To: OSA Reform Team
By email: digitaldutyofcare@communications.gov.au

18 September 2026

Dear OSA reform team,

The Digital Industry Group Inc. (DIGI) welcomes the opportunity to comment on the exposure draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (the Bill), released by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the Department) on 7 September 2026.[1] DIGI is a non-profit industry association representing Apple, Discord, eBay, Google, HelloFresh, Meta, Microsoft, Pinterest, Snap, Spotify, TikTok, Twitch and Yahoo. We note that some members will also provide their detailed input to you via their own submission, regarding their specific views on this reform.

DIGI shares the Government's commitment to improving online safety for Australians. We have supported a well-crafted Digital Duty of Care (DDoC) consistently since the Statutory Review of the Online Safety Act 2021 (OSA),[2] and we welcome this exposure draft as the chance to get that framework right. We support the Bill's core direction: a single, risk-based duty that requires services to assess and mitigate harm, in place of prescriptive rules tied to specific services or features.

What DIGI supports

DIGI supports the thinking behind several specific elements of the Bill:

- **Risk assessments.** Requiring providers to assess and document risk at least annually, and to take effective measures in response, is consistent with DIGI's long-standing position and the systems-based model that underpins the Codes. This is supported by DIGI in principle but it should be limited to the Duty, not all "foreseeable risks" which is an unclear standard. Additionally, the Commissioner's power to add new requirements or shorten reporting intervals by legislative instrument may be used in ways that add to the administrative burden on services but do not demonstrably improve safety outcomes. This also highlights our concerns about the unfettered scope of that discretion which runs through this submission.[3]
- **Graduated enforcement.** A path from formal warning to remedial direction to civil penalty, with the chance to rectify first, is a sound compliance model in principle. However, if the intention is for the strengthened penalty to act as an incentive on services to achieve better safety outcomes,

[1]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft, 7 September 2026).
[2]Delia Rickard (independent reviewer), Report of the Statutory Review of the Online Safety Act 2021 (Report, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, October 2024).
[3]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 26A.

that is undercut by the uncertainty of scope of the Duty and the unclear standard expected of services to achieve compliance with the Duty elsewhere in the Bill, addressed further below.[4]

- **User empowerment tools.** Requiring services to give users control over their own experience, including over recommended content, feature settings and time limits, is consistent with our position that people should have meaningful choices. This is supported in principle. However, this provision gives the Minister unfettered power to make rules that go to the fundamental operation of services, including how content is surfaced to users, without meaningful parliamentary oversight or adequate guardrails. Where not already addressed under the existing requirement to provide a safe online environment, control over the operation of services should be limited to clearly articulated user choice requirements spelled out in the Bill itself that are principles based and sufficiently flexible to take account of fundamental differences between services. Any direction should set an industry standard and not be platform-specific.
- **A single risk assessment and reporting regime.** DIGI welcomes the simplification of the OSA by replacing the existing complex framework of Codes, Basic Online Safety Expectations and multiple transparency reporting requirements with a single Duty and set of transparency reporting requirements.
- **Decoupling content requirements from the Classification Scheme.** We have long expressed concern about the difficulty of applying the National Classification Scheme, designed to individually vet the suitability of specific types of publications and films before release to the public to the online environment. Some of the new types of content introduced to replace Class 1 and Class 2 are undefined. That should be addressed in drafting and the Commissioner should also be required to be transparent on how content decisions are made to promote consistent compliance across services.
- **Fake nude material takedown powers.** Extending takedown powers to apps and websites designed or predominantly used to generate fake nude material is consistent with our existing support for criminalising nudify apps, and builds on results the industry's own Codes have already delivered: eSafety has used the industry-drafted Age-Restricted Material Codes to drive seven of Australia's most-used nudify services from the market or into compliance, described above. This is supported in principle.[5]
- **Researcher data access.** DIGI supports researcher access to platform data in principle, where it complements transparency reporting and is properly targeted at systemic risks. However, the penalties for breach of the duty to provide access where no harm is apparent, should be proportionate. Further, any scheme needs real safeguards to protect the integrity and security of services' systems and sensitive data, including users' personal information, and needs to account for the potential impact on smaller businesses, addressed further below.
- **Additional reporting on enforcement priorities by Commissioner.** The additional public transparency required of the Commissioner on enforcement priorities is an improvement we asked for and is also welcome.

[4]Ibid cl 26B–26D.
[5]Ibid Schedule 1, Part 1, Division 1, cl 86B–86C.

While DIGI supports the thinking behind these principles, as expressed in the Bill, several need significant rework before they deliver on the Government's policy goal of improved online safety outcomes for Australians.

DIGI's key concerns

In summary, DIGI's key concerns are:

- **Scope by discretion.** Too much of the Duty's reach is left to the Minister and the Commissioner, including the Minister's power to determine what material and conduct counts as harm, what services are in scope of the Duty and certain requirements, and the ability to design specific features of services, and the Commissioner's powers in respect of complaints processes, transparency reports, and remedial actions. These powers are unconstrained by the draft Bill and do not include any specific requirement for the Commissioner to consult with the community.

