



BY EMAIL AND PDF ONLY

May 15th, 2026

To:

Ms Anthea Fell (Assistant Secretary, Online Safety)

Mr Andrew Hyles (Assistant Secretary, Digital Platforms, International and Policy)

Dear Ms Fell and Mr Hyles,

The team at Match Group has read with interest the recent Australian Government's Response to the Statutory Review of the Online Safety Act (OSA).

Attached is a position paper that the team has prepared which focuses on key issues arising from the Government Response to the OSA Review, particularly in regard to the Digital Duty of Care (DDC). The paper is informed by Match Group's experience working with other jurisdictions that have implemented similar approaches to online trust and safety.

Our SVP Trust & Safety, Yoel Roth, is visiting Australia in June accompanied by our APAC Corporate Affairs Lead, Camélia Assaoui. Yoel and Camélia look forward to discussing these and other issues with you during their upcoming visit.

Please do not hesitate to reach out if you have any questions in the interim.

Yours sincerely,

Katie Peters

Senior Vice President, Corporate Affairs

Match Group

A handwritten signature in cursive script that reads 'Katie Peters'.

Government Response to the OSA Review

Match Group comments

Context

This note adds to Match's input to the industry consultations on the DDC in December 2025 and provides feedback following the recent release of the Government Response to the OSA Review.

About Match Group

Match Group is a leading provider of digital technologies which help people make meaningful connections. Our portfolio includes Tinder, Hinge, OkCupid, Plenty of Fish, and Match.com, serving users in more than 186 countries and over 60 languages. User safety is fundamental to Match Group's mission to spark meaningful connections. Trust and safety are embedded across our products, policies and operations, with continuous investment in tools, technologies and teams to help people connect with confidence.

In Australia, Match Group has played a leading role in advancing industry standards, including through the development of the voluntary [Online Dating Code of Conduct](#). We work closely with government, law enforcement and NGOs to strengthen safety outcomes, including through user education, reporting mechanisms, and escalation pathways for serious incidents.

Overall view

Match Group has worked with governments in other jurisdictions, including in the United Kingdom and the European Union, as they have implemented similar DDC-type models and understands that the Australian Government is seeking to learn from these experiences.

Match Group believes it will be important for the DDC framework to preserve proportionate, sector specific approaches to online safety obligations, recognising the different risk profiles, functionalities, and user bases of online services. Building on eSafety's existing Online Safety Codes and Standards framework, while preserving the role of sectoral voluntary codes such as the Online Dating Code of Conduct, would help ensure that broad DDC obligations are applied proportionately, effectively, and with clear compliance expectations for providers.

Concerns with broad, risk-based obligations

The Government Response to the OSA confirms that the DDC will place broad obligations on online providers to take greater responsibility for managing the risk

of harms occurring on their platforms. The DDC envisages these obligations will apply to harmful conduct and activity as well as harmful content. It also foreshadows further amendments to the OSA to ensure that the DDC creates an effective, simplified framework which operates coherently with related initiatives, including privacy law reforms.

As a company committed to online safety, Match Group has globally supported, and will continue to support, laws that require online platforms to take reasonable steps to keep their users safe. Match Group is strongly of the view that broad, risk-based obligations must be accompanied by the necessary level of regulatory guidance to provide a reasonable degree of certainty for responsible online service providers with a proven record of proactively investing in trust and safety solutions and complying with online safety regulation.

This is particularly important given it appears that DDC obligations will apply to harmful conduct and activity, which is significantly more challenging to define, prevent and enforce against, particularly as conduct-based harms may manifest offline or on unrelated online platforms, rather than on the platform where users were first introduced. Therefore, it is crucial that the expectations on online providers in terms of reasonable steps are practically implementable and clearly enunciated in formal regulatory guidance.

It is important to recognise that responsible online providers taking reasonable steps in accordance with their regulatory requirements will not be able to eliminate all harms, particularly in adversarial domains (such as combatting online scams and fraud). This means that the DDC should be clear that it is holding providers to a "reasonableness" standard, rather than a strict liability standard. When online providers can demonstrate they are taking the reasonable steps to promote safety and prevent harms, they should be afforded the business certainty of knowing that they are complying with their DDC obligations.

Proposed approach to provide business certainty

We ask that the Department gives utmost consideration to the need for providing clear and unambiguous regulatory guidance to online providers along with appropriate immunity/safe harbour protections for providers that undertake good-faith trust and safety actions in accordance with any reasonable steps requirements.

Comparable frameworks, including the Digital Safety Act in the EU and the Online Safety Act in the UK, include concepts that provide varying levels of safe-harbour and enforcement protections for online providers that demonstrate due diligence and compliance with regulatory requirements such as codes of practice. These protections help provide clear compliance pathways and meaningful legal certainty for providers acting in good faith.

Recommendation 9 of the OSA Review contemplates eSafety making mandatory rules/codes but expressly states that compliance with these rules/codes should not create safe harbours. The Government Response agrees with this recommendation in principle. While we understand that the Government desires to keep flexibility in light of changing technology, Match Group believes that including safe harbours is among the best ways to incentivise desired behaviour and drive effective compliance with rules/codes developed by eSafety.

Greatest reach or risk obligations

We also note that several recommendations in the OSA Review (Recs. 6, 10, 11, and 13) relating to the DDC would impose additional obligations on services considered to have the “greatest reach or risk”. The Government Response supports these recommendations in principle.

Match Group’s view is that putting the greatest obligations on platforms with the “greatest reach or risk” has worked well in other safety regulatory contexts, and believes that they could work well in Australia under similar guidelines. In particular, Match Group believes that the greatest obligations should fall on those with the greatest impact on Australian users. Looking to the DSA and the UK Online Safety Act, thresholds created under those regimes were set around 10% of the population in the jurisdiction, and Match Group believes that using a clear definition that is consistent with those set by other regulators will provide the greatest net benefit to the online ecosystem.

Internal Complaints Handling

Recommendation 25 of the OSA Review, which the Government Response supports, would require the retention of easily accessible, simple, and user-friendly internal complaint-handling processes aligned with a code on internal dispute resolution.

Match Group’s platforms already have easy-to-use reporting and complaint tools and appeals processes, which are available to users throughout their experience and have been continuously developed and refined over time to give them greater control at every stage of their journey.

Match Group notes that this part of the OSA Review (7.6 Dispute Resolution) contemplates complaint-related rights in relation to user harms and actions that might be taken against users (e.g. removal of content, suspensions, and bans). Recommendation 26, which is noted in the Government Response, calls for the development and implementation of an external Ombuds scheme.

As an organisation that takes a 'safety first' approach to complaints about unacceptable behaviour on our platforms or involving users who connected through our services, Match stresses the need for the Government to be mindful about rights and appeal mechanisms that might unintentionally undermine user safety (e.g. requiring the provision of detailed reasons to banned users to facilitate appeals could enable the user to infer the identity of a complainant, exposing that person to retaliation or other safety risks.). Match believes that the Government should consult further with industry prior to considering any external appeals processes.

Conclusion

Match Group supports the Government's objective of strengthening online safety protections for Australians. To ensure the framework is effective and workable, Match encourages the Government to provide clear regulatory guidance, proportionate obligations for services with the greatest reach or risk, meaningful safe harbour or immunity protections for good-faith compliance, and safeguards that reflect the privacy and safety sensitivities of online dating services. Match Group welcomes further consultation as DDC legislation and any related rules, codes, or guidance are developed.

Ends

OFFICIAL: Sensitive



Australian Government

 Department of Infrastructure, Transport,
 Regional Development, Communications, Sport and the Arts

Digital Duty of Care – Consultation briefing and meeting notes

May 2026

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
Monday 18 May 2026			
Tech Policy Design Institute (TPDI) 1:30pm 18 May 2026	Zoe Jay Hawkins <i>Co-Founder, Deputy Executive Director</i> Johanna Weaver <i>Co-Founder and Executive Director</i> Formerly the Tech Policy Design Centre, TPDI is an independent think tank focused on technology policy. Interests include young people's use of social media and technology's impact on democracy. TPDI is funded by the Tech Policy Design Fund whose members include DISR, Department of Finance, Amazon, Apple, Microsoft and Atlassian.	• Support preventative, risk-based obligations on industry to anticipate and prevent risks to Australian users. Legislation should be future proof – it should not need amendments to identify emerging harms as new features are introduced • Support providers being held accountable for enforcing their terms of service. • Strong compliance measures should include transparency obligations, strong penalties, direct right to action for individual users and international coordination on enforcement. • Support greater coordination of tech policy across government – online safety should be part of a broader vision for Australia's digital future, alongside reforms relating to privacy, AI and misinformation.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	MO/Dept Attendees: Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)		s47C
Digital Rights Watch 2:00pm 18 May 2026	Lizzie O'Shea <i>Chair</i> Tom Sulston <i>Deputy Chair and Head of Policy</i> Digital Rights Watch is a charity organisation founded to promote and defend human rights as realised in the digital age. They are primarily concerned with the human rights, safety and wellbeing of individuals and communities in the digital age and advocate for privacy, democracy, fairness and freedom . MO/Dept Attendees: Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)	• Broadly supportive of the implementation of a duty of care but have raised questions about implementation, what constitutes reasonable steps and whether a duty of care could lead to overreach. • Additional safeguards are necessary to ensure the Act upholds fundamental human rights and supporting principles. Online safety policies often threaten to infringe upon human rights, e.g. by undermining end-to-end encryption, privacy-invasive methods for age verification, processes which reduce or threaten online anonymity, and the reliance on increased automated content moderation. • Caution against 'unreasonable expansion' of the eSafety Commissioner's remit. Supportive of more in-depth mandatory transparency and accountability reporting from eSafety.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

			s47C
Tuesday 19 May 2026			
IGEA (Dept. only) 12:30pm 19 May 2026	s47F IGEA is the industry association representing and advocating for the video game industry in Australia, including the developers, publishers, and distributors of video games, as well as the makers of game platforms, consoles and devices. IGEA has over a hundred members including Google, Microsoft, Netflix, Nintendo, Roblox and Ubisoft. MO/Dept Attendees: Andrew Hyles, s22(1)(a)(ii)	- Consider the duty should not be applicable to online gaming services covered under the NCS. - Support decoupling the OSA from the NCS – the OSA should only address illegal and unclassifiable online content - Support a duty of care that is principles-based, proportionate, flexible, technology-neutral and outcomes-focused. The duty obligations should be proportionate to the service type and risk profile and be supported by consolidated reporting and accountability mechanisms. The duty should also be internationally coherent. - See the duty as an opportunity to simplify the OSA framework. - The duty should avoid overlap with the BOSE and codes under the OSA and consider broader regulatory arrangements across government (classification reforms, consumer law, privacy reforms) to ensure the whole of government approach is complementary. The duty should distinguish between preventing access to and preventing the creation of harmful material – preventing access will be more reasonably practicable and technically feasible.	

