INTERNET ASSOCIATION OF AUSTRALIA LTD

ABN 71 817 988 968

ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

05 November 2026

To the Committee Secretary

Senate Standing Committee on Environment and Communications
PO Box 6100
Parliament House
Canberra ACT 2600

By email: ec.sen@aph.gov.au

RE: Online Safety Amendment (Digital Duty of Care) Bill 2026

The Internet Association of Australia Ltd (**IAA**) thanks the Senate Standing Committee on Environment and Communications (**Committee**) for the opportunity to respond to the inquiry into the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (**Bill**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized internet service providers (**ISPs**), who provide internet carriage services (**ICS**) and fall within the scope of the Bill. We emphasise that IAA and our members support the Government's policy intent of ensuring Australia has an appropriate legislative framework to better protect Australians from online harms. As ISPs provide the underlying infrastructure for digital activity, we understand and recognise ISPs have a role to play in ensuring a safe online environment. To this end, IAA and our members have been actively involved in the Government's efforts to ensure the online safety of Australians, contributing to the co-regulatory industry codes governing online safety, and responding to the consultation on the Exposure Draft of the Bill completed by Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (**the Department**) in September 2026. Our response to the Exposure Draft is annexed to this response, for reference.

However, as expressed in our response to the Exposure Draft, we hold it equally important that any legislative obligations are practicable and reasonable, reflecting the technical and operational realities of the applicable online service providers in order to be truly fit-for-purpose. We are concerned that despite these points raised in response to the Department's consultation on the Exposure Draft, the Bill remains broadly - and therefore, inappropriately - scoped.

In particular, in relation to ICS, while ISPs are certainly an important part of the internet ecosystem, the nature of ICS as the underlying conduit for connectivity is fundamentally different to most of the other online services identified in the Bill which operate on the content layer, and therefore are not suitably placed to bear the proposed digital duty of care (**DDOC**). Moreover, our members, comprising the smaller entities within the sector would be disproportionately burdened by the obligations without a commensurate safety benefit for end-users, again because of the technical conduit nature of ICS, compounded by the constrained resources as small, challenger ISPs within the market.

As such, we provide our response below, primarily focusing on whether the proposed obligations reasonably reflect the role of ISPs in the digital ecosystem.

OUR RESPONSE

LACK OF CONSULTATION

Firstly, IAA reiterates our significant concern regarding the lack of consultation on the proposed DDOC framework, as was raised in our response to the Exposure Draft. Overall, IAA and our members were greatly disappointed with the Department's consultation on the Exposure Draft, which did not meet the Government's best-practice consultation standards, and therefore raises concerns about the sensibility, practicability and effectiveness of the Bill. We note that:

- the consultation was held over a two-week period, failing to meet the Office of Impact Analysis' best-practice consultation standards[1] which recommends a minimum four-week consultation period. Given the landmark nature of the proposed DDOC framework, we consider this consultation period to have been insufficient to fully assess the proposed changes;
- the consultation was limited to written responses to the Exposure Draft only, and further capped to five pages with (to our understanding) no effort to hold any public roundtables or town halls to engage stakeholders for whom providing written submission is a high barrier to engagement with law reform processes, despite the Bill being relevant to specific stakeholder groups (such as children) where non-written consultation approaches would be more suitable;
- the consultation was not listed on the Department's consultation hub,[2] despite IAA raising this with the Department - we consider this to have prevented wide engagement with the Exposure Draft as many stakeholders are likely to have been unaware that the consultation was going on, or could not access the necessary material to examine the Exposure Draft;
- to our understanding, no targeted consultation was held with specific stakeholder groups, including with ISPs, and in particular, small to medium sized ISPs;
- the Department chose to not publicise submissions received in relation to the Exposure Draft, which we also consider obfuscates transparency and reduces accountability.

While we support the Government's intent to promptly implement measures to improve the online safety of Australians, we considerer it equally important in making sure the legislative settings are appropriate and practicable in order to be effective and deliver true benefits. As such, given the above stated deficiencies in the Department's consultation approach, we do not consider stakeholders have had sufficient time to assess and provide feedback on the proposed DDOC framework.

We appreciate that the Committee's inquiry provides stakeholders with further opportunity to provide feedback on the Bill. However, we note that the submission window to submit to the Committee is similarly short (again, roughly 2 weeks). Moreover, for ISPs, the Inquiry submission window overlapped with the ACMA's consultation period on the draft *Telecommunications (Consumer Protections) Industry Standard* which is likely to have taken priority for most ISPs.