- **An undefined compliance standard.** Neither the obligation for services to "ought reasonably to know" of "all foreseeable risks", of "harm" nor the compliance standard of a "safe online environment" is defined clearly enough for services, the Commissioner or a court to assess compliance.

- **Commonplace design features across all digital services are presumed harmful.** Common features are deemed harmful by the Bill itself, rather than assessed through a holistic assessment of a service's risk in order to meet the core obligation to provide a safe environment. The requirement to implement a specific user empowerment tool should apply only where warranted by a service's assessed risk, with services able to adopt alternative or additional measures — such as timers for children — where these are more appropriate to the identified risks such as addiction.

- **Overly restrictive and burdensome on lawful forms of communication.** The only exception to the digital duty of care is for private conversations with adults. This raises concerns about the duty being overly restrictive and burdening the implied freedom of political communication where there are no public interest exceptions (e.g. news and journalism).

- **Weak safeguards on researcher access.** The data access scheme lacks independent oversight, a materiality threshold that is the basis for access and protection for sensitive data. The lack of independent oversight raises questions also about the independence of the research that will result. Open-ended data access could also be impractical for smaller digital services.

- **Unclear requirements.** The Bill removes the Codes' requirements for proactive detection of illegal child sexual abuse and pro-terror materials and protections for children without specifying any clear substitute requirements.

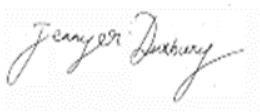
The detail of this submission sets out recommendations for changes to the Bill.

Approach to consultation on the Bill

The Department released the exposure draft on 7 September 2026 and has invited submissions of up to five pages by 22 September 2026, a two-week window that also includes a roundtable on 10 September.[6] Given the reach of this Bill, which would apply to effectively every online service operating in Australia, and the number of matters left to Ministerial and Commissioner discretion, the limited consultation process does not allow proper engagement from stakeholders with the detail of such a significant reform. This submission is longer because the issues require it. DIGI requests that it be accepted on that basis, and that the Department commit to a further consultation opportunity, with adequate time to respond, before the Bill, with its Explanatory Memorandum, is introduced into Parliament.

DIGI and its members remain committed to working constructively with the Department and the Commissioner on a Digital Duty of Care that is workable, durable, and delivers better safety outcomes for Australians. We welcome the chance to discuss this submission further.

Yours sincerely



Dr Jennifer Duxbury
Director Policy, Regulatory Affairs and Research
Digital Industry Group Inc

[6]Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, correspondence and consultation materials on the Digital Duty of Care exposure draft (September 2026), inviting submissions of up to five pages by 12:00pm 22 September 2026.

DIGI's recommendations on the exposure draft

Australia's Online Safety Codes are delivering improved safety outcomes

DIGI led development of the 15 industry Online Safety Codes and two regulator-developed Standards registered under the OSA, covering eight sectors across the technology stack through more than 300 risk-based safety measures. These Codes are a working, enforceable model for online safety regulation. eSafety's recent enforcement record shows this in practice: action against a UK-based nudify provider in late 2025 forced three of Australia's then most-visited nudify services from the market; Directions to Comply issued in May and June 2026 under the industry-drafted Age-Restricted Material Codes targeted providers attracting close to 40,000 and around 50,000 Australian visits a month respectively; and the seven most widely used nudify services in Australia have now either withdrawn from the market or implemented age-assurance measures. Non-compliant services face civil penalties of up to $49.5 million under the Codes. The Minister for Communications has recognised this framework publicly, saying the Government is leading the way with the OSA including its enforceable industry codes.[7]

[7]eSafety Commissioner, media release, 'eSafety action prevents services ‘nudifying’ Australian school children' (27 November 2025); The Hon Anika Wells MP, Minister for Communications, press conference, Brisbane, 14 July 2026; DIGI, Submission to the Senate Environment and Communications Legislation Committee, Inquiry into the Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill 2026 (23 July 2026) 7.

This record compares well with frameworks in the UK and EU, and in several respects goes further:[8]

Feature	Australia (Codes & Standards)	EU (DSA / Terrorist Content Reg)	UK (Online Safety Act 2023)
Sectors covered	Eight, the full technology stack: social media, messaging, hosting, ISPs, search, app stores, apps, websites, dating services, equipment manufacturers and suppliers, ISPs, and generative AI models/chatbots.	Partial. DSA mainly targets platforms and search; hosting, equipment and ISPs are largely out of scope	Partial. Focus on user-to-user services and search; ISPs, equipment and email are out of scope
Proactive CSAM detection	Required for high-risk services, including social media, file-storage and messaging	Temporary voluntary regime under the CSAM Regulation; proactive detection still developing	Required under illegal content duties for services in scope
Pro-terror content	Mandatory proactive detection and takedown	One-hour reactive removal deadline only	One-hour reactive removal; illegal content duties
Self-harm and eating disorder content for children	Explicit Class 2 obligations across the stack, including AI chatbots/nudify apps	Not explicitly addressed; depends on systemic risk assessments for the largest platforms	Listed as priority harmful content; regulator guidance still in development
Age assurance for children	Mandated for defined high-risk categories of services and materials	Required only for legal-but-harmful content, and only on the largest platforms	Required for services likely accessed by children for pornographic content
Developed with public consultation	Two rounds, over 120 submissions	Through the European legislative process	Through the UK parliamentary process

