practicability rather than pretending cost does not exist.

Forbidding consideration of cost can also reduce safety. A provider may spend heavily on a visible moderation control while neglecting account security, incident response, accessibility or another greater risk. It may remove a useful feature or withdraw a service because the law does not permit a balanced selection among measures. An obligation to choose effective and proportionate controls needs the complete system of consequences.

The Bill should not proceed with this standard. If Parliament later considers another duty, reasonable practicability should be restored and should expressly include actual control, technical feasibility, available evidence, privacy, lawful expression, accessibility, service security, effects on beneficial access and cost. Cost should not excuse an avoidable serious risk where withdrawal or another measure is reasonably available.

6. Lawful content and product design

Many categories in proposed section 25D concern conduct already unlawful or closely connected to serious offences. Parliament can regulate child sexual exploitation, grooming, sexual violence, non-consensual intimate imagery, threats, terrorism and encouragement of suicide directly. A specific offence, removal power or provider obligation can identify the prohibited conduct and the relevant intermediary.

Proposed section 25E moves beyond that territory. It declares the following material and conduct harmful to children:

- pornography
- encouragement, promotion or instruction concerning disordered eating
- encouragement or promotion of hostile attitudes towards women or gender equality
- crime glorification, dangerous stunts or seriously harmful practices
- abuse, harassment or bullying
- any other material or conduct or combination of material and conduct that may cause serious harm to children

The Bill does not define encourage, promote, glorify, hostile attitudes, pornography or bullying for this purpose. The final catch-all is not confined to a listed offence, a provider's deliberate act or material reasonably likely to cause harm. It captures anything which may cause serious harm. The Parliamentary Library also identifies the uncertainty of these terms.^[2]

The provision concerning hostile attitudes is especially unsuitable for a statutory content category. Political, religious, historical and legal arguments can contain views another person regards as hostile to women or gender equality. Some such speech may be ignorant or offensive. That does not establish a sufficiently precise basis for government-backed suppression. The law should address threats, targeted harassment, incitement and discriminatory conduct through rules which identify the act and threshold. It should not establish a viewpoint category for material which a provider must interpret under threat of a large penalty.

The child-harm catch-all also qualifies the Government's claim that new harms can be added only by Parliament. The category is already open-ended. Section 25G(2) separately permits the Minister to prescribe additional design features as having negative behavioural impacts. The adult-harm rule-making power was removed; the Bill did not convert the complete scheme into a closed parliamentary inventory.

Section 28B requires the Minister to seek and have regard to the Commissioner's advice before making specified exemption, social-media, design-feature or user-tool instruments. That is a useful procedural requirement. It does not establish the substantive threshold, require publication of the advice or require the Minister to follow it.

Section 25F adds excluded material. Research, public health, harm reduction and public-interest protection are important improvements. The exclusions remain uncertain:

- public interest is not defined and no factors allocate the burden of establishing it
- professional news depends on institutional and editorial criteria which independent reporting might not satisfy
- artistic and educational material must also be not contrary to the public interest
- entertainment protection is tied to specified broadcast, on-demand and classified formats
- user-generated material within a classified computer game is expressly excluded from the entertainment protection
- material connected with a public official's duties is automatically excluded while an independent speaker must satisfy another category
- the section defines excluded material rather than excluded conduct even though sections 25D and 25E regulate both material and conduct

A service provider will make the first decision about these boundaries. The provider receives little benefit from preserving borderline lawful material and substantial exposure from preserving material later found to violate the duty. That asymmetry encourages removal, demotion and access restriction.

The United Kingdom's Online Safety Act requires regulated services to have particular regard to freedom of expression and privacy when deciding and implementing safety measures. The European Union's Digital Services Act prohibits general monitoring obligations for intermediary services and provides more differentiated duties by service type.^[12] Those regimes remain open to criticism. They still demonstrate that rights and technical boundaries can appear in operative law rather than be left to guidance.

If Parliament considers any future measure involving lawful content, it should contain an express duty to protect lawful expression, access to information, privacy, anonymity, pseudonymity and secure communication. It should provide prompt independent review where a safety measure restricts a person or removes public-interest material.