We therefore recommend that:

- **the Committee recommends the Senate not pass the Bill, and that the Bill should be re-released as a revised exposure draft for public consultation; and**
- **the public consultation period should be for a minimum of four-weeks, during which period, the Department should engage in targeted consultations with relevant stakeholder groups.**

Notwithstanding this position that the Bill should not be passed, we provide further comments on the Bill, as below.

[1] https://oia.pmc.gov.au/sites/default/files/2023-08/best-practice-consultation.pdf
[2] https://www.infrastructure.gov.au/have-your-say

SCHEDULE 2 – DIGITAL DUTY OF CARE

Online Services Scope – Internet Carriage Services

We understand that ICS would fall within the scope of an 'online service' and would therefore be subject to the new DDOC framework. However, as raised in our response to the Exposure Draft, we reiterate that an ISP has extremely limited visibility into, and no practical ability to moderate, digital content carried across its network. We do not consider a duty framed around ensuring a safe *online* environment is a suitable conceptual fit for a service that operates at the network-layer.

The limited control an ISP has is a position already recognised by the existing regulatory framework governing online safety, including the online codes and standards. We understand that the ICS is currently recognised as forming part of the Internet ecosystem under the *Online Safety Act 2021* (**the OSA**). However, the applicable obligations in the industry codes for ISPs were significantly lighter, reflecting the nature of ICS. In contrast, the Bill does not appropriately scope out ISPs from the overall DDOC framework. ICS remain broadly in scope under the overall DDOC framework (Part 2 of Schedule 2), and faces obligations disproportionate to the level of technical control.

Moreover, IAA members, as smaller ISPs, have limited resources and are particularly disproportionately affected by the regulatory burdens that these obligations would impose. Given the nature of ICS, the regulatory burden imposed by these obligations is not commensurate to the benefits for Australian end-users. This is not to say ISPs should not play a part in improving Australia's online environment, but rather, the rules that apply to ICS should reflect the nature of the ICS and level of control ISPs have over content shared over its network.

We appreciate that the scope of ICS has been narrowed since the Exposure Draft, now applying only to ICS that is supplied to the public. However, this does not resolve the issue that ICS, as a conduit service, is not well placed to address online harms, or bear a duty of care for digital content.

IAA therefore recommends the removal of ICS as a category of online service under proposed s 25B for the purposes of the proposed Part 2 DDOC framework.

Notwithstanding this position, if ICS are to remain within scope, we recommend that:

- **ICS should be exempted from the whole of proposed Part 2 of the OSA, or at the least from proposed ss 26, 26C, 27, 27B, 27C, 27D, 27E, 27F, 27G and 27H using the exemption power in proposed s 25B(3);**
- **the scope of ICS should be further clarified to exclude wholesale and enterprise network services;**
- **the matters relevant to determining what actions or measures are 'appropriate and effective' as set out in proposed s 26A should be expanded. This will be further discussed below in relation to the proposed s 26A.**

Notwithstanding this position, IAA raises further concerns and makes recommendations in relation to specific provisions and obligations under the proposed Part 2 DDOC framework below.

Overlap with other online services

It is unclear how the obligations should apply to an ISP in respect of other ancillary services provided in relation to their ICS.

<u>Designated internet services</u>

Most ISPs provide and operate ancillary services or products, such as customer portals or mobile applications alongside, and to support the provision of, ICS. Given the broad definition of 'designated internet service', we consider it possible that these ancillary services will also be captured by the DDOC framework. **If so, we recommend that these also be expressly carved out from the DDOC in accordance with proposed s 25B(3).**

Such portals are functionally distinct from typical designated internet services in that they do not enable interaction between end-users, nor present the exposure risks that we understand the DDOC framework intends to address. However, the compliance burden of distinctly capturing the portal will be disproportionate, particularly for smaller ISPs.

A service that manufactures, supplies, maintains or installs equipment

We query the breadth of proposed s 25B(1)(i), which also captures services that manufacture, supply, maintain or install equipment for use in Australia that enables communications using an ICS. The persons who manufacture, supply, maintain and install equipment are different, and it is unclear whether the intent is to capture all of them. For example, general retailers of consumer networking equipment could be said to 'supply' equipment. ISPs often supply routers and modems to customers but have limited control over their design or function, and responsibility should sit with the manufacturer.