Australia's co-regulatory model was built on partnership with the Commissioner through extended, multi-round public and industry consultation and is already delivering the enforcement outcomes comparable regimes are still working towards. The report of the Tech Policy Design Institute of its multi-stakeholder design dialogue on 10 August, showed there was strong support for retaining existing

[8]Online Safety Act 2023 (UK) ss 41, 43 (codes of practice, parliamentary procedure); Regulation (EU) 2022/2065 (Digital Services Act) arts 34–35 (systemic risk assessment and mitigation); Regulation (EU) 2021/784 (Terrorist Content Online Regulation); DIGI, Australia's Online Safety Framework: The Codes and Standards (internal briefing, 2026).

protections and capabilities in the OSA Codes: “participants broadly agreed that reform should build upon, not weaken, the protections and regulatory powers and already present in Australia's online safety framework”.[9] The Bill dispenses with these Codes. Schedule 3 repeals Division 7 of Part 9 of the OSA, the provisions underpinning the current Online Safety Codes, once the Duty commences.[10] While DIGI welcomes simplification of the existing OSA framework, if the clear baseline protection of the Codes is removed, the Bill needs to be just as clear about how services are expected to meet their duty without it, an issue this submission discusses further below.

Parliament, not the Minister, should set the scope of the Duty

The Duty's scope depends to an unprecedented extent on the discretion of the Minister and the Commissioner.

Clause 25C lists seriously harmful material and conduct for adults, and clause 25D lists material harmful to children, but the Minister may add to either list by disallowable legislative instrument, whenever satisfied the addition may cause serious harm, which concept is not defined in the Bill. Clause 25G deems five design features: a recommender feature, a logged-in feature, an endless feed, a feedback feature and a time-limited feature, to inherently have negative behavioural impacts, and lets the Minister add to that list the same way.[11]Similarly clause 26(4) grants powers for the Minister to require specified online services to provide specified "user empowerment tools" without definition of what these entail.

None of these powers carries a requirement to consult the public before they are exercised. A disallowable instrument is not an adequate safeguard: it takes effect and is enforceable from registration, and stays in force unless an individual senator or member moves, and wins, a disallowance motion within the ordinary 15 sitting-day window. By using this mechanism the Government can bring a large range of content, conduct or services’ design features within scope of the Duty, with penalties attached, before Parliament, let alone the public, has had a chance to consider it.[12]

These powers can be used to require services to restrict conduct, activity and platform features that are currently entirely lawful for a user to engage in or use. There is no requirement on the Minister to consider how this impacts on the rights and needs of other stakeholders to communicate and reach their audience online, for example, community groups, news media or small businesses. The Bill also places no corresponding obligation on users themselves not to create, post or engage in material the Minister

---

[9] 2026, *Tech Policy Design Institute Digital Duty of Care: Make Tech Care*, Policy Spotlight September 2026, Pp.19

[10]Ibid Schedule 3, Part 1, item 5 (repeal of Division 7 of Part 9 of the Online Safety Act 2021, which underpins the current registered industry Codes).
[11]Ibid cl 25C(2), cl 25D(2) para (f)(ii), cl 25G(2).
[12]Ibid cl 25C(2), cl 25D(2) para (f)(ii), cl 25G(2). Instruments made under these powers are legislative instruments and are disallowable under s 42 of the Legislation Act 2003 (Cth), but take legal effect on registration and remain in force unless and until disallowed.

determines harmful; only services carry that burden. Without corresponding obligations on adult users, enforcement will be more challenging.

Hate speech and misinformation are good examples of the kind of material the Minister could add this way. Neither appears in the Bill, but either could be brought within the Duty later under the same instrument powers, with no requirement to consult the communities most affected. The recent experience of the Australian Parliament on these topics shows why that consultation is important. The Government's own attempt to lower the threshold for a Commonwealth hate speech offence was dropped from the Combatting Antisemitism, Hate and Extremism Bill 2026 shortly before it passed, once it became clear the provision, it lacked parliamentary support.[13] The Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 met the same fate, withdrawn largely over widespread disagreement about how its terms should be defined and its impact on freedom of expression, particularly political expression.[14]Proposals to regulate speech that are contested amongst the community belong in primary legislation, tested through full parliamentary debate.

Similarly the Commissioner has expansive and unconstrained powers to determine complaints processes, transparency reports, and remedial actions 26F, 192G, 205F.

If the current range of broad discretionary powers remain with the Minister and the Commissioner in some form, the Bill should at least require those offices to have regard to a defined list of considerations before exercising any discretion under the Bill, including clauses 25C(2), 25D(2), and 25G(2): the severity of the harm and the extent there is evidence to support it; the breadth of services and users likely to be impacted; whether less restrictive alternatives would achieve the same outcome; the views of affected stakeholders obtained through public consultation; consistency with Australia's human rights obligations, including privacy, freedom of expression and the rights of children including the best interests of the child; the cost and technical feasibility of compliance across different services in scope; and a requirement to review the determination's effectiveness after a fixed period.