Design categories are not proof of harm

Proposed section 25G declares every recommender feature and every logged-in endless feed, feedback feature or time-limited feature to have negative behavioural impacts. The rule does not ask how the feature operates, what material it handles, whether the user selected it, whether it improves accessibility or whether evidence establishes harm in the relevant service.

A recommender system can amplify harmful material. It can also help a person find emergency information, educational resources, a support community, a small creator or material they deliberately requested. Feedback can create unhealthy comparison or help a creator understand whether public-interest or safety information reached its audience. Time-limited communication can be manipulative or privacy-protective. Endless interfaces can encourage continued use or provide a simple way to navigate a finite personal collection.

The relevant question is not whether a feature belongs to a named category. It is what the implementation does, which incentives shape it, what the user can control and what evidence shows about its effects. Declaring a technology harmful by statutory category replaces that analysis with a label.

The Bill then requires children under sixteen using a social media service to have no access or exposure to those features. That rule sits beside the separate social-media minimum-age framework which prevents under-sixteen account holding on specified age-restricted platforms. The Government should explain the intended population and how the two schemes interact when a child uses a shared device, views public material, evades an age control or accesses a service later designated as social media.

I support a narrow right for an adult user to choose a non-profiled or following-based feed and to have that choice persist. That is an agency measure. It can be enacted and assessed separately. It does not justify a general duty over every service or prove that the Government should define broad feature categories as harmful.

7. Child privacy and age assurance

The Privacy and Other Legislation Amendment Act 2024 already requires the OAIC to develop a Children's Online Privacy Code. The Code is an APP Code under the Privacy Act. It will apply to relevant online services likely to be accessed by children or primarily concerned with children's activities. The final Code must be registered by 10 December 2026.^[13]

The exposure draft already addresses many practices the Government invokes when promoting the Digital Duty of Care:

- collection, use and disclosure should be strictly necessary by default
- collection and later handling must be consistent with the child's best interests
- consent must be voluntary, informed, current, specific and unambiguous
- services must explain actual data handling in age-appropriate terms
- children receive access, correction and destruction rights
- monitoring and geolocation controls require notice
- complaint processes must be child-friendly
- privacy impact assessments and a register are required
- a service can apply the Code to every user instead of identifying each user's age first

The Code does not solve child sexual exploitation, threats, violent conduct or every harmful interaction. Criminal law, targeted Online Safety Act powers and provider controls remain necessary. The Code does directly address profiling, manipulative data use, unsafe defaults, monitoring, retention, AI companions, recommendation profiles and the identity consequences of age assurance.

My submission to the OAIC supported strong privacy-by-default rules while warning against blanket age verification, biometric estimation, government document uploads, persistent age credentials and excessive parental monitoring. It argued that child protection should mean less data, less profiling and safer defaults rather than identity infrastructure around every user.^[14]

The Digital Duty of Care Bill risks undoing that work. A provider facing a safety obligation may collect more identity, age, behavioural and content information to demonstrate compliance. A general reference to safety could become the justification for processing that the Privacy Code is intended to constrain. Section 26A expressly includes service security but does not require consideration of privacy, data minimisation, anonymity or the Code. Section 27D adds a separate age-assurance obligation without an equivalent privacy architecture.

Parliament should not create overlapping schemes before the final Code is registered, its commencement and interaction are known and its impact analysis is complete. At minimum, any later online-safety proposal should include a published crosswalk showing where each Code requirement applies, which regulator owns the boundary and how compliance with one scheme avoids creating a breach or incentive under another.

Section 27D creates identity infrastructure

Section 27D was not in the September exposure draft. It appeared in the introduced Bill after the constrained public consultation.^[2]

The provision applies where there is a reasonably foreseeable risk that a child could access or be exposed through an online service to pornography or material describing or depicting specified fetish practices or fantasies. Every responsible person must, where technically feasible and reasonably practicable, ensure that Australian users receive a choice of at least two appropriate age-assurance measures plus access controls.^[1]

Pornography, specific fetish practices, appropriate age assurance and the required quality of an access control are not defined for this purpose. The obligation is not confined to dedicated adult services. It applies to any online service with the relevant foreseeable risk. The resulting age check concerns Australian users generally because the service must distinguish adults from children before granting access.

