BCA
Business Council of Australia

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

30 October 2026

Introduction

The Business Council of Australia (BCA) supports a clearly defined digital duty of care focussed on preventing and mitigating illegal activity and harm to children, while protecting privacy and lawful expression. This submission builds on BCA's submission of 22 September 2026 that responded to the exposure draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026*.

We welcome specific improvements made in the revised Bill introduced to Parliament on 15 October 2026, including a narrower definition of responsibility, a more targeted risk-assessment framework, excluded material protections from legitimate content, retention of the low-risk-assessment framework, removal of proposed ministerial powers to add harm categories by legislative instrument, simpler point-of-contact arrangements, and a reasonableness test in the research-access scheme.

The duty has whole-of-economy reach across a broad range of online services, not only social media, spanning higher-risk interactive services and low-risk online retail, transactional and enterprise-facing services. The BCA's central concern remains, that settings designed for the highest-risk platforms would apply to all of these services. Our position is that obligations must match the actual risk a service presents. Otherwise government is imposing significant red tape on businesses which will negatively impact productivity and wider consumer benefits, whilst detracting from the core objectives of this Bill.

Clear, risk-based obligations would allow providers and the eSafety Commissioner to focus effort on the most serious risks, while protecting privacy and lawful expression.

The BCA is also concerned that the revised Bill removes several safeguards contained in the exposure draft, including the 'so far as is reasonably practicable' qualifier on the duty, privacy as a relevant factor, and confidentiality protections for transparency information. We consider these changes a step backwards: they reduce certainty about what compliance requires and weaken protections for privacy and sensitive information.

Further unresolved issues which are outlined in this submission relate to:

- international alignment and the scope of the duty
- clarity and proportionality in compliance and enforcement
- design and age-assurance requirements
- protection of sensitive information and service security
- coverage of low-risk services
- implementation time.

Key recommendations

- Australia's digital duty of care framework should align more closely with established international models, particularly the United Kingdom's *Online Safety Act 2023*.
- Ministerial and regulatory discretion that can materially affect compliance should be bounded by objective criteria, transparent processes, appropriate consultation and mechanisms for accountability.
- The compliance test must expressly account for lawful expression, access to information and accessibility.
- Privacy should be reinstated as an express factor in section 26A(1), alongside security, so that privacy and end-to-end encryption are expressly considered.
- Penalties must distinguish substantive safety failures from minor administrative errors.
- Illegal content and activity should be addressed for all users, while additional protections against lawful but harmful content should focus on children.
- Safety requirements must address demonstrated risks without presuming that certain features are inherently harmful.
- Compliance should not require general monitoring of private communications or weakening encryption.
- Publication protections for transparency information should be restored and extended, with public summaries as the default, detailed assessments provided confidentially subject to privilege, and disputes resolved before publication.
- Technical access powers should be necessary and proportionate, confined to a defined regulatory purpose, and subject to strong protections for proprietary and security-sensitive information.
- Exclusions should reflect the material risk presented by a service, rather than the size of the business providing it.
- Section 25B should expressly exclude services supplied under contract to organisations for internal use where the customer administers the service and its users, reflecting their different risk profile.
- Regulated financial services should be excluded from the duty and related obligations.
- Any exclusion for regulated financial services should apply across the duty (section 25A) and the related transparency-reporting (Part 12A), research-access and data-access obligations (Part 14).
- The implementation period should increase from 12 to 24 months after Royal Assent.
- Rules, exemptions and essential guidance need to be available at least 12 months before obligations commence, with deferral where necessary.
- The higher penalties for existing codes and standards should commence with the duty, without delaying compliance with existing obligations or urgent action against harmful material.

Align with international models and define the duty clearly

Australia's digital duty of care framework should align more closely with established international models, particularly the United Kingdom's *Online Safety Act 2023*.

Like the UK model, the Australian framework should distinguish between duties addressing illegal content and activity, which apply to all users, and clearly defined, enhanced protections for children from harmful content. This approach would support freedom of expression by avoiding an open-ended duty that could restrict lawful content accessed by adults.