DIGI's position: The content, conduct and features within the Duty's scope should be set by Parliament, in primary legislation. If the Government considers future additions are needed, they should go through a further Act, informed by public consultation and debate. The current broad discretionary powers should be constrained by a requirement on these offices to consider factors designed to ensure that these powers are exercised in a way that is proportionate, technically feasible and respectful of Australians' rights and freedoms.

---

[13]Combatting Antisemitism, Hate and Extremism (Criminal and Migration Laws) Bill 2026 (Cth). An earlier version included a proposed racial vilification offence lowering the threshold for criminal liability from an intent-based standard to a broader 'promote' standard; this provision was withdrawn before the Bill passed on 20 January 2026, once it was clear it lacked parliamentary support: see 'Understanding the Federal Government's Proposed Hate Speech Laws', Law Society Journal (online, 19 January 2026).
[14]Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 (Cth), withdrawn November 2024 following public and parliamentary concern about the scope of 'misinformation' and 'disinformation'.

Design features should not be deemed harmful without a proper risk assessment

Clause 25G presumes that five common design features, recommending, staying logged in, an endless feed, feedback signals and time limits, cause harm, regardless of the service or how the feature is implemented. Read literally, this reaches far beyond social media services.[15]

The term “negative behavioural impacts” is itself not defined anywhere in the Bill. Clause 25G asserts that the five listed features have negative behavioural impacts without specifying what a negative behavioural impact is, what evidence would establish one, or how it differs from ordinary, expected engagement with a service. This is a second, definitional gap sitting in addition to the undefined concept of harm addressed elsewhere in this submission. As a result, there are no criteria to evaluate whether restricting a feature or providing empowerment tools has a positive behavioural impact. It also makes it difficult to ensure the Minister is accountable for the fairness and reasonableness of any decision to add a further feature to the list under clause 25G(2).[16]

The definition is broad enough to capture ordinary, everyday services used by Australians and local businesses with no connection to the harms the Duty targets.[17] An online shopping or retail site recommending products from a customer's browsing or purchase history has a recommender feature. A job site matching candidates to vacancies, or recommending roles based on a user's profile, has one too. A maps or navigation app suggesting a route or a nearby point of interest from a user's location data, or a supermarket app suggesting a weekly shop from past orders could all fall within the same definition and be treated as inherently harmful. A login feature and a notifications feed are core to how small business and enterprise tools work.

This Bill is not about a handful of large social media platforms. As drafted, its obligations reach any service with a recommended feed, a login or a search function, including services with no connection to the harms that the reform targets. Undefined obligations of this breadth will be hardest to meet for the smaller Australian services in scope.

A feature's risk is only one aspect of the overall risk of a digital service. Its safety implications need to be evaluated in that broader context, for example, by considering the data it uses, the content it surfaces, the safeguards already in place and whether other technical interventions such as time-outs may be a better solution to address the risk. Judging a feature as ‘harmful’ in isolation misses that crucial point.

DIGI's position: Clause 25G should be removed. Design features should be assessed as part of the risk assessment already required under clause 26A.

---

[15] Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 25G.
[16] Ibid cl 25G.
[17] Ibid cl 25F(1)–(2) (definition of a recommender feature: a service that can select material by reference to information associated with an end-user's account and display it to that end-user).

How the Bill addresses design-feature risk

Beyond the general presumption in clause 25G, the Bill addresses the risk design features pose to users in two different ways. First, clause 25B(1)(c) restricts specific design features from operating for children under 16, regardless of whether users that age are likely to access the service but only on services that meet the definition of a "social media service." Second, clause 26(3)(a) requires services to give all users, not just children, tools to manage those same design features. Both mechanisms are addressed separately below.

The under-16 restriction depends entirely on whether a service meets the definition of a "social media service" in section 13 of the current Act: an electronic service whose sole or primary purpose is online social interaction between two or more end-users, that allows end-users to link with each other and to post material, or any other electronic service specified in the legislative rules.[18] That definition is broad, and literally could reach far beyond conventional social media into messaging apps, multiplayer games with chat functions, professional networking services and dating apps, any service built around end-users interacting with each other. Because the definition can itself be extended to further services by legislative rules, this compounds the Ministerial discretion problem addressed in DIGI's position on scope above. Not only can the Minister add to the list of design features treated as harmful, but the Minister can also expand the range of services to which the resulting restriction applies. Separately, clause 25B(2) lets the Minister determine, by legislative instrument, that a particular service is or is not a "social media service" for this purpose.

We are concerned that in some cases restricting certain design features from operating for under 16's will make some services technically unusable or inaccessible For example, services currently within scope of the social media minimum age restrictions can provide access to under 16 users in a logged out state. The new under 16 restriction may in effect require services to restrict access to account-holders only, impacting use of the services in ways that are beneficial for children, for example, for educational purposes and impacting the rights of adults to access a service without having to create an account because it is in practice impossible to determine the age of a user without an account.