Providing two methods does not make either method private, accurate, accessible or safe. Both could depend on identity documents, face analysis, behavioural inference, a small group of vendors or reusable credentials. Both could fail the same person. The provision contains no explicit requirements for data minimisation, local processing, deletion, vendor restrictions, anonymity, fallback, accessibility or correction of a wrong age decision.

Age assurance determines who must prove what, to whom, how often, through which supplier and with what retained evidence. It is identity infrastructure even when the immediate question is age. Once deployed, that infrastructure can expand into unrelated content control, account recovery, advertising, fraud scoring, law enforcement and future regulatory schemes.

The OAIC Code already contains a more privacy-conscious structure. Its section 8 requires reasonable steps to ascertain age before collection but permits the entity to apply the Code to every user instead. It requires prompt destruction of sensitive information collected for age assessment where retention is not otherwise required.^[8] The OAIC process has also included a much longer public consultation and published submissions. The OAIC states that it will undertake a regulatory impact analysis before finalising the Code.^[13]

Section 27D should not proceed. If Parliament later considers a narrow age control for specified adult services, the proposal should begin again with exact content scope, proven necessity, least-intrusive architecture, independent error measurement, fallback access, deletion, no secondary use and express protection for anonymous adult participation.

8. Private communications and encryption

Section 26B says the duty does not require action concerning lawful communication occurring in private solely between consenting adults. This is not a general protection for private communication or encryption.

The exception does not cover communication involving a child, a mixed-age group or a group the Government does not regard as private. The explanatory memorandum says large group chats or servers are not private and identifies child-sexual-abuse detection or video and call disruption as expected mechanisms where serious illegal harm is at risk.^[11]

Targeted action against reported abuse, malicious accounts and identified illegal material can be legitimate. A general duty which makes private communication outside the narrow exception part of a safe-environment obligation creates pressure to inspect content, infer age and weaken confidential communication.

Encryption protects children and adults against criminals, abusive partners, hostile governments, account compromise and mass data collection. It also permits confidential legal, health, journalistic, political and personal communication. The fact that unlawful conduct can occur through encryption does not establish that everybody's communication should become inspectable.

The Bill contains no equivalent to the European prohibition on imposing a general monitoring obligation. It does not state that a provider is not required to weaken end-to-end encryption, build client-side scanning, retain message contents or identify every participant. Those limits should be express before Parliament considers any related measure.

The omission is especially notable because section 235 of the current Online Safety Act already prevents State and Territory laws from making unaware Australian hosting providers or internet service providers liable for particular content and from requiring them to monitor, investigate or retain records about carried or hosted content. The proposed Commonwealth duty includes carriage and hosting services without restating an equivalent federal boundary.^[15]

9. Existing codes and transition

The existing Online Safety Act uses Basic Online Safety Expectations plus industry codes and Commissioner-made standards. This framework is complicated and has generated classification disputes. That establishes a case for precise reform. It does not prove that one broad duty is superior.

In *X Corp v eSafety Commissioner* [2026] FCA 1123, the Federal Court held that X was a social media service and could not also be required to comply with the relevant-electronic-services standard. The Court resolved the matter through service classification and therefore did not determine alternative challenges concerning consultation on the final standard. The judgment exposes a genuine drafting and classification problem. Parliament can correct that problem directly without repealing every code and standard or replacing them with an uncertain general duty.^[16]

The current instruments contain specific, enforceable requirements. eSafety's own guidance states that code and standard requirements are mandatory. Industry standards are legislative instruments tabled in Parliament and capable of disallowance. The Commissioner can reject an inadequate industry code then determine a standard.^[15]

Minister Wells described the seventeen codes and standards as an old-fashioned approach in which industry writes its own rules without parliamentary scrutiny. That statement does not preserve the distinction between a registered industry code and a Commissioner-made standard. It also does not explain why enforceable provisions should disappear before equivalent requirements exist elsewhere.^[3]

Schedule 3 repeals Division 7 of Part 9 after twelve months. The Bill does not carry each current safeguard into the duty. Existing instruments include concrete obligations relating to illegal material, age-restricted material, model testing, differentiated outputs, reporting and age assurance. A risk assessment or future guidance does not automatically reproduce them.^[17]

The explanatory memorandum says current compliance will leave services well placed for the new regime. Being well placed is not legal continuity. A provider can no longer comply with a repealed requirement and a user cannot enforce a policy intention.