The UK Act is also more targeted, applying mainly to user-to-user and search services, with separate provisions for pornography published by service providers. The residual category in paragraph 25E(1)(f), covering any other material or conduct that may cause serious harm to children, must be tightly bounded by objective criteria consistent with the serious-harm threshold, so the scope of the duty, including for users aged 16 and 17, is not left to open-ended interpretation by providers or the regulator. Alignment with the UK does not require wholesale adoption of its complex service-categorisation system or extensive regulatory guidance. Australia should retain a simpler, risk-based framework.

Importantly for businesses seeking to comply, aligning the scope and key concepts of the duty with comparable international frameworks would provide greater regulatory certainty and reduce the cost and complexity of complying with materially different regimes across jurisdictions. Any departure from established international approaches should respond to clearly identified risks that are not adequately addressed by existing frameworks and be no broader than necessary.

Keep compliance and enforcement clear and proportionate

Businesses need clear thresholds, responsibilities and ways to demonstrate compliance, while retaining flexibility over technical solutions. Consistent with the explanatory memorandum's recognition that different services need different safeguards, obligations – including assessments and reporting – need to expressly reflect service functions, Australian reach, risk and the provider's capacity to address it. Material elements that determine the scope and core obligations of the duty belong in primary legislation wherever practicable.

We are particularly concerned about ministerial discretion.

Ministerial and regulatory discretion that can materially affect compliance should be bounded by objective criteria, transparent processes, appropriate consultation and mechanisms for accountability.

This must apply to the Minister's powers to declare further design features as having negative behavioural impacts (subsection 25G(2)) and to require user empowerment tools (section 27A). It must also apply to the eSafety Commissioner's powers to give remedial directions where it reasonably believes a provider has failed or is failing to comply with the duty (section 26E), to set additional risk-assessment requirements (paragraph 27(2)(f)) and to impose publication obligations on classes of services (section 192L). Greater certainty would help businesses spend their efforts reducing risk, not defending against enforcement. It would also support consistent expectations across online services, making workable industry standards easier to develop.

Compliance is best assessed against reasonably foreseeable risks relevant to the duty, the safeguards implemented and information reasonably available at the time. The revised test retains proportionality to risk but expressly excludes consideration of the cost of implementing safety measures (subsection 26A(3)). Excluding cost altogether departs from established Australian safety law. Under the model work health and safety laws,

cost is considered once the risk and the available controls have been assessed, including whether the cost is grossly disproportionate to the risk. The duty needs to treat cost on the same basis.

> The compliance test must expressly account for lawful expression, access to information and accessibility.

The duty in section 26 should be qualified by 'so far as is reasonably practicable', as in the exposure draft, or reasonable practicability made the measure of 'appropriate' action under section 26A. This would preserve a systems-and-processes focus and provide a clearer compliance standard.

Reasonable practicability is a well-understood standard in Australian safety law, including work health and safety law. A maximum civil penalty of 60,000 penalty units demands clear requirements. Improving clarity would give providers greater certainty about what the duty requires.

> Privacy should be reinstated as an express factor in section 26A(1), alongside security, so that privacy and end-to-end encryption are expressly considered.

The express exclusion of financial and operational costs in section 26A(3) is inconsistent with proportionality and may create prohibitive barriers for smaller businesses or deter beneficial product development.

> Penalties must distinguish substantive safety failures from minor administrative errors.

The Bill retains the same stated maximum penalty for duty breaches and minor breaches in documentation, such as risk assessments. Our view is that minor documentation breaches warrant lower maximum penalties.

Relevant guidance, testing and remediation must inform compliance decisions, and the presence of individual items of harmful content alone is not enough to establish a breach. Section 26A should also recognise diligent, good-faith risk management, so enforcement distinguishes systemic disregard from transparent efforts to identify and fix problems. Except where urgent action warrants otherwise, providers require notice of an alleged contravention and an opportunity to respond or remedy deficiencies before civil penalty proceedings commence.