It is also unclear what risks or harms a supplier of such equipment is expected to foresee, or what the Government's intent is in capturing this class of service. **We recommend that this class be removed from the Part 2 DDOC framework. At the least, this class should be exempted in accordance with the proposed s 25B(3).**

Exemption power - s 25B(3)

We recommend that the exemption framework set out in ss 25B(3)-(5) be expanded to:

- **allow the Minister to exempt an online service or class of online service where satisfied the service has limited or no control over harmful material, in addition to the existing 'little risk' test; and**
- **an objective and tiered threshold for reduced or scaled obligations by subscriber number, or annual turnover, to ensure smaller ISPs are afforded proportionality in respect of the DDOC**

'Appropriate and effective' – s 26A

We understand this standard of what is 'appropriate and effective' has replaced the 'reasonably practicable' standard proposed in the Exposure Draft. However, we consider reasonable practicability should still be taken into account. We also oppose proposed s 26A(3), under which cost must not be taken into account. The cost of a measure is a relevant consideration in determining whether it is appropriate to the level of risk posed.

We therefore recommend that the matters set out in proposed s 26A be expanded to include:

- **the nature of the online service provided by the person;**
- **whether taking action or measures is reasonably practicable, including the person's degree of control over, and visibility of, material on the service;**
- **the impact of actions on the privacy of the end-user, including the effectiveness of end-to-end encryption;**
- **whether the action or measure is reasonably practicable;**
- **the size and resources of the person;**

Risk assessment – s 27

We posit that imposing obligations for ISPs to conduct annual risk assessments have little end-user benefit, compared to the cost for providers. Conducting annual risk reviews is no small task for resourced constrained telco operators, many of whom also face overlapping risk assessment obligations under the *Security of Critical Infrastructure Act 2021*.

We recommend that ICS be explicitly carved out from s 27, or be exempted in accordance with s 25B(3).

Notwithstanding this position, we also recommend that:

- **the proposed s 27 should expressly specify that the risk assessment relates only to online safety and the person's DDOC; and**
- **the frequency of the risk assessment review should be scaled to the nature of the service and the extent of change to a service, recognising the largely unchanged nature of ICS that would give rise to risk.**

Age assurance and access control measures – s 27D

We consider the proposed threshold of when s 27D is to apply is too broad and likely to capture ISPs as ICS is the underlying network over which all digital content (such as pornography or material describing or depicting specific fetish practices or fantasies) is shared, regardless of its limited control over that content. While we understand and appreciate that s 27D(2) adds the qualifier that a person responsible for the online service must implement age assurance and access control measures, '*where technically feasible and reasonably practicable*' (emphasis added). However, we do not consider this is clear enough in setting expectations as to what, if any, measures an ISP must take to comply with this proposed s 27D. This is particularly the case for small ISPs who we reiterate have limited regulatory capacity to understand and decode legislative instruments.

The industry code which currently deals with the content intended to be targeted by this proposed s 27D (Schedule 2 of the consolidated Industry Codes in relation to Class 1C and Class 2 Material) aptly limits the compliance measures that reflect the level of control and visibility of ISPs and the nature of ICS, as follows:

- informing end-users of filtering products and how to obtain them, including promotion of the Australian Telecommunications Alliance's Family Friendly Filter program;
- where an ISP provides its own filtering tool, keeping the product updated and ensuring compatibility;
- providing plain language safety information for parents and carers; and
- informing end-users about complaints rights and processes.

In contrast, the age assurance measures under the proposed 27D are not workable given the nature of ICS. While typically, an ISP's contractual relationship is with an adult account holder, the connection can be used by multiple people and the ISP has no visibility as to who is using the internet service. Moreover, while the filtering tool may be an access control measure, it is not reasonable to require all ISPs to develop and provide its own filtering tool, which paragraph 27(D)(2)(b) may imply.

We recommend that ICS be explicitly carved out from s 27D, or for ICS to be exempted under proposed s 25B(3). In any case, there should be clear legislative assurance that ISPs are not expected to age-restrict their service or age-assure their end-users as doing so would not be 'technically feasible and reasonably practicable'.