Before repeal, Parliament should receive a measure-level transition table identifying:

- every existing obligation
- its current legal basis and affected service class
- the harm or outcome it protects
- whether it will continue, change or end
- the replacement provision and its binding status
- the regulator and remedy

- the commencement sequence
- evidence supporting any deliberate reduction in protection

Schedule 1 Part 5 makes the transition more concerning. It retrospectively protects the validity of registered codes and determined standards where a statutory consultation or waiting period was shorter than required. The explanatory memorandum supplies no substantive reason for those provisions and the Parliamentary Library identifies their apparent retrospective validating effect.^[2]

Parliament should not validate an unidentified procedural defect in unidentified instruments without knowing which periods were deficient, who was affected, whether proceedings or challenges exist and why ordinary correction is unavailable. Part 5 should be removed and considered separately with complete reasons.

10. Enforcement, remedies and research

The Bill increases a range of existing civil penalties from 500 to 6,000 penalty units. Some of those provisions can apply to natural persons as well as corporations. The Parliamentary Library notes that a 6,000-unit maximum for a person can appear disproportionate when the Crimes Act permits a court to impose no more than 2,000 penalty units instead of or in addition to imprisonment for an offence carrying life imprisonment.^[2]

The general duty and several related obligations carry 60,000 penalty units. The Regulatory Powers Act permits a five-times corporate multiplier. A fixed maximum of that scale bears differently on an individual, small service, Australian entrant and multinational platform. It may determine whether one service remains viable while remaining immaterial relative to another provider's global revenue.

Penalties should reflect the seriousness, duration, control, knowledge, concealment, cooperation and repeated nature of a contravention. A deliberate systemic failure by a dominant platform is not equivalent to an inaccurate first risk assessment by a small operator acting openly. Record-keeping defects should not automatically share the same maximum as a decision knowingly exposing people to a serious avoidable danger.

The Bill also changes the Commissioner's function from monitoring compliance to monitoring, investigating and enforcing compliance. Formal warnings may be published. Remedial directions can require specified future action and are expressly not legislative instruments. These powers place substantial practical pressure on providers before a court determines whether the underlying duty was breached.^[1]

At the same time, an affected person receives no general new right to enforce the duty or obtain correction, restoration or compensation. Section 27G permits the Commissioner to prescribe classes of service and complaint-process requirements later. Systemic enforcement and personal remedy are different. A large penalty paid to the Commonwealth does not restore an account, remove an erroneous restriction, compensate a victim or explain why a provider rejected a complaint.

I do not assume that a private cause of action is always the best answer. Litigation can be expensive, slow and inaccessible. Parliament should require a complete remedy map covering provider review, independent dispute resolution, regulatory escalation, urgent interim relief, correction, restoration, compensation and judicial review. Every route should state its scope, evidence access, time limit and available outcome.

Targeted independent redress would protect people more directly than a general duty whose primary enforcement relationship is between the regulator and provider.

Investigative and research powers

Independent research can reveal failures a provider or regulator missed. Access to data and lawful controlled testing can support accountability. The Bill's research provisions still require stronger boundaries.

Approved-researcher eligibility is limited to employees of Australian universities meeting future rules. That excludes independent researchers, civil-society organisations, journalists, qualified practitioners outside universities and international collaborators regardless of capability or public interest. Eligibility should turn on competence, governance, purpose and safeguards rather than one employment category.

The data-access rules may cover decision-making algorithms, moderation, recommendation and circumstances requiring human review. Future rules may address privacy, security, confidentiality, conflicts, request procedures and fees. The Bill places civil penalties, warnings and remedial directions on responsible providers but the Parliamentary Library observes that the equivalent enforcement framework does not appear to apply directly to approved researchers.^[2]

Research access should require data minimisation, secure environments, purpose limitation, deletion, incident response, publication review limited to genuine confidentiality risks and independent reconsideration when a request is refused. It should not hand unrestricted personal data to a person merely because a university employs them.