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
Wednesday 20 May 2026			
Alannah and Madeline Foundation (AMF) and Dolly's Dream 10:00am 20 May 2026	Ariana Kurzeme <i>Director, Policy & Prevention</i> Sarah Davies AM (did not attend) <i>Chief Executive Officer</i> Jessie Mitchell <i>Advocacy Manager</i> AMF is a national not-for-profit focussed on keeping children free from violence and trauma. AMF engage in advocacy work and provide care and prevention programs through the eSmart program and in partnership with Dolly's Dream. Dolly's Dream are a nationally trusted, evidence-based anti-bullying organisation, committed to helping children, young people and families live happy and safe lives, free from bullying. Their focus is on kids in rural, regional and remote areas across Australia. MO/Dept Attendees: Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)	• Supportive of introduction of duty of care. • Support risk-based regulation but concerned about industry self-categorisation. Risk profile should be informed by functionality. • Concerned by narrow scope proposed in previous consultation. Would like to see the duty go beyond content and address conduct, contact, compulsion harms and commercial harms, systemic risks from platform design and operations, and other risks from emerging technologies. • Question where AI fits into the duty of care model. • Expressed importance of aligning framework with other relevant reforms including children's online privacy code and AI regulation. • New reforms must be supported by a strong community education and awareness raising.	s47C
Equality Australia	s47F	• No known positions on duty of care.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
11:30am 20 May 2026	s47F A national organisation dedicated to equality for LGBTIQ+ people, to improve the wellbeing and circumstances of LGBTIQ+ people in Australia and their families. Teddy Cook is the Chair of #transequality within the organisation. MO/Dept Attendees: Andrew Hyles, s22(1)(a)(ii)		s47C
DIGI 2:00pm 20 May 2026	Jenny Duxbury <i>Director Policy, Regulatory Affairs, and Research</i> Sunita Bose Kate Blashki DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, Linktree, Meta, Microsoft, TikTok, Twitch, Spotify, Snap, X (f.k.a Twitter) and Yahoo. MO/Dept Attendees: Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)	• In principle, support a duty focused on systems and processes and underpinned by safety by design, risk assessment, mitigation and measurement, that is flexible and proportionate. • Support a focus on content and behaviours that cause psychological and physical harms, rather than broader economic, societal or reputational harms dealt with by other legislation. • Recommend drawing on UK approach which is explicitly proportionate in relation to defined harms rather than a singular legal duty. Support flexibility provided by UK OSA. • Raised concerns about overlapping requirements in an already complex framework. The duty should aim to reduce	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
		the existing regulatory complexity created by BOSE and codes/standards. • Should be enforced by the Commissioner, rather than creating an individual right of action. • The duty should be advanced concurrently with a multi-Commissioner model of governance to facilitate better collective decision-making in an increasingly complex landscape.	s47C
Project ROCKIT 2:30pm 20 May 2026	Lucy Thomas OAM <i>CEO & Co-Founder</i> Project ROCKIT is a charity which runs workshops for school students that teach strategies for responding to challenging bullying. Describes itself as Australia's youth-driven movement against bullying, hate and prejudice. MO/Dept Attendees: Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)	• Have raised concerns about harms that exist for young people aged 18-25 and the ability for the duty to deal with harms in this age group. • Support model that captures all services to avoid unforeseen gaps. • Support ongoing engagement with youth through duty of care development, including children under 16.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Thursday 21 May 2026			
Apple 10:00am 21 May 2026	s47F MO/Dept attendees: Summer Brady, Andrew Hyles, s22(1)(a)(ii)	s47G(1)(b)	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
Snap 10:30am 21 May 2026	s47F [REDACTED] [REDACTED] [REDACTED] MO/Dept Attendees: Summer Brady, Andrew Hyles, s22(1)(a)(ii) [REDACTED]	- Concerned by a duty of care framework targeted at the 8 most used platforms in Australia. Consider how the obligations, including any tiering of obligations, will work in practice. - Support using duty of care as an opportunity to streamline the Act and remove duplication. Consider replacing existing schemes (BOSE and codes) where possible. - Have suggested conducting a mapping exercise to inform transitional arrangements and properly consider the unintended consequences of introducing a duty of care on the existing framework. - Consider UK OSA a solid foundation for a duty of care.	s47C [REDACTED]
s47F 11:00am	s47F [REDACTED] [REDACTED]	Very supportive of introducing a duty of care that is broad, comprehensive and moves beyond a focus on content harms. An	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
21 May 2026	s47F [REDACTED] MO/Dept Attendees: Summer Brady, Andrew Hyles, s22(1) [REDACTED] (a)(ii)	overarching duty of care is future proof, will keep pace and hold platforms accountable. • Key to overarching duty is the guidance from regulators. • Ensure the framework captures AI services. • Should allow for use of sock puppet accounts and public interest scraping by researchers. • Supportive of EU framework – notes that the DSA is working and showing a higher rate of change than the UK OSA. UK OSA is too content focused. • Supportive of higher penalties while recognising that \$50/\$100 million penalties will not impact large companies. • Reforms to OSA should be considered alongside other reforms including relating to privacy and AI.	s47C [REDACTED]
Meta 11:30am 21 May 2026	s47F [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	• Previously raised concerns about how duty of care will work alongside SMMA and other existing elements of the Act, including BOSE and Codes. • Preference for prescriptive UK model that allows regulation to be risk-based and	[REDACTED]