Delegated powers

We are concerned that a significant number of provisions in Schedule 2 allow the Minister or Commissioner to determine scope, impose new obligations, or compel action from providers, by legislative instrument or written notice, without sufficient guardrails. **Given the consequences the exercises such powers can have on an entity, especially a resourced constrained smaller ISPs, we recommend that prior to the Minister or Commissioner exercising such powers:**

- **they should be required to consult – publicly, or directly, depending on whether the power operates across a class of services, or is directed at a single entity; and**
- **the Bill should expressly scope out matters that must be considered, such as (and to the extent applicable):**
    - **the level of risk posed by the service;**
    - **the nature of the service and the person's degree of control over, and visibility of, material on it;**
    - **the size and resources of the person, including subscriber numbers and turnover;**
    - **the cost/benefit of the obligation or action;**
    - **technical feasibility;**
    - **impact on privacy and security (including encryption);**

- **overlap with existing regulatory obligations; and**
- **the burden on smaller providers.**

Public consultation

We recommend that public consultation (of at least 30 days) be made a statutory requirement in respect of the following:

- exemptions under s 25B(3), and the Minister's determinations under s 25C(2) and 25G(2);
- user empowerment tool instruments under s 27A(1);
- the Commissioner's additional risk assessment requirements and shorter review intervals under ss 27(2)(f) and 27(4);
- the Commissioner's determinations under s 27G, namely the requirements for complaint and dispute processes (s 27G(1)(b)) and the classes of prescribed online service (s 27G(3)) – we posit that wider consultation is necessary rather than the proposed requirement for the Commissioner to only consult the Privacy commissioner as set out in proposed s 27G(4);
- publication determinations under s 192L, with factors that the Commissioner must consider when specifying a class on online services to be set out in the Bill; and
- the approved researcher and data access legislative rules under ss 205B and 205C.

Targeted consultation

Where a power is exercised to compel a person to do something by written notice,[3] we recommend that the Commissioner be required to consult that person directly, to give person must be given an opportunity to make submissions prior to issuing the notice.

Additionally, a person to whom a formal warning or remedial direction is to be issued should be given an opportunity to make submissions, prior to the warning or direction being issued.[4]

Parameters and Scope

We are also concerned that several provisions express powers of the Minister or Commissioner as being 'without limitation'.[5] **We do not consider this appropriate, and recommend that such powers be expressly and appropriately scoped in the Bill.**

Complaints handling – s 27G

ISPs are already subject to complaints-handling obligations under the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*. The proposed s 27G obligations would therefore impose overlapping obligations. **We therefore recommend that ICS not be prescribed for the purposes of proposed s 27G.**

Commencement Timeframe

We understand the Bill proposes for the DDOC obligations under Part 2 to commence 12 months following Royal Assent. We submit that this commencement timeframe is too short, and does not appropriately reflect the operational realities of particularly smaller ISPs with respect to new regulation. Again, we reiterate the resource constraint of small ISPs.

Given the scale of the new compliance obligations, we recommend that the proposed commencement timeframe be extended to 18 months following Royal Assent. At the least, we recommend a staged commencement timeframe based on the online service category, and size and/or revenue thresholds to provide ISPs, and in particular, small ISP a longer lead time. We consider this would be appropriate as other online services should be prioritised based on the risk of harm compared to ICS.

[3] This would apply to proposed ss 28A, 192B, 199, Division 2 of Part 14.

[4] This would apply to proposed ss 26D, 26E, 27B, 27E(2), 27F, 27G(6), 27H.

[5] ss 27A(2), 28A(3), 192C(1), 192L(2)–(3) and 205C(4).

Privacy Act Amendments

Due to time constraints, and given that the *Privacy Act 1988* (**Privacy Act**) is also currently under review, we have not been able to fully assess the privacy impacts of the proposed addition of the Commissioner as an 'enforcement body' for the purposes of the Privacy Act. However, we anticipate this will create further confusion and complexity for ISPs given the already extensive data-retention and disclosure obligations under the *Telecommunications (Interception and Access) Act 1979*.

SCHEDULE 3 – REPEAL OF ONLINE CONTENT SCHEME INDUSTRY CODES AND STANDARDS

We understand that the existing co-regulatory framework under Division 7 of Part 9 of the OSA is to be replaced by the proposed DDOC framework. As expressed in our response to the Exposure Draft, in principle, we support the legislative intent to repeal the codes and standards so as to prevent duplicative online safety frameworks in the event the DDOC is established. **Therefore, in the event that the DDOC framework is established, we support the repeal of the industry codes and standards.**

However, we strongly argue that the DDOC framework should be established under a co-regulatory model instead of the prescriptive framework as currently drafted.