The false-identity provisions also need correction. Sections 205H to 205K authorise approved researchers and the Commissioner to create accounts under false identities, observe and download material, engage with services, engage with users where necessary to prevent account closure, test features and test service responses. The Commissioner may also test whether a service can generate material whose production, dissemination or possession is an offence.^[1]

Minister Wells says these provisions are not covert surveillance and compares them with mystery shopping. An undisclosed false identity used to observe, record, download and test a service is covert investigation in ordinary language. The activity may be justified in a particular case; changing its label does not supply the safeguards.^[3]

The Bill should specify written authority, purpose, duration, service, permitted interactions, data limits, evidence custody, supervision, no-provocation rules, treatment of children and bystanders, incident response, deletion and independent review. The Commissioner should not generate illegal material unless another law expressly authorises the exact conduct and controls its custody. Researchers need a clear criminal as well as civil liability boundary where authorised work necessarily encounters illegal material.

The explanatory memorandum describes section 205K as a non-exhaustive list even though the introduced provision no longer contains the exposure draft's "without limitation" language. The memorandum should be corrected. An authority to operate under a false identity must not expand through an explanatory mistake.^[2]

11. Consultation and impact analysis

The Department's May to June consultation summary says there was broad support across stakeholders for introducing a duty. The same summary records demands for proportional obligations, rights protection, regulatory certainty, continuity of codes, gradual transition, ongoing consultation and transparent regulator safeguards.^[18]

Support for a preventative concept is not support for the introduced Bill. Participants in May and June could not assess section 26A's cost exclusion, section 27D's age-assurance rule or the final public-interest provisions because those words did not yet exist.

The released FOI record reinforces that distinction. FOI 27-228 includes submissions and briefing material from industry, advocates and experts with conflicting positions. The Department's stakeholder-issues register identifies concerns including carrier exemptions, continuity of existing instruments, scope, safe harbours, audit powers, small-provider support, private rights of action and transition. In the released copy, detailed comments, consideration status and outcome fields are substantially redacted or otherwise unavailable. Meeting-note columns are also withheld under section 47C.^[19]

That release does not establish that the Department ignored submissions. It establishes that the public record does not permit an independent reader to reconstruct how major issues were resolved.

The difference in access is also relevant. MO 27-011 records continuing correspondence and meeting arrangements between Teach Us Consent and the Minister's office from November 2025 into 2026. A private March letter jointly associated with Teach Us Consent, Reset.Tech Australia and Digital Rights Watch sought follower feeds by default through the duty. The Government later announced My Feed, My Way.^[20]

There is nothing inherently improper about meeting advocates or adopting a proposal they support. The record does not prove that the meetings caused the policy. It does show that some advocates had sustained direct access while the later public exposure-draft process offered approximately two weeks, imposed a five-page limit and promised not to publish individual responses.

I wrote to the Department on 12 September asking for at least four weeks, removal or relaxation of the page limit and further explanatory material. The Department replied on 16 September. It acknowledged the short period and said the Government was prioritising introduction before the end of the year. It would endeavour to consider a further draft by 24 September. I replied that a few additional days did not permit responsible analysis and asked who selected the timetable, why it was adequate, whether supplementary material would be accepted and whether the Department would reconsider. The consultation inbox then returned an automatic notice saying feedback was closed. The Office of Impact Analysis advised that the Department was the proper body to answer the process concern. I also called the Department. As at 26 October 2026 it had not substantively answered the outstanding questions.