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	s47F MO/Dept attendees: Summer Brady, Andrew Hyles, s22(1)(a)(ii)	proportionate to harms – a broad based duty might create challenges in understanding obligations. • Raised concerns about the complexity of the OSA and about how transitional arrangements will work to reduce complexity.	s47C
ANZSA 2:30pm 21 May 2026	Paul Muller <i>Chief Executive Officer</i> Andrew Fischer <i>Senior Director</i> ANZSA represents the film and television content and distribution industry in Australia and New Zealand including direct-to-consumer online-curated-content / video-on-demand ("OCC" / "VOD") services. Members include Walt Disney Studios Motion Pictures Australia, Fetch TV, Netflix Inc; Motion	• Seeking an exemption from being subject to the Online Safety Act and the duty of care. • Support decoupling the OSA from the National Classification Scheme or to exempt SVOD services from being regulated by the OSA. • Advocate for BVOD and SVOD services to be treated the same and afforded the same 'level playing field'. • Support a risk-based approach and low regulatory impost where the service does not provide for user generated content and already subject to the classification scheme.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	Picture Association, Paramount Pictures Australia, Sony Pictures Releasing International Corporation, Village Roadshow Limited and Warner Bros. Pictures International, a division of Warner Bros. Discovery Inc.		s47C
ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) 3:00pm 21 May 2026	Nicholas Carah <i>Director of Centre for Digital Cultures and Societies, University of Queensland</i> Prof Christine Parker <i>University of Melbourne</i> Prof Jeannie Paterson <i>Co-director of the Centre for AI and Digital Ethics at the University of Melbourne</i> Prof Jean Burgess <i>Digital Media Research Centre, QUT</i> <i>*All attendees are ADM+S investigators</i> ADM+S brings together universities, industry,	• Support introduction of overarching, risk-based and systems-based duty of care that responds to online safety risks, respects the rights of Australians, and supports long-term public value in the digital environment. • At a minimum Australia should adopt a risk-based approach (e.g. UK OSA, EU DSA), with a preference for the EU model. • Suggest that Australia go further and adopt an outcomes-based duty (e.g. UK consumer duty in the financial services sector) that specifies positive outcomes that regulated entities must promote in addition to their obligations to identify and reduce risks. A regulated entity must design its systems and continuously monitor its business to seek to ensure specified outcomes are being promoted.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	government and the community to support the development of responsible, ethical and inclusive automated decision-making. MO/Dept attendees: Summer Brady, Sarah Vandenbroek, s22(1)(a)(ii)	- E.g. The overarching obligation could be: <i>Platforms must deliver a safe, inclusive and healthy digital environment.</i> - Existing transparency measures focused on aggregated data are insufficient. Platforms should proactively explain risk management practices and the regulator should have the power to request more information about platforms' risk management practices. - Need legal and technical infrastructure to enable users, regulators and civil society to meaningfully monitor and observe platform behaviour (calling for a dedicated national platform observatory).	s47C
Roblox 3:30pm 21 May 2026	s47F [REDACTED] [REDACTED]	s47G(1)(b)	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
Teach Us Consent 4:30pm 21 May 2026	Chanel Contos <i>Founder & Executive Director</i> Teach Us Consent's 'Fix our Feeds' campaign advocates mandating social media platforms to offer an option to 'opt-in' to social media algorithms, giving users the autonomy to turn algorithms on and off. This intervention may help prevent gender-based violence and radicalised misogyny, and prevent exposure to disordered eating, self-harm and suicide material; racism; homophobia; mis and disinformation; and other harmful content. MO/Dept attendees:	<i>Duty of care</i> - Recognise the need for structural intervention to address existing 'whack a mole' issue in OSA and broadly support introduction of a duty of care. - Supported broadening the scope of the duty beyond a focus on children and illegal content/activity. Particularly concerned with how the duty will address extreme misogyny and gender-based violence. <i>Algorithms</i> - Point to European Union as a stepping stone (have regulated algorithms through 'opt-out' model) but would prefer an 'opt-in' model in Australia.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	Summer Brady, Sarah Vandenbroek, Andrew Hyles, s22(1)(a)(ii)		s47C
Friday 22 May 2026			
Leon Zwier (Arnold Bloch Leibler) <i>(Dept. only)</i> 12:00pm 22 May 2026	Leon Zwier <i>Partner, Arnold Bloch Leibler</i> Mr Zwier is a litigation and corporate recovery services lawyer. Mr Zwier is currently representing several Jewish organisations in the Royal	No known positions on duty of care.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	Commission on Antisemitism and Social Cohesion.		s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Monday 25 May 2026			
Tech Council of Australia (Dept. only) 10:30am 25 May 2026	s47F [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Dept attendees: Andrew Hyles, s22(1)(a)(ii) [REDACTED]	- Not opposed to a duty of care as industry view it as an opportunity to reduce regulatory complexity. - Support simplification of regulation and raised concerns of regulatory duplication, noting difficulties in compliance when sections of industry are regulated under multiple regimes. - Suggested through the Review that obligations under the OSA be risk-based, proportionate and targeted to the harms that they seek to address. - Note the concept of content/activity harmful to children is broad, and that industry seek clarity in the kinds of harms captured and to what degree.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Australia Council of State School Organisations (Dept. only) 2:00pm 25 May 2026	Dianne Giblin <i>CEO</i> Peter Garrigan <i>Interim Board Chair</i>	• Support a broad-based duty of care to children with additional obligations, including new reporting notices, and audit and record-keeping requirements. • Suggest eSafety need to be able to quantify and qualify how services are complying with their obligations under the duty. • Recognise the need to avoid any gap in protections during the transition, including by maintaining takedown and complaints pathways. • Suggest the rollout of new obligations should be staged and well communicated with families and educators, including through plain-language resources for parents, practical guidance for schools and materials suited to children and young people.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Australian Telecommunications Alliance (Dept. only) 4:00pm 25 May 2026	Christiane Gillespie-Jones CEO s47F - <i>Vocus</i> s47F - <i>Aussie Broadband</i> s47F - <i>Superloop</i> s47F - <i>TPG</i> s47F - <i>TPG</i> s47F - s47F - s47F - <i>AARnet</i> s47F - <i>Verizon</i> s47F s47F - <i>Telstra</i> s47F - <i>Optus</i> s47F s47F	- Supportive of the objectives of DoC but concerned about complexity and compliance challenges for its members – particularly if the DoC is “layered onto” the existing OSA framework and operates concurrently with it. - Queried what the “gap” is that the DoC is seeking to fill, given the existing coverage of the OSA and its instruments. - Supportive of a more risk-based approach which accounts for the technical capabilities and legal constraints which their carriage service providers (CSP) members operate under. - Supportive of threshold criteria for a service being within scope of the Duty: - Significant risk of harm from content through the service - Visibility and control over the content and its distribution - No legal constraints from obtaining visibility or exercising control - Consider many services they represent, such as SMS/MMS services, email services (where provided by CSPs), internet carriage service providers/ISPs (ISP) and business/enterprise services ought to be exempt. Compliance with authorised blocking requests ought to satisfy ISP’s fulfillment of the Duty.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Tuesday 26 May 2026			
Microsoft 9:30am 26 May 2026	s47F Summer Brady s22(1)(a)(ii)	- Support a duty of care that is principles-based, based on systems and processes and clearly defines harms. - Opportunity to simplify and streamline the OSA and align with emerging international best practice. - Obligations within the existing framework (and across Government) are overlapping and create challenges for industry to prioritise action and understand what compliance requires.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Butterfly Foundation (Dept. only) 12:00pm 26 May 2026	Jim Hungerford <i>Chief Executive Officer</i> Melissa Wilton <i>Head of Communications & Engagement</i> Departmental attendees Andrew Hyles s22(1)(a)(ii) [REDACTED]	- Support the shift to a systems-based, preventative model of a duty of care, and suggest the prevention of foreseeable harms is a significant and positive development for those vulnerable to eating disorders and body image concerns. - Retain “disordered eating” as an explicitly named harm in the final duty of care legislation, with framing that extends beyond “instruction or promotion” to cover algorithmic amplification. - Suggest the Government address disordered eating content in the duty of care codes as a priority and consult Butterfly on the development of duty of care codes, particularly those addressing mental and physical wellbeing. - Suggest including eating disorder and mental health expertise in the new Online Safety Commission’s membership or advisory structures. - The duty of care should explicitly encompass AI chatbots and generative AI tools that	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
		engage with users on food, weight and body image.	s47C
Thursday 28 May 2026			
Reddit (Dept. only) 9.00am 28 May 2026	Serena Wong <i>Head of Public Policy, Australia and New Zealand</i> Jessica Ashooh <i>VP of Policy</i> Reddit is an American social media platform which operates as a collection of forums with user to user interaction. Reddit is subject to the SMMA, and has filed a High Court challenge alleging that Australia's social media restrictions are being applied to the company inaccurately. Departmental attendees: Andrew Hyles, s22(1)(a)(ii)	- Support regulatory alignment with international jurisdictions, particularly the UKOSA, and note this would improve compliance ability for small to medium services. - Criticised the OSA as 'too prescriptive' and suggested moving away from defined categories of services, like the UK model.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
auDA (Dept. only) 2:00pm 28 May 2026	s47F auDA (.au Domain Administration) the policy authority and industry self-regulatory body for the .au domain.	• Question whether they should be subject to the Duty – although their service may be considered a DIS, and therefore captured by the OSA, they are not a focus for eSafety’s regulatory efforts. • Support proportionate and risk-based regulation, which appropriately reflects the technical and infrastructural role of their service vis-à-vis content services. • Argue that any requirements for action by registries like auDA ought to be a last resort for addressing online content harms.	
Friday 29 May 2026			
SmackTalk (Dept. only) 2:00pm 29 May 2026	Wayne Holdsworth Founder Kim Burley Chief Executive Officer Dept attendees: Andrew Hyles, Sarah Vandenbroek, Michelle Gannon, s22(1)(a)(ii)	• Supports proposed scope including focus on protection of children up to 18. • Supports broad Duty, but with clear and measurable compliance obligations.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
International Justice Mission (Dept. only) 3:00pm 29 May 2026	Attendees David Braga <i>CEO, IJM Australia</i> John Tanagho <i>Executive Director, IJM's Center to End Online Sexual Exploitation of Children</i> Katia Joo <i>Advocacy Specialist, IJM's Center to End Online Sexual Exploitation of Children</i> Laura Cugley	- Policy paper outlines IJM's proposed duty of care model, including: - proportionate, risk-based obligations with universal core duties for tech companies across every section of the tech industry. - device manufacturers and operating system services should be required to utilise AI-powered CSEA detection technology tools via devices' operating systems. - obligations across three tiers, with the strongest applying to services reaching over 10% of Australians or with very high-risk features (age-	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	<i>Advocacy Research Support, IJM Australia</i> Briony Camp <i>Policy & Campaigns Lead, IJM Australia</i> Departmental: Andrew Hyles, s22(1)(a)(ii)	restricted content, financial transactions). ○ any service with a risk of facilitating CSEA image and video production, distribution, or consumption should be subject to full duty of care obligations regardless of size or reach. ○ language of “best efforts” preferred to “reasonable steps”. ● Noted that children and adults may be affected by the use or misuse of a service even if they are not users of the service.	s47C
Tuesday 2 June 2026			
Match Group (Dept. only) 9:00am	David Quilty <i>Managing Director, National Advisory</i> Casey Burton	● Concerned about transitional arrangements, particularly regarding the voluntary online dating code (VODC). Would like compliance with the VODC to be considered in setting	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
2 June 2026	<i>Associate General Counsel, Match</i> Hala Sawalha <i>Director, Global Trust and Safety Regulatory Compliance</i> Match Group is the American parent company for several major online dating apps, including Tinder, Hinge, OkCupid, and Plenty of Fish. National Advisory is an Australian based Government relations firm, and represents Match Group. Dept attendees: Andrew Hyles, Michelle Gannon, s22(1)(a) (ii)	obligations under the Duty (<i>note: VODC is not made under OSA or enforced by eSafety</i>). • Support focus on illegal content and activity. • Support aligning with other jurisdictions. • Support compliance based on due diligence rather than perfect prevention, inclusion of safe harbours and guidance and assurance for services that they are complying.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Digital Defence Australia (Dept. only) 9:30am 2 June 2026	s47F Digital Defence Australia is a non-profit organisation which campaigns focus on improving online safety policies and strengthening the regulatory environment to prevent Australians from experiencing digital harms. Dept attendees: Andrew Hyles, s22(1)(a)(ii)	s47G(1)(b)	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
International Centre for Missing and Exploited Children (Dept. only) 12:30pm 2 June 2026	Colm Gannon <i>CEO</i> Mikaela Jago <i>Acting Head of Government Affairs and Law Enforcement Outreach</i> Cherise Holley <i>Coordinator, Government Affairs & Public Policy</i> The International Centre for Missing and Exploited Children operates globally and works to	• Supports a duty of care as a means of establishing safety obligations across all platforms, prioritising child safety. • Concerned that smaller/less obvious platforms may fall out of scope, especially those which can be abused by harmful actors, e.g. Uber being used by offenders of CSEA. • The best interests of the child must be prioritised.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	prevent the sexual abuse and exploitation of children. Departmental attendees: Andrew Hyles, s22(1)(a)(ii)		s47C
Amazon 3:00pm 2 June 2026	s47F MO/Departmental attendees Summer Brady Andrew Hyles s22(1)(a)(ii)	s47G(1)(b)	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
Bumble (Dept. only) 5:00pm 2 June 2026	s47F Departmental attendees: Andrew Hyles, s22(1)(a)(ii)	s47G(1)(b)	s47G(1)(b) and s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
Wednesday 3 June 2026			
OpenAI 9:00am 3 June 2026		No known positions on Duty of Care.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Tiktok 3:30pm 3 June 2026	s47F [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] MO/Departmental attendees: Summer Brady, Andrew Hyles	• Support international alignment to minimise regulatory complexity. • Support working within existing regulatory framework to improve online safety (through objects of the Act and eSafety Commissioner's functions). • Support more regulatory certainty and guidance. • Question whether DDOC will bring significant online safety improvements over the BOSE or Codes. • OSA definitions for regulated entities considered rigid and not fit for purpose. • Critical of SMMA consultation.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Google 4:00pm 3 June 2026	s47F 	- Concerned about compounding reporting requirements beyond what exists under BOSE and codes. - Preference for UK OSA that is prescriptive and flexible. Appreciate the safe harbours and specificity of codes.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
	s47F	- Flexibility comes from 'comply or explain' model, which accepts alternative approaches if they address harms adequately. - An overarching duty doesn't provide practical benefits to users or providers. Individual duties do not matter so long as they are outcomes focused, proportionate and provide the regulator sufficient flexibility. Concerned about unlimited ability to make codes. - Avoid duplicative and overlapping regimes. - Risk assessments should be based on user safety and consider the size and risk profile of a platform. Any categorisation of platforms should consider size/reach, risk profile and functionality (noting functionality does not always give rise to risk).	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
Thursday 4 June 2026			
X Corp (Dept. only) 9:00am 4 June 2026	s47F Attendees: s47F Sarah Vandenbroek, Andrew Hyles, Michelle Gannon, s22(1)(a)(ii)	s47G(1)(b)	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
Discord (Dept. only) 12:00pm 4 June 2026	Ishtar Vij <i>AU Public Policy</i> Department attendees: Andrew Hyles Michelle Gannon s22(1)(a)(ii)	- Concerned that harms discussed in policy debate primarily relate to bigger platforms and don't consider smaller services. - Consideration should be given to the function and features of platforms, rather than the size. - Support transparency for development of rules / codes as associated with the BOSE process. - Support inclusion of remediation opportunities, through a more collaborative relationship with the regulator - Ofcom as an example of a constructive relationship. - Support information sharing between the regulator and industry on harms and mitigation actions – tailored to platforms. - Concerned about the transitional arrangements. Support adapting the codes and standards into the duty.	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
Yahoo (Dept. only) 12:30pm 4 June 2026	Raani Costelloe <i>General Counsel – AU & NZ</i>	- Concerned about existing definitions of service categories in the OSA and their relation to code-making. Prefer a risk-based and functional approach to industry segmentation. - Want obligations to be risk-based, to minimise impact on smaller platforms whose features pose lower risk. - Would like international alignment of obligations as far as possible. - Want to avoid intensive compliance regimes, such as onerous reporting requirements as they consider themselves smaller and lower risk.	s47C
Delia Rickard 2:30pm 4 June 2026	Delia Rickard <i>Independent Reviewer of the Online Safety Act 2021</i> Kathleen Reen	s47G(1)(b)	s47G(1)(b)

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
		s47G(1)(b)	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47G(1)(b) and s47C
Friday 5 June 2026			
Special Envoy to Combat Islamophobia (Dept. only) 9:30am 5 June 2026	Aftab Malik <i>Special Envoy to Combat Islamophobia</i>	- The Special Envoy's Report recommends the Government act on the OSA review's recommendations regarding online hate*. Concerning the Duty, this would entail including online hate as a category of harm within scope. <i>*Relevant recommendations are:</i> <i>Recommendation 5 – recommends harm categories which include “attacks based on ... protected characteristics” including race, ethnicity and religion</i> <i>Recommendation 21 – recommends the Act include a definition of online hate material</i>	s47C

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
		<i>Recommendation 22 – recommends considering the effect of online hate material in the threshold for adult cyber abuse.</i>	s47C
UNICEF (Dept. only) 11:00am 5 June 2026	John Livingstone <i>Head of Policy and Advocacy</i>	- Support a Duty of Care, covering systems and processes, with comprehensive child risk assessments, mitigation and transparency obligations. - Want the Duty to cover commercial and contract risks to children. - Want to ensure scope will include new and emerging technologies. - Support robust transparency measures, including public reporting, independent audits, ad archives/repositories and researcher access. - Advocate meaningful consultation with children and young people in developing reforms.	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
			s47C
LEGO	Michael McNeill	LEGO may be concerned about the potential regulatory impost of the Duty on services	

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Meeting information	Stakeholder attendance	Known position on Digital Duty of Care	Key takeaways (meeting notes)
(Dept. only) 3:00pm 5 June 2026	<i>Managing Director,</i> <i>Bower Group Asia</i> The LEGO Group run LEGO Play, an online community oriented to children and their LEGO products. s47G(1)(b)	such as theirs, which are targeted at children s47G(1)(b) • They may highlight features and measures already in place on their service to ensure child safety, privacy, and rights – and may wish to understand what additional obligations a Duty would entail.	s47C

OFFICIAL: Sensitive



Outlook

RE: Issues Paper Release - Digital Duty of Care 26/05/2026 [SEC=OFFICIAL]

From Leon Zwier <LZwier@abl.com.au>

Date Fri 29/05/2026 13:01

To s22(1)(a)(ii) @communications.gov.au>

Cc Nicole Flint <NFlint@abl.com.au>

 1 attachment (19 KB)

Briefing Note re Private Rights of Action.docx;

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Dear Andrew,

Thank you for making the time to meet with me last week.

I attach as a courtesy a copy of a short briefing note in relation to the private right of action which I discussed with you.

I also believe that director obligations to ensure compliance is important, and civil penalties for breaches of duty.

Best regards
Leon

Leon Zwier | Partner

Arnold Bloch Leibler
Level 21, 333 Collins Street, Melbourne Victoria 3000
E: LZwier@abl.com.au | T: +61 3 9229 9607 | M: s47F | [Vcard](#)

Wurundjeri Country



From: s22(1)(a)(ii)@communications.gov.au>
Sent: Tuesday, 26 May 2026 12:48 PM
Subject: Issues Paper Release - Digital Duty of Care 26/05/2026 [SEC=OFFICIAL]

OFFICIAL

Hi there,

Thank you for your engagement on the Digital Duty of Care during targeted stakeholder consultations.