Align service design and age assurance with demonstrated risk

> Illegal content and activity should be addressed for all users, while additional protections against lawful but harmful content should focus on children.

The duty must not create an open-ended obligation to prevent lawful content that may harm adults. Putting aside arguments with regard to freedom of expression, such an approach would be inherently uncertain and render compliance by businesses exceedingly challenging. Measures affecting adults need to preserve access to lawful content and individual choice, and any restrictions should be clearly defined and supported by evidence. Broad or uncertain thresholds can also create incentives to restrict lawful content, such as news, health information or public debate, simply to manage regulatory risk. Clear limits are therefore important to both lawful expression and effective, predictable compliance. The duty should focus on service-level risks and controls rather than requiring providers to assess or profile individual customers.

Safety requirements must address demonstrated risks without presuming that certain features are inherently harmful.

That presumption can unnecessarily restrict legitimate content and useful service and safety functions, and overlooks the purposes these features serve, including delivering age-appropriate content. Any potential harm from a feature should be established through the service-specific risk assessment, rather than presumed by default.

For example, the definition of a 'safe online environment' in paragraph 25C(1)(c) applies the relevant restriction specifically to social media for children under 16, but section 25G defines recommender and logged-in features as having negative behavioural impacts across online services, potentially capturing ordinary recommender systems used in online retail and other low-risk services.

Requirements need to distinguish harmful features from transactional, security, accessibility and user-requested personalisation functions that help Australians and deliver them the quality of service they expect. Requirements should also allow equally effective technical approaches.

Recommender and ranking systems can also support access to timely public interest information, including emergency and current affairs information. The draft user-empowerment rule should apply reasonable steps standards, define 'similar experience' by reference to core features, accommodate mixed-feed designs and equivalent overseas approaches, and allow phased implementation for engineering-intensive prompts. Rule-making powers for service design need to be outcomes-based and risk-proportionate, accommodate different service architectures, and avoid one-size-fits-all requirements across services.

Age assurance should protect children while minimising personal data collection and preserving access to essential services. Because section 27D requires services within scope to offer a choice of at least two appropriate age-assurance measures, the triggers need to be clear: 'pornography' and material depicting 'specific fetish practices or fantasies' are best defined by reference to established classification arrangements and existing online safety codes and standards where appropriate. The added requirements for specified sexual material must operate consistently with the exclusions for legitimate health, education and other public-interest content. The excluded-material provisions are a useful safeguard, including for classified films and games, but must also avoid unintended capture of lawful commercial content and services not directed to children where they present little or no relevant risk.

Compliance should not require general monitoring of private communications or weakening encryption.

The Bill needs to state this expressly. Providers should not be required to repurpose personal information collected for unrelated purposes, unnecessarily profile users, or infer sensitive or vulnerability-related characteristics where less privacy-intrusive measures can adequately address the risk. This includes any requirement to decrypt private communications or weaken other security controls. Where automated tools are used to identify vulnerable users or harmful behaviour, safeguards are needed to reduce the risk of customers being wrongly classified or unnecessarily restricted.

Protect sensitive information and service security

Transparency should support accountability without exposing personal information, confidential business material or vulnerabilities that could help bad actors circumvent safeguards and undermine the safety, security and integrity of systems.

Publication protections for transparency information should be restored and extended, with public summaries as the default, detailed assessments provided confidentially subject to privilege, and disputes resolved before publication.

The introduced Bill removes these protections that our earlier submission sought to strengthen.

Transparency reporting also needs to be confined in primary legislation to services presenting material online-safety risk, rather than leaving the scope solely to regulatory discretion. In particular, the protections formerly in exposure draft subsections 192G(2) and 192M(6) should be restored, and security-sensitive and commercially confidential parts of risk assessments excluded from publication under section 192L. Protecting this information also encourages candid risk assessments.