The preference to introduce a Bill before year-end explains scheduling pressure. It does not establish that the resulting consultation was adequate. PM&C's standard legislative timeframes assume four weeks for exposure-draft consultation and say consultation should generally not be less than one month. They tell departments to consider stakeholder needs and allow additional review time where substantial feedback is expected.^[9]

Minister Wells said during her National Press Club Q&A that the Digital Duty of Care had been worked on for about two years. The proposal was not an unforeseen emergency. A long internal development period makes the two-week public opportunity to inspect the statutory text harder to justify, not easier.^[3]

On the morning of introduction the Minister also said the Government had anticipated a Senate inquiry and still expected passage before Christmas. Welcoming scrutiny does not answer whether the timetable gives the committee and public enough time to perform it.^[3]

The Government then changed material provisions before introduction. The parliamentary inquiry opened on 15 October, submissions close on 30 October and the committee reports on 20 November. The public has therefore again received little time to examine a 90-page Bill, a 105-page memorandum, the September comparison, existing instruments and overlapping privacy reforms.

FOI 27-274 seeks the records supporting the consultation window, five-page limit and refusal of extensions. FOI 27-275 seeks the latest stakeholder-issues register or its successor including each issue's consideration, outcome and reasons. The Department acknowledged both requests on 13 October 2026 and stated a decision date of 9 November 2026 subject to lawful extension. That date falls after the committee's submission deadline. The absence of those records by 30 October is not evidence of unlawful delay. It is a reason for the committee to obtain the same material directly and permit supplementary evidence after release.

The published impact analysis does not assess the Bill

The Office of Impact Analysis published an Impact Analysis Equivalent on 9 September. It relied on the earlier statutory review. OIA expressly says it does not assess the quality of reviews used as equivalents; it assessed relevance and coverage of the impact-analysis questions.^[7]

The analysed proposal differs materially from the introduced Bill. The OIA record describes:

- proportionate obligations calibrated to service reach and risk
- code-making powers supporting compliance
- possible later concessions or exemptions for very low-risk services
- clear guidance as the intended control against excessive moderation
- an intention to transition away from codes while minimising compliance burdens

The introduced Bill:

- changes reasonably practicable to appropriate action and effective measures
- forbids considering cost
- leaves low-risk relief to a future discretionary ministerial instrument
- introduces age assurance and access controls not contained in the exposure draft
- reaches broadly across service and equipment classes
- relies on providers to interpret lawful child-harm categories
- repeals the code-making framework the analysed model contemplated using

The Department estimates an average annual increase of A\$1.408 million in regulatory costs across Australian businesses over ten years. The public record does not explain the population, distribution, engineering assumptions or sensitivity behind that average. An average can conceal a negligible burden on one group, an existential burden on another and large foreign costs outside the estimate.

The memorandum says the Bill will have only a minor effect on Commonwealth expenditure. That means much of the assessment, moderation, identity, engineering, complaint and evidence cost is expected to sit with providers and users. Section 26A then says those costs cannot be considered when judging compliance.

Parliament should require a new impact analysis of the actual Bill. It should model affected service classes, small and non-commercial providers, service exit, market concentration, privacy, age-assurance errors, lawful-content restriction, complaints, regulator resources, code transition and interactions with the OAIC Code. It should compare targeted alternatives rather than only a broad duty against the status quo.

12. Targeted measures

Rejecting this Bill does not require rejecting every measure contained within it.

Schedule 1 includes proposals which address specific problems:

- removal notices directed to app distributors and search engines for services predominantly designed or used to generate fake nude material
- complaint waivers where a provider lacks an accessible process or another complaint creates a foreseeable risk
- treatment of reposted material previously subject to a notice
- link-deletion notices tied to an underlying removal notice
- shorter 24-hour periods in specified complaint and removal-notice pathways

Each requires scrutiny. Fake nude material should be defined. Notices need accurate targeting, reasons, review, revocation and preservation of evidence. Repost rules should distinguish the same material from a materially different lawful use. Time limits should allow urgent action without making accurate review impossible. Penalties should be proportionate to the actor and failure.

Those questions can be answered in a separate Bill. Combining targeted victim remedies with a general duty creates a false choice: accept the complete architecture or appear to oppose protection from abuse. Parliament should refuse that framing.