The issues paper has now been published on the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts website.

You can view the issues paper here - [Publications | Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts](#)

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

We would like to thank you for your continued support as we progress these reforms.

Thank you,
Andrew

Andrew Hyles

Assistant Secretary • Digital Platforms, International and Policy • Online Safety and Classification

Andrew.Hyles@communications.gov.au

P s22(1)(a)(ii) • M s22(1)(a)(ii)

OFFICIAL

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

----- Disclaimer -----

This email and any attachments are confidential and may contain privileged information. If you are not the intended recipient you must not disclose, print, copy or use this email or any attachments. If you have received this message in error, please notify the sender immediately and delete it from your system.

Please be aware of the increase in cybercrime and fraud. If you receive an email purporting to be from someone at ABL which seeks to direct a payment to bank details which differ from those which we have already given you (in our engagement letter and on our invoices) it is unlikely to be genuine. Please do not reply to the email or act on any information contained in it but contact us immediately. It is possible for emails to be intercepted in transit and email details changed. When receiving an email from ABL containing bank account details, please phone us (on the number on our website) to verify the account details before transferring the funds.

Arnold Bloch Leibler does not accept liability for any loss or damage (whether direct, indirect, consequential or economic) however caused, and whether by negligence or otherwise, which may result directly or indirectly from this email or any attachments (including as a result of your failure to scan this email for viruses or as a result of interference or unauthorised access during communication). In any event, our liability is limited to the cost of re-supplying this communication.

DisclaimerID:AUUYYGH000012

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Briefing Note

Purpose

The purpose of this briefing note is to set out the rationale for a right of private action to enforce compliance with the proposed duty of care that Government is considering imposing on Platforms pursuant to proposed amendments to the Online Safety Act (OSA), and to provide a mechanism by which affected persons may seek timely relief in relation to posts that evidence non-compliance with that duty or other applicable Australian laws.

Background

The Platforms are disproportionately powerful counterparties in any legal processes that may be commenced against them. The Platforms have immense resources, operate across jurisdictions, can sustain years of litigation without any material impact on profitability, deploy elite counsel and lawyers, and strategically use technicality, delay and procedural complexity. See *eSafety Commissioner v X Corp* [2026] FCA 629 (judgment 21 May 2026).

The Platforms litigate like Big Tobacco.

Recent enforcement experience demonstrates the significant resource asymmetry between affected persons, Australian regulators and global digital Platforms. Where affected persons are required to litigate against Platforms, the litigation economics usually favour the Platform. A private right of action should therefore be designed deliberately to alter those economics and to ensure that Platforms bear the evidentiary and financial consequences of failing to act when notified of offending posts.

Regulation by Private Litigation - Uncontroversial

Corporate conduct has been better managed by the creation of private rights of action under laws initially intended to establish regulatory bodies. The ASIC Act established ASIC and a regime for corporate regulation. The ACCC was established under the now repealed Trade Practices Act and the TPA granted the ACCC broad investigatory powers to ensure compliance. When those Acts also created private rights of action, corporations that failed to comply with their obligations under those Acts were and are now at risk of class litigation and exposed to damages in addition to regulatory proceedings. The litigation risk helps ensure compliance with the laws.

The same regulatory logic applies to Platforms. Public enforcement by the eSafety Commissioner remains essential, but public enforcement alone cannot be expected to address the scale, speed and volume of harmful online material. Private litigation can supplement public enforcement by enabling affected persons to compel compliance and by changing the incentives of Platforms when they receive notice of offending posts.

Right of Private Action

The Government may wish to amend the OSA to create rights of private action with the following attributes:

- 1. Prior notice to the Platform.** Before commencing proceedings, the Applicant must first give written notice to the Platform seeking removal of, or disabling of access to, the specified posts. The notice should identify the posts with sufficient particularity, including by URL, screenshot, account name, date, time or other available identifying information; state why the posts are alleged to evidence non-compliance with the Platform's duty of care or other Australian laws; identify the relief sought; and require the Platform to remove the posts, disable access to them, restrict their dissemination or otherwise take appropriate remedial action within a prescribed period.

2. **Time for response.** The prescribed period for response should be short, given the speed at which online harm can be amplified. A period of 48 hours may be appropriate in ordinary cases, with provision for a shorter period in urgent cases and for the Court to abridge or dispense with notice where giving notice would defeat the purpose of the proceeding, expose a person to serious or imminent harm, or otherwise be contrary to the interests of justice.
3. **Proceedings after failure to act.** The Applicant may commence proceedings if the Platform fails to remove the posts, fails to disable access to them, fails to respond within the prescribed period, or gives a response that does not adequately address the alleged non-compliance. The prior notice requirement ensures procedural fairness while also giving the Platform an opportunity to avoid litigation by taking prompt remedial action.
4. **Costs.** The jurisdiction to pursue a private action should generally be a no-costs jurisdiction similarly to the Fair Work Act. Unreasonable conduct by an Applicant or Respondent should allow the Court to make adverse costs orders. However, once the Court determines that the specified posts are prima facie evidence of non-compliance with the Platform's duty of care or other Australian laws, the Court may order the Platform to pay all of the Applicant's costs of the legal proceedings, including any appeals. This costs power is central to changing the economics of proceedings against Platforms.
5. **Relief.** The relief should be declaratory relief in relation to the Platform's non-compliance with its duty of care or breaches by the Platform of other Australian laws, and injunctive relief in relation to particular posts. The relief should not include damages. The objective is compliance, removal or restriction of offending posts, and deterrence of future non-compliance, not compensation.
6. **No additional claims against authors.** The private right of action will not establish additional or new claims against the people making the posts. The proceeding is directed to the Platform's compliance with its statutory obligations and other Australian laws, not to creating a new cause of action against the authors of the posts.
7. **Preliminary determination.** The Applicant will be required at the outset to apply to the Federal Court for a preliminary determination that the prior notice requirement has been satisfied or should be dispensed with, and that the subject posts are prima facie evidence that the Platform has not complied with its duty of care or other Australian laws. Courts often apply the same or similar tests in relation to parties seeking injunctive relief. The preliminary determination may be heard by a Judge or, where appropriate, managed or determined by a Registrar, subject to any review or referral to a Judge required by the Federal Court's ordinary processes.
8. **Paper-based procedure.** The initial application will be made on the papers only. The Applicant will make written submissions limited to 12 pages. The Respondent will make reply submissions limited to 10 pages. The same limitations are imposed on parties in relation to a Special Leave application in the High Court of Australia. This will ensure that the initial application can be dealt with speedily, cost effectively and efficiently.
9. **Reversal of the legal burden of proof.** The Applicant bears the initial legal burden of satisfying the Court, at the preliminary stage, that the specified online material, considered together with the notice given to the Platform and the Platform's response or non-response, constitutes prima facie evidence that the Platform has not complied with its statutory duty of care or other applicable Australian laws. Once the Court is so satisfied, the Platform is presumed, for the purposes of the proceeding, not to have complied with the relevant duty or law unless the Platform proves otherwise on the balance of probabilities. The Platform therefore bears the legal burden of establishing that, in relation to the material the subject of the proceeding, it took all reasonable steps required of it, including by reference to its systems, processes, risk assessments, escalation pathways, moderation steps, complaint-handling processes and other mitigation measures. In determining whether the Platform has

discharged that burden, the Court may have regard to the Platform's control over the relevant information, the asymmetry of resources and knowledge between the parties, and the Platform's capacity to produce evidence of compliance. The Court may draw adverse inferences from any failure by the Platform to adduce evidence of matters peculiarly within its knowledge or control.

10. Justification for reverse onus. The reversing of the onus of proof is not novel. The Fair Work Act presumes "adverse action" was taken unless the respondent proves otherwise. In this context, reversal of the legal burden is justified because the Platform controls the systems, records, moderation processes, risk assessments, escalation pathways and technical information necessary to prove compliance. An affected person cannot realistically be expected to prove the absence or inadequacy of systems that are internal to the Platform and unavailable to the Applicant.

Conclusion

This private right of action changes the economics of a legal dispute with Platforms over posts. The notice requirement gives Platforms an opportunity to remove offending posts and avoid litigation. If a Platform does not do so, and the Court determines that the posts are prima facie evidence of non-compliance, then it is appropriate that the Platform bear the legal burden of proving compliance and, where ordered, the Applicant's costs of the legal proceedings including any appeals.

If Platforms are ordered to pay the legal costs of those suing them and the onus of proof is reversed, then it is in the better financial interests of Platforms to remove offending posts rather than defend the posts and their compliance with their statutory duty. This is the intended incentive structure.

The private right of action would have the practical effect of augmenting the eSafety Commissioner's more limited resources in seeking to better regulate the Platforms.

The Platforms will also remain exposed to a penalty for breach of the duty. This often occurs in corporate regulation too.

The Government will avoid bearing any cost consequences of this private right of action.

The beneficiaries of the private right of action are a broad cohort of Australians.

The right of private action does not create any new claim against the authors of the posts. Any order affecting access to particular posts would be made by a court, after notice to the Platform or dispensation from notice in appropriate cases, and would be directed to the Platform's compliance with its statutory duty of care or other Australian laws.

The legal costs of the process are minimised by making the initial application determined on a combined maximum of 22 pages of submissions without an oral hearing.

The initial application can be heard or managed by a Registrar where appropriate, with any contested substantive issue, final declaration, injunction or significant costs order able to be referred to or reviewed by a Judge in accordance with the Court's ordinary processes.

This initiative should be pursued outside the recommendations of the Royal Commission on Antisemitism and Social Cohesion but should be disclosed to the Commissioner as a complementary reform directed to online hate, platform accountability and social cohesion without creating any additional claim against the authors of posts.

This is not novel or bespoke in terms of regulation, particularly regulation of large, well-resourced corporate entities. However, like Australia's legislation to make 16 the minimum age for use of social media, a private right of action would be an Australian advance on existing regulatory models because it would directly address the power imbalance between affected persons and large digital Platforms.

2 June 2026

Mr Andrew Hyles
Assistant Secretary
Digital Platforms, International and Policy Branch
Online Safety and Classification Division
Department of Infrastructure, Transport, Regional Development, Communications, Sports & the Arts
Email: Andrew.Hyles@communications.gov.au

Dear Andrew

IGEA's response to Digital Duty of Care Issues Paper

Thank you for sharing with the Interactive Games & Entertainment Association's (IGEA) Policy Team a private copy of your Issues Paper on a proposed Digital Duty of Care (DDoC) under the *Online Safety Act 2021* (Cth) (OSA), and meeting with us on 19 May 2026. Since that time, we note that the Department has published this Issues Paper on 26 May.¹ This follows from your roundtable with industry associations on 5 December 2025, and our subsequent private response to your Issues Paper.

Following our meeting, we would like to share our additional preliminary comments.

Recognising that the Department is still developing the details of how a DDoC may operate, we strongly encourage ongoing engagement to support thorough consultation. We look forward to contributing further to help ensure strong outcomes and avoid unintended consequences. This is especially important given the concurrent, interrelated reforms underway (e.g. reforms to the National Classification Scheme (NCS) and the Office of the Australian Information Commissioner's (OAIC) development of the Children's Online Privacy (COP) Code), existing regulatory arrangements, and the Minister for Communications' public statements that online gaming platforms would be in scope.

Please note that these are in addition to our comments provided in December 2025, although some issues may be reiterated. Our previous and current comments should be read together as the DDoC framework continues to be developed.