Again, the Bill gives the Minister discretionary power to determine design requirements for an unspecified category of services, without requiring prior consultation, assessment against Australia's human rights obligations (privacy, freedom of expression, children's rights and the best interests of the child), consideration of cost and technical feasibility across different services, or periodic review of the determination's effectiveness.[19]

The second mechanism, user empowerment tools, discussed above. Clause 26(3)(a) requires services to give all users, not only children, tools to manage design features: control over recommended content, the ability to turn features off, and time limits.[20] This is a more direct way of putting control in users' hands than restricting a feature outright for one age group. However, what counts as a qualifying "user

[18]Online Safety Act 2021 (Cth) s 13 (definition of social media service).
[19]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 25B(2).
[20]Ibid cl 26(3)(a).

empowerment tool" will be determined via a separate legislative instrument, not yet released, that we understand the Government will consult on independently of this Bill although there is no requirement that this is the process which will be followed .

The approach taken to design features does not sensibly address the safety risk the Government aims to address with the Bill. The risk that any individual feature of a digital service poses depends on the specific service it sits within, as discussed above. This includes the likelihood it will be accessed by a child. The risk of specific features should not be presumed but must be evaluated through the risk assessment in clause 26A. User empowerment tools that enable user choice can be a good way to mitigate an assessed risk on certain types of services. The Bill could require services to incorporate those tools or alternatives such as timers where appropriate for addressing risks identified by the risk assessment process. However, what qualifies as a user empowerment tool should be defined in the Bill in a way that emphasises user choice and is flexible enough to adapt to different service types with different technical capabilities and risk profiles, set out in the Bill consistent with DIGI's position above. The concept of user empowerment tool should not become a way for the Minister to mandate a single feed model or product design.

DIGI's position: The under-16 restriction in clause 25B(1)(c) and the user empowerment requirement in clause 26(3)(a) are blunt instruments that impact a range of low-risk services and will have unintended consequences, for example, rendering certain services practically unusable or accessible only by signed-up account-holders. The definition of "social media service" that triggers the under-16 restriction should be clarified in the Act given its breadth, and any future extension of it by legislative rules should require consultation and consideration of other relevant considerations. The Bill should be amended to require specific service categories to implement user empowerment tools or alternative tools such as timers where they are a suitable mechanism for giving users meaningful control over these features which a section 26A assessment shows are reasonably likely to cause serious harm. The concept of user empowerment tool should be defined flexibly in the Bill itself.

"Harm" needs a workable legal definition and risk assessments must be tied to the duty

Clause 25E leaves harm undefined. It states only that harm can be caused by material or conduct, whether or not a user experiences or engages with it, with no severity threshold and no requirement that the harm actually, or is likely to, exist. As drafted, this could capture fleeting offence or discomfort on the same footing as serious injury, regardless of a user's engagement, or interaction, with the potentially harmful material or conduct, and gives services, the Commissioner and the courts no objective basis for assessing compliance.[21]

Further, the obligation to act so far as reasonably practicable also considers what the person "ought reasonably to know" about the harm, the risk of harm, and the ways of eliminating or minimising the risk

[21] Ibid cl 25E.

of harm. This significantly broadens the meaning of reasonably practicable and is tied closely to the risk assessment requirement to identify all reasonably foreseeable risks.

This impacts the standard of harm as well. Harm underpins the Duty's compliance standard: Clause 26 requires a person responsible for a service to ensure, so far as reasonably practicable, a safe online environment, and clause 25B defines that environment as one where people are protected from seriously harmful material and conduct, and children are additionally protected from harmful design features.[22] That test, what counts as harmful, and what it means to be protected from it, rests on a concept the Bill leaves undefined. A service cannot design its systems against a standard with no clear meaning, the Commissioner cannot apply it consistently across the services regulated, and a court reviewing a contested penalty has no clear benchmark to test compliance against.

This issue also impacts on the approach to the risk assessment. The current scope of the risk assessment is not limited to the digital duty of care and instead requires service providers to identify 'all reasonably foreseeable risks, including those relevant to the provider's digital duty of care'.It is unclear what risks, in addition to those required to protect children and protect persons from seriously harmful material, are meant to be assessed and addressed.

Under the current industry Codes and Standards, services know, in granular and practical terms, what proactive steps they must take under the Codes to detect and remove illegal material and to apply age assurance to content harmful to children. None of that clarity carries across to the Duty. It is unclear, in practice, when a service must proactively detect content, or apply age controls, against the standard in clause 25D, once the Codes that currently contain those requirements are gone.

The current OSA already has better understood concepts of harm. Section 5 defines serious harm as serious physical harm or serious harm to a person's mental health, including serious psychological harm and serious distress, but excluding ordinary emotional reactions such as distress, grief, fear or anger. This standard has applied to the adult cyber-abuse scheme since 2022.[23]

DIGI's position: The Bill should adopt the existing section 5 definition of serious harm for adults. For children, the Bill should either apply the same standard or the existing section 6 test: material likely to seriously threaten, intimidate, harass or humiliate a child. Clause 25D(1)(f)(i) currently sets no defined standard at all.[24] The 26A risk assessment process should be tied to the Duty of care so it is clear what risks services must assess to be compliant.