Other narrower work is already available:

- enforce criminal law and targeted removal powers against defined unlawful conduct
- complete and enforce the Children's Online Privacy Code
- retain and improve current online-safety codes and standards
- regulate deceptive and unfair design through consumer and privacy law
- provide usable parental and device-level controls without forcing identity on every user
- establish independent complaint and correction routes
- preserve encryption while supporting user-controlled reporting, blocking and account security
- improve digital literacy and support for parents, children and schools
- enact a separate user right to a persistent non-profiled or following-based feed if the evidence supports it

These mechanisms allocate responsibility to an identified risk. They are easier to test, amend and repeal when they fail. They do not require Parliament to declare the complete internet a regulated safe environment.

13. Questions for the Government

The committee should require direct answers to the following questions.

1. Why does Minister Wells repeatedly describe reasonable steps when section 26 uses appropriate action to ensure an outcome and section 26A excludes cost?
2. Where is the low-risk self-assessment and minimal-obligation pathway described in the second-reading speech and which services will be exempt at commencement?
3. Why does section 25B impose one duty across carriage, hosting, AI generation and equipment supply, maintenance and installation instead of allocating responsibility by actual control? Why are State and Territory agencies excluded while low-risk private services require a future exemption?
4. How will providers apply the open-ended child-harm category and terms such as hostile attitudes and bullying without suppressing lawful political, religious, health, artistic and educational material? How does that category support the claim that Parliament must approve every new harm?
5. Why does the Bill contain no general protection for lawful expression, privacy, anonymity, accessibility, end-to-end encryption or freedom from general monitoring?
6. Why was section 27D added after exposure-draft consultation, what evidence supports it and how will it interact with the Children's Online Privacy Code's less intrusive all-users pathway?

7. Why did the Minister deny covert surveillance when sections 205H to 205K authorise undisclosed false-identity observation and testing? Which laws authorise generation, possession or downloading of illegal material and why are qualified researchers outside Australian universities excluded?
8. Which obligations in the current codes and standards will continue after Schedule 3 takes effect? Which instruments require retrospective validation under Schedule 1 Part 5 and what defects are being validated?
9. What evidence establishes that this general duty would protect people more effectively than targeted amendment of existing offences, remedies, codes, standards, privacy law and consumer law?
10. What evidence supports the claim of overwhelming public support? Who selected the two-week and five-page consultation, how were stakeholder issues resolved and why have the Department's consultation-process questions and relevant FOI records remained outstanding?
11. What impact analysis covers the introduced standard, cost exclusion, age assurance, broad service scope, lawful-content categories and repeal architecture?
12. What remedy will let an affected person obtain urgent review, correction, restoration or compensation when a provider or regulator applies the scheme wrongly?

14. Recommendations

I recommend that the committee:

1. Recommend that the Bill not be passed.
2. Recommend that Schedules 2 and 3 be withdrawn. Targeted measures in Schedule 1 should be separated and assessed on their own merits.
3. Remove Schedule 1 Part 5 unless the Government identifies each affected instrument and procedural defect then establishes why retrospective validation is necessary.
4. Require any future duty to follow actual control over a defined risk and use a complete proportionality test including technical feasibility, evidence, privacy, accessibility, service security, beneficial access and cost.
5. Reject open-ended lawful-content and viewpoint duties. Preserve lawful expression, anonymous and pseudonymous access, end-to-end encryption and freedom from general monitoring.
6. Reject section 27D. Complete and evaluate the Children's Online Privacy Code before proposing another age or child-data obligation.
7. Preserve the current codes and standards until Parliament receives a measure-level map showing an enforceable replacement for every protection which should continue.
8. Require independent redress for affected people and narrow, authorised and independently supervised research, data-access and false-identity powers.
9. Require a new impact analysis of the actual proposal and realistic targeted alternatives.
10. Obtain the records sought in FOI 27-274 and FOI 27-275, permit supplementary submissions after their release and require at least three months of public exposure-draft consultation for any replacement general duty.

15. Closing

The Government has attempted to frame this Bill as a choice between protecting children and permitting technology companies to cause harm without responsibility. That is a false and deeply objectionable choice. Real suffering does not establish that every proposed power is necessary and it should not shield this legislation from scrutiny.

Australia can prosecute exploitation, remove illegal material, protect personal information, regulate deceptive conduct, improve complaint systems, preserve targeted standards and give users greater control without creating a general government-supervised duty over lawful content, identity, private communication, product features and infrastructure.