Below is a summary of our issues and comments:

Issues	IGEA's comments
1. Consultation process	As the Department continues to develop the DDoC, appropriate opportunities should be provided to impacted stakeholders, including the ability to make written submissions and sufficient timeframes for meaningful engagement. Prior to consultation on a Bill, this should

¹ See: <https://www.infrastructure.gov.au/departments/media/publications/digital-duty-care-australia-developing-duty-care-framework-online-services-used-australians>

Issues	IGEA's comments
	include, at a minimum: (1) draft policy options addressing clearly identified issues, released ahead of any Exposure Draft Bill; and (2) an Exposure Draft Bill accompanied by Explanatory Materials.
2. Resolving the overlap between the NCS and OSA	• <u>Online games classified under NCS</u>: The Australian Government's policy recognises online games are currently regulated under the NCS, which provides clear guidelines on age-appropriateness and content, and to regulate online games under new law would create unnecessary regulatory overlap.² In line with that policy, where a service's sole or significant purpose is online games and are classified under the NCS, they should be automatically excluded from the scope of the DDoC. In other words, such online games should not be within the scope of the DDoC by default. • <u>Online gaming services with communications functionality, limited communications functionality, and no communications functionality</u>: Specific exclusion of online games should be aligned with the broader regulatory schemes of the OSA, mirroring the test applied in the Unlawful Material (Phase 1) Codes and Standards, and Age-Restricted Material (Phase 2) Codes to identify online gaming services with communications functionality, limited communications functionality, and no communications functionality. Under the OSA (including industry codes and standards), online gaming services are already required to implement important compliance measures to minimise the risk of illegal content being shared or generated, providing an additional layer of protection for children and younger users. In any event, there are clear categories of online games that are recognised under the OSA framework as inherently low risk (e.g. games with limited or no communications functionality) - these should not be subject to any DDoC consideration by default. • <u>Delineation between NCS and OSA</u>: ◦ More broadly, we reiterate the importance of implementing the recommendations from the Steven's Review and subsequent Statutory Review of the OSA, to clearly delineate the roles of the OSA and the NCS.³ ◦ The OSA should be expressly limited to illegal and unclassifiable online content, as well as its role in addressing currently defined categories of seriously harmful online conduct (e.g. cyber bullying, cyber abuse, image-based abuse, material that depicts abhorrent violent conduct). ◦ In contrast, the NCS should regulate classified and classifiable content, providing consumers (including parents and guardians) with information to make informed choices. This includes supporting age-based restrictions for higher classification categories (such as R 18+).

² The Hon Michelle Rowland MP, Former Minister for Communications, Online Safety Amendment (Social Media Minimum Age) Bill 2024 - Second reading speech, <https://minister.infrastructure.gov.au/rowland/speech/online-safety-amendment-social-media-minimum-age-bill-2024-second-reading-speech>

³ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Review of Australian classification regulation' (Report, May 2020) ('Stevens Review'), pp. 39, 120, <https://www.infrastructure.gov.au/sites/default/files/documents/review-of-australian-classification-regulation--may2020.pdf>; Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Statutory Review of the Online Safety Act 2021' (Report, October 2024), p. 16, <https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>

Issues	IGEA's comments
	○ These distinctions between the OSA and NCS are particularly relevant to video games, just as they are for film. ● <u>NCS-first approach for regulating online games</u>: Further, where gaps are identified in how online games are regulated, these should be addressed within the NCS in the first instance, rather than through the OSA or other regulatory frameworks (including any future DDoC). ● <u>Complaints handling</u>: Complaints handling illustrates a further risk of duplication and regulatory conflict between the DDoC and NCS. Including classified games within the DDoC framework would be inappropriate, given the NCS already provides a formal mechanism for contesting classification decisions. It risks creating inconsistent regulatory outcomes, where content appropriately classified and found not to be prohibited material under the NCS is simultaneously characterised and treated as 'harmful' under the DDoC, in the absence of any coordination mechanism between the regimes. This highlights the importance of clearly delineating their respective roles.
3. Scope of harms	● <u>Overly broad scope</u>: ○ The reference to 'harms' as the basis for the DDoC (while intending to cover 'serious harms' or 'seriously harmful' content and activity) is extremely broad. While we agree that illegal content and conduct should be addressed through appropriate legal frameworks, there is a risk this approach creates overlap or duplication with existing laws (and associated enforcement bodies) outside the OSA. We consider that the OSA should retain its scope over illegal and unclassifiable content and conduct, insofar that it is aligned within its current scope e.g. cyber bullying, cyber abuse, image-based abuse, material that depicts abhorrent violent conduct. ○ Even more contentious, we are concerned that the broad use of terms such as 'harms' or 'harmful' could inadvertently capture classified or classifiable content that is not illegal. These risk expanding the scope of the DDoC beyond its intended remit and creating uncertainty for regulated entities. ● <u>Criteria for harms</u>: A clear set of criteria should be developed to ensure that the scope of harms is properly defined and limited to psychosocial and physical harms, avoiding overlap or duplication with existing regulatory regimes, while meaningfully addressing gaps in the current framework. ● <u>Conflicts with NCS</u>: Without clear criteria to define the scope of harms, there is a further risk that the DDoC conflicts with the NCS (as discussed above). The classification framework accommodates content containing mild classifiable elements (including themes, violence, sex, language, drug use and nudity), even at PG level. It would be inappropriate for the DDoC to automatically deem classified content containing such elements as 'harmful' content. ● <u>Design features</u>: Whether a particular design feature is harmful should not be determined in isolation, but assessed in context through a proper risk assessment (see discussion below on proportionality and risk-based approach). A feature that appears harmless in one context may prove harmful in another, making risk assessment the appropriate mechanism for determining harm, rather than prescriptive definitions alone. Where a feature is deemed harmful, the risk may be reduced or eliminated through appropriate mitigating measures.

Issues	IGEA's comments
	• <u>Algorithms</u>: We are concerned that the Issues Paper may imply that algorithms are inherently harmful. This overgeneralises a diverse set of functionalities with markedly different risk profiles and potential to cause harm. For example, game recommendation tools that suggest similar titles based on user activity are not inherently harmful. As with design features, whether an algorithm gives rise to harm should be assessed in context through risk assessment, rather than assumed.
4. Compliance and enforcement	• <u>Role of codes</u>: ○ The Government's response to the Statutory OSA Review supported in-principle that eSafety should be empowered to create mandatory rules (in the form of codes) associated with a DDoC.⁴ We support codes to be developed to enable entities to properly meet their obligations. ○ Subordinate legislative instruments (e.g. codes) that give effect to a DDoC should clearly set out the standards or expectations that entities are required to meet to ensure compliance. These should form the basis for demonstrating compliance. We are pleased to hear that these will be disallowable by Parliament - such checks and balances are important for ensuring this policy reflects the expectations of the Australian public. ○ For DDoC codes to function effectively, compliance must carry meaningful consequence. Safe harbour for compliant entities replaces vague expectations with regulatory certainty and consistency, giving entities a defined standard to meet and a clear incentive to meet it (as opposed to managing legal uncertainty), in the public interest. Such a concept is not unusual in other contexts such as in Work Health & Safety.⁵ • <u>Operation of codes</u>: Should eSafety be responsible for developing codes for a DDoC, proper consultation should be undertaken with directly affected stakeholders including industry. These codes should be developed alongside supporting guidance. Following the registration of the codes and accompanying guidelines, compliance with these codes should occur at least 24 months after the date of registration. • <u>Graduated approach to compliance and enforcement</u>: We support a graduated approach to enforcement. Further considerations should be given to establishing clearer pathways for resolving disputes before they escalate to judicial or merits review, reducing reliance on costly litigation and allowing resources to be directed towards user protection. • <u>Civil penalties</u>: Civil penalties should be treated as a last resort power. The maximum amount should be limited to \$50m as recommended by the Statutory OSA Review and supported in the Government's response to the review.⁶
5. Assessment of audits by researchers	• <u>eSafety handling of confidential information</u>: We support eSafety adhering to appropriate safeguards in handling confidential information provided as part of an entities' reporting obligations.

⁴ Government Response to the Independent Review of the Online Safety Act 2021 (April 2026), p. 15, <https://www.infrastructure.gov.au/sites/default/files/documents/govt-response-to-the-independent-review-online-safety-act-2021.pdf>

⁵ See: <https://www.safeworkaustralia.gov.au/law-and-regulation/codes-practice>

⁶ Government Response to the Independent Review of the Online Safety Act 2021 (April 2026), p. 11

Issues	IGEA's comments
	• <u>Audits</u>: ○ We note that eSafety already has broad information-gathering and investigation powers, and the rationale for conferring additional audit powers has not been clearly justified. Regulatory powers should be proportionate to demonstrated need, where existing powers are sufficient. This is particularly important for smaller entities who lack resources and would therefore be disproportionately impacted. ○ Setting that issue aside for the moment, if entities are compelled by eSafety to undertake an independent audit (which may be subsequently reviewed by eSafety via a third-party e.g. researcher), providers should not be required to share data to third-parties. There should also be a clear set of guidelines and thresholds established to ensure transparency for both eSafety and providers on what would warrant an independent audit to be required. eSafety should also clearly articulate the purpose of collecting the information and how it will be managed including protecting confidentiality.
6. Small business support	• The video games industry is a broad ecosystem that includes businesses of different sizes and risk profiles that may be captured under a DDoC. Small businesses should receive additional support to uplift practices to meet any DDoC requirements, including reasonable commencement timeframes, reduced frequency of undertaking risk assessments and regulatory reporting, and targeted and practical guidance to assist with complex obligations.
7. Proportionality and risk-based approach	• <u>Risk-based approach</u>: We reiterate that a DDoC should recognise that different digital services have distinct risk profiles. A one-size-fits-all approach risks over-regulation, poorly targeted regulation and unintended consequences. A risk-based approach needs to consider the nature of the service, the likelihood and extent of a serious online safety harm, measures in place to mitigate risks, and the actual online safety risks posed, ensuring regulatory effort is directed to areas of meaningful impact. How a provider discharges their duty should be at their discretion, as long as they can demonstrate how they have protected users on their service. We recommend that any codes are principles based to allow providers this flexibility. • <u>Rebuttable assumption</u>: Where a service is designated as subject to the DDoC, the service provider should have the opportunity to undertake a risk assessment to demonstrate that the service presents a lower level of risk. Obligations should then be calibrated to reflect that assessed risk level, rather than applying a uniform standard to all designated services. • <u>Reach</u>: Consistent with this approach, we would be concerned if a service's risk profile were assumed to be high based solely on its reach. While many popular services have significant reach, this does not necessarily equate to higher risk. For example, a classified online game with no, or limited, communications functionality may be inherently low risk, despite potentially having a large user base. Reach alone should not be determinative of risk - whether a service (or specific features within it) is considered high risk should be established through a holistic risk assessment.
8. Governance and accountability	• We previously stated that stronger transparency and governance requirements should be built into the legislative framework to bolster