As discussed above, IAA is concerned about the lack of engagement with the sector in relation to the proposed DDOC framework, and the plans to repeal the co-regulatory codes and standards. It is unclear why the existing co-regulatory model was deemed unfit to pursue more stringent DDOC objectives. Many of these codes and standards were only reviewed, consulted on and registered very recently with the first set of industry codes addressing class 1A and class 1B illegal material (**Phase 1 Codes**) only having commenced in late 2023, while codes addressing class 1C and class 2 material (**Phase 2 Codes)** only came into effect in December 2025. There has not been sufficient time to assess whether the co-regulatory industry codes and standards are deficient. Even if it is considered a more stringent DDOC must be established, we consider the co-regulatory approach to be more suitable. Co-regulation has the benefit of being designed by the industry participants who have the technical and operational expertise to ensure effective and practicable regulation.

As such, we reiterate that the DDOC provisions set out under the proposed Part 2 of the OSA should be amended so that ISPs are only subject to a lighter set of obligations, proportionate to the nature of ICS in the context of online safety.

Furthermore, in consulting further on the Bill (as recommended above), Government should also consult on developing a DDOC framework via a co-regulatory approach.

SCHEDULE 1 – NOTICES OF CERTAIN MATERIAL AND DISCLOSURE OF INFORMATION

We appreciate and support that the proposed obligations under Schedule 1 do not intend to target ICS. As stated in the Explanatory Memorandum, we understand that the measures under Schedule 1 are primarily intended to address apps and websites that are used to generate fake nude material, hosting providers that host unsafe material and internet search engines that provide links to cyber-bullying or cyber-abuse material. This is appropriate as ISPs have little to no visibility or control over content shared across their networks, and therefore, should not be held responsible for such content. **This same principle should be applied to the rest of the DDOC framework.**

We note that some ISPs may still be subject to certain obligations[6] by virtue of falling within the broadly defined designated internet service – or other - category, such as where ISPs provide and maintain ancillary websites, customer portals or mobile applications in connection with the provision of their internet carriage service. However, we understand the risk of materials of the kind captured by the OSA (for example, cyber-bullying material targeted at a child) being provided by such an ISP operated website or portal is low, and unlikely to give rise to the exercise of the Commissioner's removal notice powers in respect of ISPs.

Given the low risk of harm posed to end-users, and to reduce any confusion for ISPs, we recommend that an ISP's customer portal, website or mobile application that support the ISP's provision of ICS,

[6] For example, removal notices under ss 65, 77, 88 and 109 of the OSA.

and do not enable interaction between end-users be specified as services that are not designated internet services under s 14(2) of the OSA.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Committee's inquiry into the *Online Safety Amendment (Digital Duty of Care) Bill 2026*. We reiterate our commitment to online safety, and our recognition of sound legislation that will help achieve this. To that end, we emphasise the need for legislation that is set at the appropriate level and does not unnecessarily impose obligations on online service providers who lack the relevant technical or operational control. We look forward to working with the Government, regulators, industry, and other stakeholders to develop an effective regulatory framework that is proportionate, practicable and reflective of the Internet ecosystem it seeks to regulate.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (**WAIA**), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our public policy work is guided by the following principles:

We stand for an internet for the common good

We stand for an open internet platform

We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

ANNEXURE: IAA'S RESPONSE TO THE EXPOSURE DRAFT

INTERNET ASSOCIATION OF AUSTRALIA LTD

ABN 71 817 988 968

ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

22 September 2026

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

By email: digitaldutyofcare@communications.gov.au

RE: Online Safety Amendment (Digital Duty of Care) Bill 2026 – Exposure Draft

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (**Department**) for the opportunity to respond to the consultation on the exposure draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (**Bill**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers (**ISPs**). IAA and our members have been actively engaged in the Government's efforts to ensure the online safety of Australians. As ISPs are an integral part of the online ecosystem providing the underlying infrastructure for digital activity, we understand and recognise all Internet players and participants have a role to play.

In principle, we support the policy intent of ensuring Australia has an appropriate legislative framework to better protect Australians from online harms. However, we are concerned that as currently drafted, the Bill overreaches and is disproportionately scoped. From the outset, we emphasise that while ISPs are certainly an important part of the Internet sector, the nature of its services as providers of the underlying 'pipe' for connectivity is fundamentally different to most of the other online services identified in the Bill which operate on the content layer. We further stress that our members, comprising the smaller entities within the sector would be disproportionately burdened by the obligations without a commensurate safety benefit for end-users, again because of the nature of ISPs' operations.