Children need protection from crime, exploitation and predatory commercial practices. They also need privacy, access to information, secure communication and adults willing to exercise responsibility rather than transferring every difficult judge-

ment to a platform or regulator. Adults should not have to identify themselves or accept government-defined content controls merely because a service can also be reached by a child.

The Bill's most consequential powers will not remain confined to the examples used to sell them; future Ministers, regulators and providers will inherit the words Parliament enacts. Those words are too broad, too uncertain and too dependent on later discretion.

Bluntly. This Bill should not pass.

References

- [1] Parliament of Australia, *Online Safety Amendment (Digital Duty of Care) Bill 2026: first-reading text*, introduced 15 October 2026, especially Schedule 2, proposed ss 25B to 28C and 192A to 205L plus Schedule 3.
- [2] Parliamentary Library, *Online Safety Amendment (Digital Duty of Care) Bill 2026*, Bills Digest No. 26, 2026-27, 23 October 2026.
- [3] Anika Wells MP, "The Today Show with Sylvia Jeffreys", 7 September 2026; "Address to the National Press Club", Q&A, interview on the introduced Bill and "Digital Duty of Care next step in Australia's world-leading reforms", 15 October 2026; "Podcast interview, The Daily Aus", 22 October 2026.
- [4] Anika Wells MP, *Second Reading Speech: Online Safety Amendment (Digital Duty of Care) Bill 2026*, House of Representatives, 15 October 2026.
- [5] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *Exposure Draft: Online Safety Amendment (Digital Duty of Care) Bill 2026*, 8 September 2026, proposed ss 25H and 26.
- [6] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *exposure-draft consultation page*, 8 September 2026.
- [7] Office of Impact Analysis, *Digital Duty of Care Model for Online Safety*, 9 September 2026.
- [8] Office of the Australian Information Commissioner, *Privacy (Children's Online Privacy) Code 2026: Exposure Draft*, proposed ss 8 to 11 and 30 to 40.
- [9] Department of the Prime Minister and Cabinet, *Standard timeframes for Legislative Projects*, December 2025, p. 2.
- [10] Parliament of Australia, *Online Safety Amendment (Digital Duty of Care) Bill 2026*, progress and committee-referral record.
- [11] Parliament of Australia, *Explanatory Memorandum: Online Safety Amendment (Digital Duty of Care) Bill 2026*, especially pp. 51 to 79 and 87 to 101.
- [12] United Kingdom, *Online Safety Act 2023*, s 22; European Parliament and Council, *Regulation (EU) 2022/2065*, especially arts 8, 20, 34, 35, 38 and 40.
- [13] Office of the Australian Information Commissioner, *Draft Children's Online Privacy Code consultation*, updated 20 August 2026.
- [14] Zen Dodd, *Submission on the Privacy (Children's Online Privacy) Code 2026*, 4 May 2026, especially sections 4 to 7 and 29 to 34.
- [15] Commonwealth of Australia, *Online Safety Act 2021*, s 235 and Part 9, Division 7, especially ss 140 to 150; eSafety Commissioner, *Online Safety Codes and Standards Regulatory Guidance*, September 2026.
- [16] Federal Court of Australia, *X Corp v eSafety Commissioner*, [2026] FCA 1123, 12 August 2026, especially the catchwords and paragraphs 1 to 5.
- [17] eSafety Commissioner, *Register of Online Safety Codes and Standards*; Commonwealth of Australia, *Online Safety (Designated Internet Services-Class 1A and Class 1B Material) Industry Standard 2024*, especially s 22 concerning testing, mitigation and differentiation of generative-AI outputs.
- [18] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *Digital Duty of Care stakeholder consultation May-June 2026: Key Outcomes*, 2026.
- [19] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *FOI 27-228 Documents released*, 9 October 2026: request, decision and released documents. The release substantially overlaps the Department's FOI 27-006 disclosure and contains the stakeholder-issues register as Document 17.
- [20] Minister for Communications, *MO 27-011*, released 24 September 2026: Departmental disclosure-log entry and FOI Monitor record.