Issues	IGEA's comments
	public trust, ensure proportionate regulatory decisions, and address perceptions of unfettered power. • <u>Structural review of eSafety</u>: In considering the latest proposals, there is a risk that the DDoC will provide eSafety with even greater unfettered discretionary regulatory powers. We note that the Government's response to the Statutory OSA Review supports, in principle, a structural review of eSafety. Consistent with this, we reiterate that the introduction of a DDoC should be coupled with structural reform to ensure the regulator is appropriately equipped to implement, administer and enforce the framework in a transparent and appropriate way. Strengthened governance arrangements will be critical to ensuring appropriate checks and balances, robust decision-making, and transparency and accountability in the exercise of regulatory powers. • <u>Good governance in practice</u>: Along similar lines, any legislative and regulatory powers (particularly discretionary powers) proposed to be conferred to the Minister or eSafety (including via Minister-delegated authority) should be subject to appropriate Parliamentary oversight and public scrutiny. These include powers to make binding rules related to designating additional harms, specifying compliance requirements, and specifying exempted services. Proper checks and balances should include: Parliamentary powers to scrutinise all DDoC-related matters; mandatory public consultation for any proposed new DDoC requirements; a clear and specific explanation of the powers available to the Minister and eSafety in connection with the DDoC; and mandatory enforcement reporting to Parliament.
9. Recognise existing online safety requirements and transition arrangements	• <u>Streamlining BOSE</u>: In principle, we support leveraging the DDoC as an opportunity to simplify and streamline the entire OSA regime to create a system that is easy for both platforms and end-users to navigate. This includes repealing the BOSE and instituting a singular and overarching DDoC. We would prefer to avoid a situation where both the DDoC and BOSE are in place for a transition period, as so many layers of obligations are unworkable. The transition from the BOSE to the DDoC should be clean and without overlap. • <u>Reporting requirements</u>: An expected outcome from a more streamlined approach under the DDoC is a single reporting regime (replacing multiple reporting obligations that currently exist across the various legislative instruments under the OSA). Reporting requirements should be proportionate and triggered by a significant event or material change (rather than fixed to a predetermined interval or schedule). Such an approach would eliminate unnecessary regulatory burden and costs. • <u>Grandfathering</u>: We note that the Department's proposed DDoC intends to initially transition from the BOSE, followed by the industry codes and standards over time. For entities that currently meet their obligations under the BOSE, Unlawful Material Codes and Standards, and/or Age-Restricted Material Codes, there should be a grandfathering provision that allows complying entities to continue operating under those obligations. If there are significant changes to the service, there may be consideration to transition to the new obligations; however, clear criteria should be developed to clarify what fairly constitutes significant changes to a service. • <u>Regulatory guidance</u>: To support a more seamless transition for entities transitioning from the current BOSE, and online safety codes and standards, the Department or eSafety should clarify how the DDoC

Issues	IGEA's comments
	obligations are intended to align with, or change from, the current online safety requirements, including by providing guidance on key similarities and differences between the two regimes. This would assist entities that already comply with the current online safety arrangements to understand where existing practices may satisfy DDoC expectations, and where additional measures are required.
10. Concurrent reforms including COP Code	• In addition to the NCS reforms currently underway, we reiterate the importance of the Department having regard to the OAIC's ongoing development of the COP Code. There are potential areas of overlap (including the interaction between privacy-by-default and online safety-by-default obligations) that require careful consideration and coordination with the OSA (including a DDoC).
11. Implementation period	• eSafety should publish targeted and practical guidance to support the implementation of the DDoC, and provide a reasonable implementation period of at least 24 months following the publication of that guidance. This will enable service providers to properly understand and meet their obligations.

We welcome continued engagement on the development of the DDoC and would be pleased to provide further input as the framework progresses.

Should you have any questions, please do not hesitate to contact the IGEA Policy Team at policy@igea.net.

Warmest regards

s47F

4 June 2026

Andrew Hyles

Assistant Secretary – Digital Platforms, International and Policy,
Online Safety and Classification

Department of Infrastructure, Transport, Regional Development,
Communications, Sports and the Arts

Via email only: Andrew.Hyles@communications.gov.au, [s22\(1\)\(a\)\(ii\)@communications.gov.au](mailto:s22(1)(a)(ii)@communications.gov.au)

Dear Andrew,

Feedback on the Issues Paper *A Digital Duty of Care for Australia*

The Australian Telecommunications Associations (ATA) and our CSP members welcome the opportunity to provide feedback on the Issues Paper on a digital duty of care (DDOC). We also appreciated the opportunity to meet with you and your team to discuss the proposals.

Following on from [our submission in response to survey on the DDOC in December 2025](#), the Issues Paper, and our recent discussions with your team, we provide the following high-level feedback:

1. Clarity of Scope and Proportionality:

- We maintain that exemptions from the DDOC for the services that our CSP/ISP members provide would provide the most practical and appropriate approach to a DDOC for such services, given the very limited control over and risk profile of such services.
- Failing such exemptions, we acknowledge that CSPs (including ISPs) would be included under the proposed, board DDOC framework. We emphasise that obligations must be calibrated by both risk and reach (together), and actual control – meaning that lower-risk services (e.g., basic connectivity/infrastructure with minimal content involvement) should face only proportionate, technically feasible duties, consistent with the ‘so far as is reasonably practicable’ standard. Given ISPs’ primary role as connectivity providers (with broad reach but limited content control), we consider these ISP services have comparatively low online content risks.
- For services with minimal content exposure – such as products for enterprise customers, services delivered via reseller/wholesale arrangements, or one-to-one communications (like SMS, MMS, and email) – regulatory expectations should remain limited, reflecting CSPs’ limited ability to monitor or influence user content. Notably, utility communications services such as SMS/MMS and email already have dedicated anti-abuse frameworks (e.g. *Spam Act 2003* requirements and telco anti-scams/cybercrime measures) and do not facilitate the kind of open content sharing seen on social media platforms. The DDOC should explicitly account for these differences and ensure any obligations on such services are minimal and technically feasible, to avoid imposing unrealistic or duplicative requirements on channels where broad content moderation is impractical.



2. Interaction with Existing Online Safety Frameworks:

- We support ensuring the new DDOC complements (and does not duplicate) existing *Online Safety Act 2021* (OSA) complaint schemes, codes, and standards. We note that the Department has verbally indicated that the DDOC is intended to incorporate and/or replace elements of the existing framework over time. Notwithstanding this, greater clarity is required on which components will be incorporated, which will be replaced, and how this transition will operate in practice.
- In this context, we seek clarity on whether the DDOC will incorporate, supersede, or operate alongside the current suite of 17 industry codes and standards (which cover numerous service categories and types of materials), and how a CSP's compliance with existing obligations (e.g. responding to eSafety removal notices, meeting *Basic Online Safety Expectations* (BOSE), and abiding by the industry codes/standards) will be recognised under the DDOC. It is essential to maintain coherence and minimise regulatory complexity, particularly during any transition where elements of the existing regime may be progressively replaced.
- We understand the Department is seeking views on whether the codes and standards should cease or coexist with the DDOC (with deemed compliance). Some ATA members have expressed a clear preference for the continued coexistence of the two frameworks/instruments, whereby compliance with the applicable codes and standards would be deemed sufficient to demonstrate compliance with the DDOC. Other members consider it too early to take a position without greater clarity on the DDOC's scope and how it will operate in practice.

3. Need for Clear and Practical Guidance:

- We emphasise that a broad, principles-based DDOC must be underpinned by clear, authoritative guidance to ensure practical and consistent implementation. We strongly support the Department's plan to develop detailed guidance (and if needed, service-specific rules) during the transition, and we urge the early release of these materials.
- Such guidance should clearly spell out what 'effective systems and processes' entail for different types of services, reflect safety-by-design best practices, and provide concrete examples of risk assessment and mitigation measures. This will enable CSPs – especially those with limited content visibility or control – to confidently align their internal processes and governance with the DDOC's expectations.

4. Transition Timing and Implementation:

- We welcome the proposed 12-month transition period, which is essential for orderly implementation. We recommend that the key compliance guidance and any binding rules be released well before the DDOC's commencement, allowing sufficient time for CSPs' implementation planning, system updates, staff training, and risk assessments.
- If there are delays in finalising guidance or subordinate instruments, we suggest considering flexible timing or phased obligations to ensure CSPs are not forced into non-compliance due to late-breaking requirements.

5. Support for Simplifying the Online Safety Framework:

- We are broadly supportive of a proportionate, flexible DDOC that helps uplift and simplify the online safety framework. We appreciate the collaborative consultation process and the Government's emphasis on minimising regulatory burden and complexity.
- By focusing on clear scope, non-duplication with existing schemes, and robust guidance (including clarity on how the current framework will be incorporated or replaced), the DDOC can be well-calibrated to protect users while providing certainty for industry.

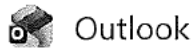


If you have any questions or wish to discuss, please contact Deputy CEO, Christiane Gillespie-Jones (c.gillespiejones@austelco.org.au).

Kind regards,

A handwritten signature in blue ink, appearing to read 'C. Gillespie-Jones', written in a cursive style.

Christiane Gillespie-Jones
Deputy CEO



FW: NOTES: Special Envoy to Combat Islamophobia [SEC=PROTECTED]

From Hyles, Andrew <andrew.hyles@communications.gov.au>

Date Fri 05/06/2026 10:26

To s22(1)(a)(ii)@communications.gov.au> s22(1)(a)(ii)@infrastructure.gov.au>;
s22(1)(a)(ii)@infrastructure.gov.au>

📎 1 attachment (2 MB)

Digital Duty of Care Consultation presentation.pptx;

OFFICIAL

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Hi team – see below Sarah’s notes from our meeting with the Special Envoy to Combat Islamophobia this morning.

Note in particular that we have agreed to set up a 6 weekly meeting with his team to keep them in the loop as this reform develops. I also committed to send him the attached presentation as well as the Issues Paper (so he had it all in one place). s22(1)(a)(ii), understand that s22(1)(a)(ii) has spoken to you about this already.

Thanks

Andrew

Andrew Hyles

Assistant Secretary • Digital Platforms, International and Policy • Online Safety and Classification

Andrew.Hyles@communications.gov.au

p s22(1)(a)(ii) • M s22(1)(a)(ii)

OFFICIAL

From: VANDENBROEK, Sarah <Sarah.Vandenbroek@infrastructure.gov.au>
Sent: Friday, 5 June 2026 10:00 AM
To: Hyles, Andrew <andrew.hyles@communications.gov.au>
Cc: VANDENBROEK, Sarah <Sarah.Vandenbroek@infrastructure.gov.au>
Subject: NOTES: Special Envoy to Combat Islamophobia [SEC=OFFICIAL]

OFFICIAL

Consultation on DDoC with the Special Envoy to Combat Islamophobia
Friday 5 June 2026 – 9:30am

s47C



12 June 2026

Mr Andrew Hyles
Assistant Secretary
Digital Platforms, International and Policy
Department of Infrastructure, Transport, Regional Development,
Communications, Sport and the Arts
By Email: s22(1)(a)(ii) @communications.gov.au

Dear Mr Hyles,

Re: Issues Paper - A Digital Duty of Care for Australia

Thank you again for meeting with us on 29 May 2026 to discuss the proposed Duty of Care as set out in the Department's issues paper. We appreciate the opportunity to contribute to this reform process, and to provide our feedback and recommendations. We found the discussion productive and helpful in clarifying the intention of the proposed duty, as well as the timeline moving forward.

As highlighted during the consultation, it is IJM's position that the issues paper is a step in the right direction, and we support the Department's clear intention to hold service providers accountable for illegal and harmful content on their platforms. IJM is also particularly encouraged to see that device manufacturers and operating system providers will be included within the scope of the duty of care and encourages the Department to ensure that this layer of the tech stack is maintained in the proposed bill. Obligations at the device level should be strengthened as they have significant potential to scale privacy-preserving prevention device-wide, as reflected in the UK Prime Minister's recent demand of Apple and Google.¹

Further to the consultation, we wish to provide a brief summary of our overall feedback regarding key risks and areas for refinement:

Ensure non-users are captured within scope of the duty – IJM is glad to see that the best interests of the child are captured as a key consideration for service providers in discharging the core obligations of the duty,² aligned with Recommendation 8 of the Rickard Review.³ This would strengthen the existing Basic Online Safety Expectation that "that the best interests of the child is a primary consideration in the design and operation of services likely to be used by children".

IJM urges the Department to consider expanding this wording to make it explicit that this includes **both** children as users of the service, and children who are non-users but may nonetheless be impacted by the use of the service by other persons. Similarly, as outlined in the safety by design considerations on page 5, service providers are required to prioritise the best interests of users in the design and operation of their services. IJM strongly suggests that

¹ International Justice Mission Australia, *IJM Welcomes Device-Level Child Safety Announcements, Urges Tech Companies to Go Further* (June 2026). Available from: <https://ijm.org.au/news/childsafetyannouncement>

² "Service providers will also be required to consider the best interests of the child in assessing and mitigating risks arising from the design and operation of their services." - page 7, issues paper.