Given the compressed consultation timeframe and page limit, we have not been able to full assess the Bill or its implications, and consider it likely that further issues and concerns will emerge. This response should therefore not be treated as a complete statement of feedback.

OUR RESPONSE

CONSULTATION APPROACH

Firstly, IAA raises significant concerns regarding the consultation process. IAA and our members are greatly disappointed about various aspects of the Department's consultation approach, which we do not consider meets Government's best-practice consultation standards.

Firstly, the compressed timeframe of only two weeks being afforded for the consultation of a law reform proposal of this significance is gravely insufficient. We note that the Office of Impact Analysis' best-practice consultation standards sets out a minimum four-week consultation window, to longer where necessary in the circumstances, commensurate with the scale and substance of the law-reform package.[1] While we understand in certain circumstances, urgency is required to prevent serious harms which may justify a shorter consultation window, in such cases, the competing interests must be balanced where due consideration should be given to the benefit of allowing a sufficient consultation period that allows

[1] https://oia.pmc.gov.au/sites/default/files/2023-08/best-practice-consultation.pdf

stakeholders to thoroughly consider and assess the proposed changes, and provide sound feedback to ensure the resulting legislation is effective and practicable.

Moreover, in this case, we do not consider the content of the Bill to justify such a compressed consultation timeframe. That is not to say we do not recognise the importance of online safety. Indeed, we reiterate our support for the underlying policy intent and recognise the importance of online safety and the need for timely legislative measures to ensure all Internet industry participants are playing the part to improve online safety for Australians. However, the Bill is not a narrow nor time-critical legislative intervention of the kind that would justify departure from consultation best practices. Rather, the broad ranging reforms including the introduction of a landmark 'digital duty of care' (**DDOC**) legislative framework and the repeal of the existing co-regulatory framework in relation to the online content scheme indeed warrants a much more extensive review, which cannot be completed in the short timeframe provided.

We further note that feedback is limited to written submissions only, and further limited to a five-page cap. To our understanding, there has been no effort to hold public roundtables or town halls to engage stakeholders for whom providing written submission is a high barrier to engagement with law reform processes. This is particularly the case for smaller ISPs whom IAA represents, that are often unable to provide formal written submissions due to their resource constraints. We also note that the exposure draft and consultation information has not been listed on the Department's consultation hub,[2] which we consider is likely to further obfuscate wide engagement.

Additionally, there has been no engagement of the Internet sector by online service class or category. Each of these industry categories has distinct technical and operational realities that warrant dedicated engagement to work through the specific issues and challenges arising from the Bill.

We therefore recommend the consultation period be extended by a minimum of 4 weeks. During which period, the Department should:

- **conduct online service category-specific engagement through roundtables or similar forums;**
- **list the exposure draft and consultation on the Department's official consultation hub; and**
- **commit to a further consultation opportunity, informed by matters raised during this consultation process before the Bill is introduced to Parliament.**

SCHEDULE 1 – NOTICES OF CERTAIN MATERIAL AND DISCLOSURE OF INFORMATION

We understand the proposals under this Schedule 1 are not targeted at the internet carriage service category. We support the distinction between the various online service categories and further support the recognition that ISPs by virtue of their provision of the internet carriage service, should not be subject to the obligations proposed under this Schedule. ISPs have little to no visibility or control over content shared across their networks, and therefore, should not be made responsible for such content. Due to the compressed consultation timeframe and limited relevance of this Schedule 1 to our members in their capacity as ISPs, we limit our comments on the reforms proposed under this Schedule.

However, we note that some of our members may still be subject to certain obligations by virtue of falling within the designated internet service – or other - category, where ISPs maintain ancillary websites, customer portals or mobile applications in connection with the provision of their internet carriage service.

We note that we have not, within the available timeframe, been able to fully assess the implications of these provisions on our members' ancillary offerings. We would welcome a further opportunity to engage with the Department on this matter.

SCHEDULE 2 – DIGITAL DUTY OF CARE

Online Service Scope

We understand that internet carriage services are proposed to fall within the scope of an 'online service', subject to the new DDOC framework. However, as noted above, we reiterate that an ISP has extremely limited

[2] https://www.infrastructure.gov.au/have-your-say.

visibility into, and no practical ability to moderate digital content carried across its network. We do not consider a duty framed around ensuring a safe *online* environment is a suitable conceptual fit for a service that operates in the network-layer.