The eSafety Commissioner must also account for information already supplied or published across the transparency, publication and researcher-access regimes to avoid duplication. Published material must not identify individuals or incidents, expose customer vulnerabilities, or disclose fraud and cybersecurity controls in a way that could enable circumvention. These safeguards would protect Australians from potential harms caused by disclosure.

Technical access powers should be necessary and proportionate, confined to a defined regulatory purpose, and subject to strong protections for proprietary and security-sensitive information.

Research-access arrangements need to include explicit protections for algorithms and other proprietary or commercial-in-confidence information. The new technical-access power reinforces the need for these safeguards. This is particularly important where access could expose trade secrets, intellectual property or security vulnerabilities, including vulnerabilities that could be exploited in ways that affect user safety.

Businesses also need reasonable response periods and a process to raise privilege or conflicting obligations. Testing of authorised fictitious accounts must preserve legitimate fraud prevention, customer identification and cybersecurity controls. Any authorised use of fictitious accounts should be confined to clearly defined statutory purposes, subject to necessity and proportionality, and not override legitimate fraud, security or platform integrity controls beyond what is necessary for that authorised activity. A provider acting in good faith under ordinary account integrity controls, without knowledge that an account is being used under sections 205H or 205J, should not contravene the Act or data access rules, and the eSafety Commissioner's policies under subsection 205K(3) need to be developed with industry.

Guidance must set out the minimum evidence required to demonstrate that risks were assessed and controls were effective, so providers need not retain personal information beyond what is necessary. Any exercise of the algorithm disclosure power in section 28A must be necessary and proportionate, protect source code and other proprietary technical information, and be confined to information needed for a defined regulatory purpose. The power should only be exercised where a service is, or may be, in breach of the duty and should be subject to appropriate confidentiality protections, including a right for the provider to object to an appointed nominee on reasonable grounds, such as a conflict of interest. The access power in paragraph 28A(1)(b) must also account for confidentiality, legal privilege, privacy and data-protection obligations, and conflicting legal obligations in other jurisdictions.

Apply risk-based exclusions and avoid duplication

The BCA supports the exemption power for services that pose little risk and the Government's stated intention that providers of low-risk services, including websites and applications operated by small businesses, face proportionate obligations. The removal of the exposure draft's additional 'used minimally' ground makes it more important that clear class exclusions for low-risk services are settled before commencement rather than left solely to guidance.

> Exclusions should reflect the material risk presented by a service, rather than the size of the business providing it.

Any residual exemption power under subsection 25B(3) needs to be guided by statutory criteria. For services presenting little or no material risk, proportionate obligations should be invoked when the service or its risk profile materially changes, rather than mandatory annual reporting, and information-gathering requirements calibrated to the service's risk.

Across sectors, clear statutory boundaries and reliable exclusions are needed for low-risk informational and transactional websites, enterprise, business-to-business and infrastructure services. Revised AI coverage (paragraph 25B(1)(h)) needs clarification for routine workplace and customer-service tools, with responsibility reflecting each business's control or material influence (subsection 25B(2)).

Equivalent sector complaints processes and internal or comparable overseas risk assessments need to be recognised where they meet Australian requirements. Clear statutory boundaries would also make the regime more administrable for the eSafety Commissioner by focusing regulatory attention on services that present material risk. These boundaries also support the effectiveness of the regime: bringing low-risk services into the same compliance architecture can diffuse regulatory attention and resources away from higher-risk services.

> Section 25B should expressly exclude services supplied under contract to organisations for internal use where the customer administers the service and its users, reflecting their different risk profile.

Recognition of internal or comparable overseas risk assessments should turn on substantive coverage of the matters in subsection 27(2), with supplementation for Australian users, rather than requiring reformatting. The eSafety Commissioner could also be given the power to prescribe streamlined assessments for low-risk services. Guidance must also identify the evidence needed to show that an existing internal or sector-specific assessment satisfies the duty.

> Regulated financial services should be excluded from the duty and related obligations.