³ "The best interests of the child should be a primary consideration for online service providers in assessing and mitigating the risks arising from the design and operation of their services, including risks to children who may use the service and risks to children as a result of how the service may be used." Delia Rickard PSM (October 2024) *Report of the Statutory Review of the Online Safety Act* Available from: <https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>

this should likewise be explicitly expanded to include non-users who may be impacted by the design and operation of the service.

In the case of livestreamed child sexual abuse, children experience repeated hands-on sexual abuse at the hands of a trusted adult precisely because that abuse is accessed in live videos online by paying sex offenders in countries like Australia. These child victims are not end-users of the digital platforms through which the abuse occurs but they are harmed by users in Australia who access live child sexual abuse videos while using those platforms from Australia. In fact, digital safeguards that prevent Australian users from accessing live video child sexual abuse would undercut the financial motivation of adults in 'source side' countries like the Philippines to abuse children in this way, thereby preventing the underlying abuse. The Duty of Care framework should result in live online video platforms being "designed" in such a way as to not allow the uninterrupted streaming and accessing of Class 1 "child sexual exploitation material" on the platform.

1. **Include livestreaming and live video as a feature that may increase the risk of harm** – aligned with the approach taken by the EU in its Proposal for a CSA Regulation, IJM recommends that the Department consider including livestreaming—both public and private "live video"—in the list of features that may increase the risk of harm, as outlined on page six of the issues paper. Real-time image and video transmission functionalities should be considered as posing the highest risk of harm, due to the immediate and ephemeral nature of the content, making it particularly difficult for law enforcement to investigate.⁴ Because live online child sexual abuse material currently leaves minimal digital traces for law enforcement, real-time disruption and prevention is essential to address this digital crime.
2. **Strengthen the reasonable steps standard through firm supporting language** – as distilled in IJM's March 2026 Digital Duty of Care Policy Paper, there is a concern that the continued use of highly discretionary language creates several layers of justification for service providers to avoid implementing stronger, prevention-oriented technologies. IJM continues to maintain that a standard of 'best efforts' would be more appropriate, particularly in relation to a CSAM prevention obligation, which we recommend be embedded into the Duty. However, in recognition that 'reasonable steps' is the accepted standard within like legislation, we would strongly caution against including additional discretionary language which might further dilute the obligations on companies. This is especially in light of the tech sector's apparent bad faith interpretation of the 'reasonable steps' standard when implementing the social media minimum age requirement⁵ and reasonable steps provisions in the BOSE, SMS Code and RES and DIS standards. The Department should consider whether the 'reasonable steps' standard along with discretionary language essentially makes the Duty of Care unenforceable in practice by the regulator.
3. **Reconsider company discretion** – further to the above, IJM notes our concern about the intention demonstrated on page three of the issues paper to provide determinative discretion

⁴ Council of the European Union General Secretariat (March 2024). *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – updated possible criteria and classification methodologies for the risk categorisation of services*. Available from: <https://data.consilium.europa.eu/doc/document/WK-3036-2024-REV-1/en/pdf> at p. 4, fn. 5.

⁵ eSafety Commissioner (March 2026). *Five social media platforms flagged for compliance issues*. Available from: <https://www.esafety.gov.au/newsroom/media-releases/five-social-media-platforms-flagged-for-compliance-issues>

to companies: *“Each service would be required to assess their risks and determine what preventative responses, systems and processes **they can and ought** to develop and implement to meet the Duty.”*

IJM is concerned that this language, taken together with the reasonable steps standard, could allow services to internally decide that detecting, disrupting, and preventing child sexual exploitation material in live video, falls outside the scope of the systems and processes that they “can and ought” to develop. It is our position that such discretion would undermine the very purpose of the duty. Whether a company “can” develop and implement a preventative response is a determination best suited to policymakers or regulators presented with evidence of technical feasibility, including if needed as assessed by independent testing labs. Whether a company “ought” to implement a preventative response is essentially a question of tech policy based on social and government expectations of safety. Broad company discretion could be interpreted by some, including the public, as a *de facto* delegation to industry the duty of government regulation to set appropriate standards and guardrails. It may also make regulatory enforcement more difficult, since the company can always fall back on such discretionary language.

None of this is hypothetical. The eSafety Commissioner has repeatedly stated that technology exists to detect and disrupt live online child sexual abuse, and yet companies have chosen not to use it, thus allowing Australians to remotely produce, access, and consume live child sexual abuse videos without any prevention or reporting.

4. **Ensure prevention is included as a clear obligation** – the terminology of prevention is used throughout part one of the issues paper but not included as a core obligation in part two. IJM urges the Department to consider adding a core obligation to proactively prevent illegal content including CSAM images, videos and livestreams. In addition, IJM notes that the use of the terminology ‘prevent or mitigate’ on page 4 creates a disjunctive obligation, allowing service providers to satisfy the duty by choosing the lesser action of mitigation, even where the higher standard of prevention is more appropriate. We recommend adopting the terminology ‘prevent and mitigate’, to centre prevention as the primary obligation, supported by a secondary obligation to mitigate any residual risks. This would ameliorate the risk that service providers meet the standard through minimal action.

Additional feedback and reflections on the issues paper are provided by Toby Dagg, former senior leader at the Office of the eSafety Commissioner.⁶

We appreciate the Department’s ongoing engagement in this reform process, and note that IJM is available to provide further feedback as needed. We also look forward to receipt of the exposure draft in due course and would be grateful for the opportunity to be consulted when this becomes available.

Yours sincerely,

David Braga
CEO
International Justice Mission Australia

⁶ Toby Dagg. (June 2026). *The Wait Was Worth It—Mostly: First Impressions of Australia’s Digital Duty of Care*. Available from: <https://tobydagg.substack.com/p/the-wait-was-worth-itmostly-first?r=7mv5z7>



A Briefing Document for

s22(1)(a)(ii)

Shield Our Children Online Alliance

*Advocating for child online safety laws
that work in practice*

 socoa.org

 instagram.com/socoaorg

 x.com/SOCOAorg

 facebook.com/socoa.org

 linkedin.com/company/socoa-protects/

 socoa@info.org

Graham Hellier MBE

The Shield Our Children Online Alliance (SOCOA) was founded by Graham Hellier MBE, an entrepreneur and philanthropist who was awarded an MBE for his charitable contributions in El Salvador, where he founded, funded and worked to build a village he named Pequeña Inglaterra (Little England). Pequeña Inglaterra is home to over 2,000 people who lost their homes in earthquakes.

Background of the Cause

Graham discovered that a family member had been subjected to sexual behaviour at 8 years old with other 8-year-old children in the toilets at school. Years later, this caused psychological issues, which is when the sexual behaviour was discovered. Graham initially thought that one of the children may have been abused and was repeating that behaviour at school, but further investigation led him to discover the deeply troubling fact that children are watching online pornography from a very early age. Children naturally find adult content exciting, and they then copy the behaviour they have seen.

This led Graham to establish the Shield Our Children Online Alliance (SOCOA) to advocate for child online safety laws that work in practice.

Graham has no commercial gain and is advocating the implementation of third-party systems that already exist and are free of charge.

The Age Verification Problem

Age verification to access adult content has now been legislated in several countries, but the laws are completely ineffectual, with children still finding it easy to access pornography.

There are two reasons why the systems fail. The first is that the laws require pornography companies to conduct age verification. You cannot legislate the entire internet. Many pornography sites have ignored the age verification requirement, and the government cannot sue companies in jurisdictions like Russia and China. If a website is eventually blocked (after a court process), they can set up 100 new websites the next day. It is a game of whack-a-mole that cannot be won.

The second reason is that the laws ignore VPNs. Children know how to use VPNs from an early age. When one child discovers VPNs (maybe through an older sibling), they spread this news with their young peers. A Childnet survey found that 15% of 8- to 10-year-olds use VPNs for purposes such as accessing gaming servers that are not available in their country.

Proof of Failure

Surveys have found that 79% of 18 to 30-year-old males watch pornography each month, and up to 45% of females (though researchers agree that females are more likely to conceal their online behaviour due to social stigma).

The Lucy Faithfull Foundation research (UK), combined with the Stanford Cyber Police Center research, concluded that when presented with an age verification requirement, only 1.7% to 6% of adults actually complete the verification process.

94%+ of users then take one of two routes: switch to non-compliant websites or use a VPN. Although this research is on adults, why would children be any different?

But you do not need to question if the new systems work. You can simply search and find pornography websites that ignore the laws. Annex A is a small example of 54 websites (out of 70 checked) that can be accessed by children in Australia despite the new age verification laws now being in place. The same applies in the UK. Legislating against thousands (and ever-growing numbers) of individual pornography websites on the internet is impossible.

Data Risks

Although SOCOA has been established to protect children, they also believe that 18+ should be able to easily and safely access adult content.

The new laws in the UK, Australia, etc., actually facilitate each pornography company's preference to gather data on users under the pretext of age verification. 40% to 60% of private emails can be traced directly back to the user, with that rising to up to 85% when a business email is used.

Pornography companies track user behaviour and therefore sexual preferences. This can then be linked directly to a user's personal contact data, raising significant concerns about data breaches or the sale of data for extortion.

Companies like Aylo (Pornhub) have created their own age verification company AgeID. Although there are guidelines for handling data, there are no audits and therefore no legal enforcement.

In November 2025, a third-party data provider to Pornhub was hacked by a cybercrime group called ShinyHunters. They hacked data on over 200 million users, including registered email addresses, user locations, specific videos and channels watched, and search keywords used.

ShinyHunters has approached Aylo for a ransom payment. It is not known if this was paid, but it is known that Pornhub cooperated with law enforcement to investigate the issue.

The new laws do not protect children, and they also expose the general public to a significant risk of extortion.

The Internet Service Provider Solution

All internet traffic in every country is delivered to end users through Internet Service Providers (ISPs); for cellular traffic, the ISP is the Mobile Network Operator (MNO).

Because ISPs must hold a government license to operate, they are already tightly regulated, making them the most practical partners for implementing new child protection measures. Many ISPs already provide optional content filters that can block access to pornography. These systems are proven and widely used, meaning the infrastructure to enforce restricted access to adult content already exists; it simply needs to be mandated and standardised through legislation.

Some countries already legally require their ISPs to block all adult content by default. Extending this approach to include age verification for adults, rather than outright blocking, is a simple adjustment for any nation that permits access to pornography for those over 18. Crucially, enforcement is far more practical. It is significantly easier for regulators to take action against a licensed ISP which already operates under government oversight than to pursue a pornographic website based overseas in jurisdictions such as Russia.

Anonymous Age Verification

Anonymous age verification using tokenisation is a privacy-preserving technique that allows users to prove they are above a certain age threshold without storing their details and without risking revealing any information to pornography companies or associated third parties.

For example, the EU has developed a free, open-source app that enables a person to generate a QR code identifying them as 18+ in total anonymity. This app can be adapted for any country.

To view a video of how the app works, click here.

<https://ageverification.dev/>

For the very few users who do not have mobile phones, a desktop age verification system can be offered.

A user only has to undertake their age verification once (read 'How Tokenised Age Verification Works' on the next page).

Overcoming the Simple Virtual Private Networks (VPNs) Workaround

Internet Service Providers (ISPs) can detect when a user connects to a VPN. They can therefore undertake the same “18+” check before allowing the connection. Once the user has confirmed their 18+ status on a device, they can automatically connect to an adult site or a VPN without repeating the check on that device.

How Tokenised Age Verification Works:

Steps

1. Initial Age Check

When accessing adult content or a VPN for the first time, the ISP will display an “Age Verification Gate” that requires the user to either age-verify via a website or download the age-verification app (such as the EU open-source app).

If age verification is carried out in a mobile app, the user is then provided with a QR code (which cannot be copied and is renewed repeatedly). The QR code system can then be used for all subsequent age verification, which must be undertaken once per device.

If they do not use the app, they will be required to undertake age verification on each device that they use.