What counts as a "safe online environment" is unclear

Clause 26 sets the Duty's core compliance test: a person responsible for a service must ensure, so far as reasonably practicable, a safe online environment. Clause 25B defines that environment as one where

[22]Ibid cl 26(1)–(2), cl 25B.

[23]Online Safety Act 2021 (Cth) s 7 (adult cyber-abuse scheme).
[24]Ibid ss 5–6.

people in Australia are protected from seriously harmful material and conduct, and children are additionally protected from harmful design features.[25]

The concept of “protected from” is undefined and can be read two ways. It could mean a service must eliminate exposure to harmful material altogether, or it could mean a service must take reasonable steps to reduce the risk of exposure. These are very different obligations. A zero-exposure standard is unachievable for any service that allows user-generated content or real-time interaction between users, and would set a materially stricter test than the reasonable-steps standard applied under Australian common law and comparable overseas regimes.[26]

Clause 25H's reasonably practicable test, which determines whether a service has met its duty, only works against a clear, objective standard. Every limb of that test, the likelihood of harm, its degree, and what the service knew or ought to have known about it, is defined by reference to the concept of “harm”. As drafted, a well-understood legal test is being applied to an undefined standard: whether a service is safe cannot be assessed without knowing what “harm” and “protected from” mean, and whether a service acted reasonably cannot be assessed without knowing what safe means. Left this way, compliance turns on an untested, contestable judgment call by the Commissioner, rather than a clear standard like services can design their systems against in advance.[27]

DIGI's position: Clause 25B should specify that "protected from" means a duty to take reasonable steps to implement systems and processes to minimise the risk of harm, consistent with the standard in the Basic Online Safety Expectations which it replaces.

The test of "reasonably practicable" is unbalanced

Additionally, Clause 25H defines reasonably practicable as what was reasonably able to be done at the time, weighing up a list of relevant matters: the likelihood of harm, its degree, what the service knew or ought to have known, and the availability of ways to eliminate or minimise the risk. Cost and privacy impact are also on that list, but they are not weighed the same way as the rest. Clause 25H(e) makes them relevant only "including whether" they are grossly disproportionate to the risk, a far higher bar than the ordinary weighing the other factors receive. This is contrary to the basic approach of the common law of negligence in which the duty of care concept is founded and the fundamental bases of human rights law which treats all rights as equal without any clear justification. In practice this means a measure's cost or its intrusion on privacy will be disregarded unless it is widely out of proportion to the risk, not just heavier than the risk warrants. This is likely to impact on a range of user privacy and security protective measures adopted by services such as encryption, which in effect prioritises an unclear category of “safety” harm risks over risks to a user's private communications or personal data.

[25]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 26(1), cl 25B.
[26]Online Safety Act 2023 (UK); Regulation (EU) 2022/2065 (Digital Services Act). Both regimes require services to take proportionate risk mitigation measures, not to eliminate risk altogether.
[27]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 25H.

DIGI's position: If, contrary to the above recommendation, the “reasonably practicable” test is retained, the reference to "grossly disproportionate to the risk" concept should be removed from clause 25H(e)(i) and (ii), so cost and privacy impact are weighed as ordinary factors in the test, consistent with the other matters in clause 25H, and basic principles of negligence and human rights law.

New Harm categories need to be defined in the Act, with Commissioner guidance and public transparency

DIGI supports decoupling the Bill’s content requirements from the National Classification Scheme. As DIGI has said consistently, the Scheme was designed to individually vet the suitability of specific publications and films before release, not to regulate content at internet scale in real time, and the independent statutory reviewer found the resulting Class 1 and Class 2 definitions confusing, overly complicated and unfit for purpose.[28] The new categories of seriously harmful material and conduct (clause 25C) and material and conduct harmful to children (clause 25D) are a welcome step away from that model.

The new categories are not the same as those in existing laws (although they are in some cases similar). This variance creates significant interpretation issues that need to be addressed. The Classification Scheme, whatever its faults, gave services, users and the courts a body of published classification decisions and guidelines to work from. The Bill’s new categories start with none of that. Clause 25D in particular contains an open catch-all, at present undefined, for “any other material or conduct that could inflict serious harm to a child”, which applies immediately with no Ministerial instrument required.[29] This category is open-ended and would be highly contestable in practice: reasonable people can and will disagree about what belongs within it, and services, the Commissioner and the courts have no shared reference point for deciding.