Digital banking services primarily provide information, account access and transactions, rather than interaction between users or amplification of user content. Financial service providers already face extensive prudential, conduct, complaints-handling, scams, anti-money laundering and fraud requirements. The exclusion sought in our earlier submission remains absent, creating a risk of duplicated regulation without a commensurate safety benefit. At a minimum, an exemption must be settled before commencement, with separate reporting, access and contact obligations also addressed.

The exclusion would apply to online services provided by or on behalf of a regulated financial entity when supplied in the course of regulated financial activities. Online functionality supplied outside those activities would remain subject to the ordinary risk-based framework. This entity-and-activity boundary could be framed by

reference to established concepts in the Banking Act 1959, Australian Securities and Investments Commission Act 2001, Corporations Act 2001 and National Consumer Credit Protection Act 2009, which would limit interpretive uncertainty.

Any exclusion for regulated financial services should apply across the duty (section 25A) and the related transparency-reporting (Part 12A), research-access and data-access obligations (Part 14).

If Parliament does not adopt a statutory exclusion, regulated financial services should be prescribed as exempt under subsection 25B(3), with the exemption extending across the regime and settled before commencement so businesses do not incur unnecessary implementation costs for services ultimately found to be exempt.

Provide sufficient time for implementation

The implementation period should increase from 12 to 24 months after Royal Assent.

This timetable must also account for overlapping implementation programs across Privacy Tranche 2, standards around AI and data centres, the Children's Online Privacy Code and critical infrastructure reforms, which may require changes to the same governance, data and technology systems.

Businesses need time to determine coverage, agree supplier responsibilities, change systems and test safeguards against settled requirements.

Rules, exemptions and essential guidance need to be available at least 12 months before obligations commence, with deferral where necessary.

Existing protections should remain until replacement provisions take effect.

As an alternative, obligations could commence 12 months after the later of Royal Assent and publication of the eSafety Commissioner's core risk-assessment requirements and guidance, with engineering-intensive obligations phased in. Later delegated instruments that introduce new obligations should be subject to a minimum 30 days of public consultation consistent with government best-practice, an appropriate regulatory impact assessment and a minimum six-month transition period.

The higher penalties for existing codes and standards should commence with the duty, without delaying compliance with existing obligations or urgent action against harmful material.

Currently, the Bill would have some higher penalties apply from the day after Royal Assent, before the core digital duty of care provisions commence 12 months later.

Conclusion

The BCA supports a digital duty of care that improves online safety, especially for children. The revised Bill makes useful improvements. However, the duty applies across the economy and many of its settings are designed for high-risk platforms. That mismatch creates risks the Bill does not intend:

- Businesses would face compliance uncertainty and compliance costs for low-risk services.

- Consumers would lose access to lawful content and useful services, and have more of their personal information collected.
- The eSafety Commissioner would be spread across a far larger range of services, diverting attention from where the risk of harm is greatest.

Getting these settings right would strengthen online safety by focusing obligations and regulatory effort on the services and risks that matter most. It would also give businesses greater certainty, support better service design, and protect privacy, lawful expression and access to legitimate services.

BUSINESS COUNCIL OF AUSTRALIA
GPO Box 1472,
Melbourne 3001
T 03 8664 2664
bca.com.au

© Copyright 30 October 2026 Business Council of Australia, ABN 75 008 483 216.

All rights reserved. No part of this publication may be reproduced or used in any way without acknowledgement to the Business Council of Australia.

The Business Council of Australia has taken reasonable care in publishing the information contained in this publication but does not guarantee that the information is complete, accurate or current. In particular, the BCA is not responsible for the accuracy of information that has been provided by other parties. The information in this publication is not intended to be used as the basis for making any investment decision and must not be relied upon as investment advice. To the maximum extent permitted by law, the BCA disclaims all liability (including liability in negligence) to any person arising out of use or reliance on the information contained in this publication including for loss or damage which you or anyone else might suffer as a result of that use or reliance.