2. Issuance of an Age Token and QR Code

Mobile Phone - The user can undertake age verification via a website or by downloading the app. When 18+ age verification is confirmed, the mobile phone ISP is sent a link that creates a “fingerprint,” confirming that the device and phone number are associated with an 18+ user.

Other Devices - When the ISP detects a user connecting to an adult site or a VPN on another device, they either use their phone app as confirmation that they have already proven they are 18+ (similar to how WhatsApp enables linking a WhatsApp account to another device) or carry out a separate age verification check. When an 18+ age has been verified, a token is placed on the device.

3. Presenting Tokens Online

When accessing age-restricted services or a VPN, the ISP checks the device (phone, computer, etc.) for the token.

4. ISP Checks Token

ISP then checks that the token is approved for 18+ use through a central register and allows access.

Net Result

When using the app, 18+ users only need to age verify once. Or when not using the app, users still only need to age-verify once per device. After that, they have unfettered and easy access to VPNs and pornography sites.

Please view our SOCOA video here:

<https://socoa.org/country/?c=AU>

Australian Legislation

Australia has now introduced age verification for adult sites.

The enforcement of the legislation has already failed, as it has in the UK.

The following Annex contains just a few examples of the many websites that are not complying. It is impossible to legislate against websites on the internet. It is possible to enforce legislation with Internet Service Providers.

WARNING: *These sites contain graphic adult content that is available to any child, as the new Australian law requiring Age Verification does not work and will not work (7-year-olds watch porn, 27% of children admit they have watched porn by the time they are 11 years old).*

Annex A: SOCOA Australia Website Audit Tracker — Site-Level Verification Log

Annexure A of Document 11 (pages 81 and 82) is available upon request. If you wish to obtain a copy of these documents, please contact us at foi@infrastructure.gov.au so we may consider your request further.



Briefing - Meeting with Yoel Roth

From s22(1)(a)(ii)@infrastructure.gov.au>

Date Wed 17/06/2026 16:34

To s22(1)(a)(ii)@infrastructure.gov.au>

Cc s22(1)(a)(ii)@infrastructure.gov.au>

📎 1 attachment (267 KB)

Online Safety Act Review_Match Group Comments.pdf;

OFFICIAL

Hi s22(1)(a)(ii)

As requested, please find briefing notes for this meeting (reviewed by s22(1)(a)(ii), notes from 2 June meeting, paper provided to Dept by Match.

Briefing Notes on DDOC:**Match Group**

(Dept. only)

3:30pm

18 June 2026

Attendees:**Yoel Roth**

Senior VP Trust & Safety, Match Group

David Quilty

Managing Director, National Advisory

Camélia Assaoui

Director of APAC Communications, Match

Match Group is the American parent company for several major online dating apps, including Tinder, Hinge, OkCupid, and Plenty of Fish. National Advisory is an Australian based Government relations firm, and represents Match Group.

s47C



s47C



Meeting Notes from 2 June:

s47C



Thanks,

s22(1)(a)(ii)

s22(1)(a)(ii) she/her

Policy Officer • Online Safety Reform • Digital Platforms International & Policy

E s22(1)(a)(ii) @infrastructure.gov.au P s22(1)(a)(ii)

Living and working on Ngunnawal Country

OFFICIAL



Re: Question on stand-alone AI services [SEC=OFFICIAL]

From s47F

Date Thu 02/07/2026 17:07

To s22(1)(a)(ii)@communications.gov.au>

OFFICIAL

Hi s22(1)(a)(ii)

Thank you and this is good news. Glad to hear the proposals are motoring along.

I am always in awe of the work it takes to get a proposal drafted. It's no small feat, and I am wishing you and the team luck (and sanity!) through the process.

Thanks again,

s47F

OFFICIAL

On Wed, Jul 1, 2026 at 10:32 PM s22(1)(a)(ii)@communications.gov.au> wrote:

OFFICIAL

Hello s47F

This is incredibly helpful and the team and I love these types of questions. You've provided enough context so we can move this forward in terms of progressing work about the definitions and testing their robustness so thank you very much.

For your awareness, we have been allocated a legislative drafter, but the drafting has not yet commenced in earnest as the Office of Parliamentary Counsel is tied up on a number of other legislative priorities.

This means there's still plenty of time to work up the case studies/edge cases and we will use these to test further with the drafters. If you're able to send through something by the end of the month that would be amazing.

Thanks again s47F - we really appreciate your ongoing engagement and no doubt will reach out with further questions.

Cheers

s22(1)(a)

s22(1)(a)(ii)

Director • Online Safety Reform • Online Safety and Classification Division

s22(1)(a)(ii)@infrastructure.gov.au

P s22(1)(a)(ii) • M s22(1)(a)(ii)

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

From s47F

Sent: Wednesday, 1 July 2026 02:25

To: s22(1)(a)(ii) <[REDACTED]@communications.gov.au>

Subject: Re: Question on stand-alone AI services [SEC=OFFICIAL]

OFFICIAL

Hi [REDACTED]

Thanks for reaching out and sorry for my delayed response. It's been a week. I can only imagine that yours has been as well!

s47C



Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

s47C

Thanks again,

s47F

OFFICIAL

On Tue, Jun 23, 2026 at 5:42 AM s22(1)(a)(ii)@communications.gov.au> wrote:

OFFICIAL

Hi s47F

Thanks again for meeting the Minister's office and department on 21 May to discuss the Digital Duty of Care. I'm sorry I missed this meeting as your insights are always valued, and this round of feedback has been a really useful input into our work.

We are still working through the feedback received throughout this latest round of consultation but wanted to explore further a comment you made s47C

Do you have any further information or examples that you can share to help us work through this?

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Kind regards

s22(1)(a)

s22(1)(a)(ii)

Director • Online Safety Reform
Online Safety and Classification Division

s22(1)(a)(ii) [@infrastructure.gov.au](mailto:s22(1)(a)(ii)@infrastructure.gov.au)

P s22(1)(a)(ii) • M s22(1)(a)(ii)

GPO Box 594 Canberra, ACT 2601

Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

CONNECTING AUSTRALIANS • ENRICHING COMMUNITIES • EMPOWERING REGIONS

infrastructure.gov.au

OFFICIAL

OFFICIAL

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts



Digital Duty of Care - feedback from TCA members

From s47F <[redacted]>@techcouncil.com.au>

Date Wed 01/07/2026 15:52

To s22(1)(a)(ii) <[redacted]>@communications.gov.au>

Cc s47F <[redacted]>@techcouncil.com.au>

Good afternoon

Since our discussion with the Department regarding the proposed Digital Duty of Care, the TCA has had a number of conversations with its members and received feedback on the proposal.

While I understand that this feedback is now (very!!) late, in case it is of some use to you at this stage, I have included it below. We understand that there will be further opportunities for comment and so will also provide these comments (if relevant) at that point.

Please reach out to myself or s47F <[redacted]> (cc'ed) if you have any questions.

Kind regards

s47F <[redacted]>

s47C <[redacted]>



s47C



--

s47F

[Redacted]

| Tech Council



M s47F

E s47F@techcouncil.com.au

W www.techcouncil.com.au

Released under the FOI Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts



Outlook

RE: Digital Duty of Care [SEC=OFFICIAL]

From Hyles, Andrew <andrew.hyles@communications.gov.au>

Date Tue 14/07/2026 15:46

To s47F -Digital Defence s47F@digitaldefence.org>

Cc s22(1)(a)(ii)@communications.gov.au>

OFFICIAL

Released under the FOI Act 1982 by the Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Thanks for this feedback s47F and certainly from my perspective, s47C
I'll
certainly keep the below in mind as we progress the drafting of the legislation
and have copied my team in too.

Thanks

Andrew

Andrew Hyles

Assistant Secretary • Digital Platforms, International and Policy • Online Safety and Classification

Andrew.Hyles@communications.gov.au

P s22(1)(a)(ii) • M s22(1)(a)(ii)

OFFICIAL

From: s47F -Digital Defence <s47 @digitaldefence.org>

Sent: Thursday, 2 July 2026 9:27 AM

To: Hyles, Andrew <andrew.hyles@communications.gov.au>

Subject: Digital Duty of Care

Dear Andrew,

I hope you're well.

I wanted to follow up on one issue that has been on my mind since our last meeting, prompted by something that has unfolded in the news this week.

TikTok has announced it is cutting approximately 300 jobs at its Dublin trust and safety hub. This follows Meta cutting 350 from its Irish operations in May. Both companies cite AI efficiencies. For context, Dublin is not a back office location - it is where these platforms house their moderation, data protection, and trust and safety functions for the European market.

s47C

Trust and safety work has historically been anticipatory. The value of a good trust and safety team is not in processing the harms that regulators have already catalogued. It is in identifying the patterns that precede the next one. That instinct is being downsized out of existence right now and in my humble opinion, the timing relative to incoming regulation is not a coincidence.

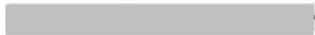
s47C



I am happy to discuss further or to put something more detailed in writing if it would be useful.

Kind Regards

s47F

Digital Defence

www.digitaldefence.org



Issue	Theme	Raised by	Detailed comments	Consideration status	Outcome (and why?)	Source
CSP/ISP providers should be exempt from DDoC	Scope	s47C				Australian Telecommunications Alliance
Compliance with BOSE, codes and standards to be sufficient for compliance with DDoC	Interaction with existing legislation and codes					Australian Telecommunications Alliance
Minimum 12 month transition period	Transition					Australian Telecommunications Alliance
Maintain 'disordered eating' as a harm category and capture AI and algorithms	Scope					Butterfly Submission
Ensuring classification captures disordered eating content	Scope					Butterfly Submission
Defining illegal and harmful materials	Scope					DIGI Submission
Commissioner's enforcement powers should only be based on the risk of serious physical and mental harm	Compliance and enforcement					DIGI Submission
Mandatory public consultation on regulator issued guidance	Consultation					DIGI Submission
Reporting and requirements should be transparent and limited in frequency	Reporting					DIGI Submission Interactive Games & Entertainment Association
Commissioner guidance to be treated as a disallowable instrument	Reporting					DIGI Submission Interactive Games & Entertainment Association
Confidentiality protocols should be included	Privacy and confidentiality					DIGI Submission Interactive Games & Entertainment Association
Mandatory independent audits should not be included or limited in scope	Reporting					DIGI Submission
Onling gaming to be excluded from DDoC	Scope					Interactive Games & Entertainment Association
A broad scope may capture unintended content and create uncertainty for industry	Scope					Interactive Games & Entertainment Association
Safe harbour and clearly defined standards and expectations	Compliance and enforcement					Interactive Games & Entertainment Association

Graduated approach to compliance and last resort measures	Compliance and enforcement	s47C	Interactive Games & Entertainment Association
Unclear rationale for additional audit powers for eSafety	Reporting		Interactive Games & Entertainment Association
Additional support or reduced requirements for small business	Reporting		Interactive Games & Entertainment Association
DDoC should be established in reference to a risk-based approach	Scope		Interactive Games & Entertainment Association
Grandfathering arrangements for entities currently complying with the BOSE	Compliance and enforcement		Interactive Games & Entertainment Association
Extending definition to include both children as users of the service and children who are non-users	Scope		International Justice Mission Australia
Include livestreaming as a feature that may increase the risk of harm	Scope		International Justice Mission Australia
Strengthening of obligations on industry	Compliance and enforcement		International Justice Mission Australia
Ensure prevention is included as a clear obligation	Scope		International Justice Mission Australia
Ongoing monitoring and observation	Reporting		University of Melbourne
DDoC should provide for public interest exemption and protections	Scope	s47F	University of Melbourne
DDoC should only cover illegal content and content harmful to children	Scope		Email submission from TCA on 1 July 2026.
Focus on services whose primary purpose is to socialise and share user content	Scope		Email submission from TCA
B2B services	Scope		Email submission from TCA
Recommender systems	Scope		Email submission from TCA
Private right of action	Scope		Email submission from TCA
Transition from BOSE, Codes and Standards	Scope		Email submission from TCA