These new categories need to be defined clearly in the Act itself, consistent with DIGI’s position elsewhere in this submission that the Duty’s scope should sit with Parliament, not the Minister. They also need practical support the Bill does not currently provide: guidance from the Commissioner on how each category will be interpreted and applied, developed in consultation with industry and other stakeholders, and transparency about how individual content decisions are made once the Duty is in force. DIGI has previously recommended that the Commissioner’s case-by-case decisions on where content falls within these categories be recorded in a publicly accessible database, so services can apply the categories consistently and the public can see how the standard is actually being applied.[30]

DIGI’s position: the content categories in clauses 25C and 25D, including the open-ended catch-all in clause 25D(1)(f)(i), should be defined exhaustively in the Act. The Commissioner should issue guidance,

[28]Delia Rickard (independent reviewer), Report of the Statutory Review of the Online Safety Act 2021 (Report, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, October 2024), finding the definitions of Class 1 and Class 2 material confusing, overly complicated and unfit for purpose.
[29]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 25D(1)(f)(i).
[30]DIGI, submissions to the Department on the Online Safety (Unlawful Material) Codes review.

developed in consultation, on how each category will be interpreted, and should publish a case-by-case record of content determinations in a publicly accessible database to ensure consistent application and public transparency.

Researcher data access needs real safeguards

DIGI supports well-designed, independent researcher access to platform data. Done well, it strengthens the evidence base for policymakers and platforms, supplements transparency reporting rather than duplicating it, and helps identify emerging online harms earlier. Established models in other regulated fields, independent ethics approval and ongoing oversight in clinical research, and the EU's vetted-researcher scheme under the Digital Services Act, show this works when scope, credentialing and oversight are clearly defined in legislation.[31]

The scheme in Part 14 falls well short of that model:

- **No independent oversight.** The Commissioner alone approves researchers, and the data access rules governing scope, process and safeguards are made by legislative rules. The scope and administration of researcher access sit entirely with the Minister and the Commissioner, with no independent body in the loop. DIGI could support Commissioner-administered approval if paired with independent oversight of individual access decisions, along the lines of the EU's Digital Services Coordinator model.[32]
- **No materiality threshold.** The duty to give access applies to any provider of an online service, a definition that reaches equipment and installation providers as well as platforms, with no scale or risk threshold limiting it to the largest services. Smaller Australian businesses with no dedicated compliance function would carry the same obligation as major platforms. DIGI could support an access obligation targeted at services that meet a defined materiality threshold.[33]
- **No defined limit on the data in scope.** What data researchers can access is left entirely to legislative rules, with no floor or ceiling set in the Bill itself. DIGI could support the Bill specifying categories of data in scope directly, with clearly sensitive material, individual user content, security infrastructure and core proprietary systems excluded from the outset.[34]
- **Commercial sensitivity is not addressed.** The rules may guard against a researcher misusing data for their own commercial benefit, but nothing in the Bill protects a service's own commercially sensitive systems, such as recommender or advertising systems, from exposure through the access process itself. DIGI could support express protection for a service's commercially sensitive systems.[35]

[31]Regulation (EU) 2022/2065 (Digital Services Act) art 40 (vetted researcher data access, overseen by an independent Digital Services Coordinator).
[32]Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) (Exposure Draft) cl 205B(1)(b), (2), cl 205C(1).
[33]Ibid cl 25A(1)(h), cl 205C(1).
[34]Ibid cl 205C(3)(a).
[35]Ibid cl 205C(3)(h).

- **No requirement to consult the service.** Nothing requires the Commissioner or an approved researcher to consult the relevant service on the scope, timeframe or feasibility of a request before access is mandated. This assumes the requested data exists and can be produced in the form sought, rather than testing that first. DIGI could support a requirement for the independent oversight body to consult the service on scope, timeframe and data availability before approving access.[36]
- **No defined research proposal required.** Online safety related research needs only to be of a kind prescribed by the legislative rules to be in the public interest, a category-level test only. DIGI could support access being tied to a specific, pre-approved research question or protocol, consistent with models used in clinical research.[37]
- **No limits on quantity or frequency of research.** Nothing limits the number of researchers or proposals which may be approved to access a service's data, or the frequency and duration of access requests. This could create a continuing and unpredictable compliance burden, particularly for smaller digital businesses without dedicated teams to assess requests, prepare data and manage secure access. DIGI could support an approach that ensures the amount and frequency of access is proportional to the capacity of a service to support it, subject to periodic review by an appropriate independent body, and limited to the data strictly needed for a defined research proposal.
- **Disproportionate penalties.** A breach of the duty to provide data access carries a maximum penalty of 6,000 penalty units, $2.184 million for an individual and $10.92 million for a body corporate.[38] This is disproportionate to the severity of the contravention, in particular when there is negligible risk of harm to Australians. The penalty value is akin to a contravention of a removal notice provision, and should be reduced proportionate to the breach.

DIGI's position: Access should be built on defined scope, demonstrated need, credentialed researchers, independent oversight, enforceable data-handling obligations and a materiality threshold, administered by a body independent of the Minister and the Commissioner, and only after that body has consulted the service on the scope and availability of the data sought.

Sock puppet identities. The Bill gives the Commissioner and approved researchers civil protection for using false identities to research online safety.[39] The Bill authorises the use of sock puppet accounts despite anything to the contrary in any Australian law, or any agreement, contract, deed, policy or other document.[40] Platforms actively detect and remove sock puppet accounts to protect users from coordinated inauthentic behaviour, a common mechanism for disinformation campaigns. Clause 205J, provides lawful means to circumvent a platform's policies and creates tension with proposed Digital Duty of Care which requires platforms to mitigate risks, including inauthentic behaviour. Protection for use by researchers of sock puppet accounts should not be needed by researchers once the data access scheme

[36]Ibid cl 205C(3)(d).
[37]Ibid cl 205B(3)(c).
[38]Ibid cl 205D.
[39]Ibid Schedule 2, Part 14, Division 3, cl 205G, 205K.
[40]Ibid cl 205J(2).

above is in place. The scheme achieves the same purpose. Further, the Bill should clarify how the sock puppet obligation and digital duty of care obligation are intended to be reconciled.

Additionally, the authorised activities which may be used by the the sock puppet identities likely involve deliberately triggering or testing a platform's safety and security, in particular Clause 205K(1)(f), and it is not clear whether: (a) intentionally testing a platform's response to a deliberate policy breach; and (b) either: (i) the platform not taking enforcement action; or (ii) the platform taking enforcement action against the sock puppet identities; exposes the platforms to regulatory risk. The Bill should not operate to circumvent platform policies and safety tools and should establish a mechanism by which the service can verify that an account is being lawfully operated under the provision, and should be limited to benign activities such as observation.

Who holds the duty

Who holds the duty. The Bill defines a person responsible for a service as the provider, or a person in a position to exercise day-to-day control, without saying whether this reaches parent companies, individual managers or trust and safety officers, or both. This should be clarified before the Bill is introduced.[41]

Penalties. A breach of the Duty carries a maximum civil penalty of 60,000 penalty units, $21.84 million for an individual and $109.2 million for a body corporate at current values.[42] The graduated model is a positive design, but any value of increased penalty regime is undermined by the vague compliance standard and a scope that can expand at the discretion of the Minister and the Commissioner via legislative instrument. The penalty quantum and its impact on "persons exercising control " should be revisited once scope and the harm standard are settled.

Summary of DIGI recommendations

A. Parliament, not the Minister or Commissioner, should set the content and conduct within the Duty's scope, in primary legislation, with future additions going through a further Act informed by public consultation. If broad discretionary powers remain, the Bill should require the Minister and Commissioner to have regard to a defined list of considerations, including the evidence for harm, the breadth of services affected, less restrictive alternatives, public consultation, human rights impacts, cost and feasibility, and a review requirement, before exercising them.

[41] Ibid cl 25A(2).
[42] Ibid cl 26B, 26D. Penalty unit value of $364 applied from 1 July 2026 under s 4AA of the Crimes Act 1914 (Cth), consistent with the value applied in DIGI's Submission to the Senate Environment and Communications Legislation Committee, Inquiry into the Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill 2026 (23 July 2026) fn 7; corporate penalties apply the ×5 multiplier under s 82(5) of the Regulatory Powers (Standard Provisions) Act 2014 (Cth).

B. Clause 25G should be removed. Design features should be assessed through the risk assessment in clause 26A instead. The risk assessment process should also be limited to assessing risks in scope of the duty, not" all foreseeable risks" as drafted.

C. The under-16 restriction in clause 25B(1)(c) and the user empowerment requirement in clause 26(3)(a) are blunt instruments that risk unintended consequences for low-risk services. The definition of "social media service" should be clarified in the Act, with any future extension by legislative rules subject to consultation. User empowerment tools should be defined flexibly in the Bill itself and required only where a clause 26A risk assessment shows a service is reasonably likely to cause serious harm.

D. The Bill should adopt the OSA's existing section 5 definition of serious harm for adults, and either that standard or the section 6 test (material likely to seriously threaten, intimidate, harass or humiliate a child) for children. Clause 25D(1)(f)(i) currently sets no defined standard at all.

E. Clause 25B should specify that "protected from" means a duty to take reasonable steps to implement systems and processes that minimise the risk of harm, consistent with the standard in the Basic Online Safety Expectations which it replaces.

F. If the reasonably practicable test is retained, "grossly disproportionate to the risk" should be removed from clause 25H(e)(i) and (ii), so cost and privacy impact are weighed as ordinary factors, consistent with the other matters in clause 25H and basic principles of negligence and human rights law.

G. The content categories in clauses 25C and 25D, including the open-ended catch-all in clause 25D(1)(f)(i), should be defined exhaustively in the Act. The Commissioner should issue guidance on interpretation and publish content determinations in a publicly accessible database.

H. The researcher data access scheme should be administered by a body independent of the Minister and the Commissioner, limited to a defined materiality threshold and scope of data, and subject to prior consultation with the service, with credentialed researchers and enforceable data-handling obligations.

I. The civil protections for the Commissioner and approved researchers to use false identities (clauses 205G, 205K) are unnecessary once the data access scheme above is properly safeguarded, and should be removed.

J. Clause 25A should clarify whether responsibility for persons exercising day to day control of an online service extends to parent companies, individual managers, or both.

K. The Penalty quantum under clause 26B and its application to “persons in control” under Clause 25A should be revisited once the Duty's scope and harm standard are settled.

L. The Department should accept submissions of the length this reform requires, and commit to a further consultation opportunity once the Bill and Explanatory Memorandum are introduced into Parliament.