We note that this limited control of an ISP is a position already recognised by the existing regulatory framework governing online safety, including the online codes and standards. While the internet carriage service category is recognised as forming part of the Internet ecosystem under the *Online Safety Act 2021* (**the OSA**), the applicable obligations are significantly lighter as set out in the applicable industry codes. This should be similarly reflected in the Bill. However as currently drafted, as providers of an online service, ISPs would face various obligations with respect to its DDOC, similar to providers of other online services despite the fundamentally different nature of internet carriage services. We understand that Government intends to replace the online codes and standards established under Division 7 of Part 9 of the OSA with the introduction of this DDOC framework. However, the DDOC fails to reflect the comparative lower level of risk posed by and control of ISPs in relation to the Internet carriage service.

IAA members, as smaller ISPs with limited resources are particularly disproportionately affected by the regulatory burdens that these obligations would impose, including (but not limited to) potentially being required to develop user empowerment tools, conducting annual risk assessments and establishing complaints and disputes resolution processes that meet further requirements. Due to the nature of internet carriage services, we do not consider the regulatory burden imposed by these obligations to be commensurate to the benefits for Australian end-users. This is not to say ISPs should not play a part in improving Australia's online environment, but this can be achieved via other avenues than prescriptive legislation such as voluntary industry codes, or more light touch regulatory obligations that are proportionate to and relevant to the nature of the service provided by ISPs rather than the full suite of the DDOC obligations set out in the Bill. We further note that ISPs are already subject to various consumer safeguard legislation which better addresses the kinds of risks under the control of an ISP. This also includes regulation of complaints handling processes, meaning the proposed regime would introduce a duplicative compliance obligation.

We appreciate that practicability has been considered with proposed s 26(1) specifying a person must ensure a safe online environment, only 'so far as is reasonably practicable'. However, we note that the application of other positive obligations such as the requirement to conduct annual risk assessments or having specific complaints and dispute resolution processes fail to reflect the proportionality principles. Furthermore, the list of factors that may be considered when assessing what is 'reasonably practicable' under proposed s 25H does not sufficiently address the technical realities that distinguish a network-layer connectivity service which constrains what is practicable for an ISP in ensuring a safe online environment.

IAA therefore recommends the removal of internet carriage services as an entire category of online service under proposed s 25A. However, if internet carriage services are to remain within scope for the purposes of the legislative framework:

- **internet carriage services should be exempted from the whole of Part 2, or at the least from proposed ss 26(3), 26A, 26B, and 26F in accordance with the proposed s 25A(3);**
- **the scope of the DDOC should be limited to services provided to individual end-users as opposed to services being provided as part of business-to-business dealings; and**
- **the proposed s 25H which sets out relevant matters affecting what is 'reasonably practicable' in relation to an entity's DDOC should be expanded to specify an entity's lack of content visibility, nature of service, and prevalence of encryption are relevant matters.**

Notwithstanding this position, IAA raises further concerns and makes recommendations in relation to specific provisions and obligations below.

Overlap with other online services

It is unclear how the obligations should apply to an ISP in respect of other ancillary services provided by the provider in relation to their internet carriage service. We note that most ISPs provide and operate ancillary services or products such as customer portals or mobile applications alongside, and to support the provision

of the internet carriage service. Given the broad definition of 'designated internet service', we consider it possible that these ancillary services will also be captured by the DDOC framework. **If so, we recommend that these be expressly carved out from the DDOC in accordance with proposed s 25A(3).**

Such portals are functionally distinct from typical designated internet services in that they do not enable interaction between end-users, nor present the exposure risks that we understand the DDOC framework intends to address. However, the compliance burden of distinctly capturing the portal will be disproportionate, particularly for smaller ISPs.

Exemption power under s 25A(3)

The exemption power should be expanded to include additional considerations as to when an exemption may be granted in accordance with s 25A(3) such as size and revenue thresholds. This is to ensure that smaller ISPs are afforded proportionality in respect of its DDOC.

We recommend the expansion of the exemption framework set out in ss 25A(3)-(5) to include an objective and tiered threshold for reduced or scaled obligations by subscriber number, or annual turnover.

Risk assessment

We are gravely concerned about the broad scope of the risk assessment obligation. The current drafting of proposed s 26A(2)(a)(i) requires an entity to identify "all reasonably foreseeable risks, ***including*** those relevant to the provider's digital duty of care" (emphasis added). This suggests that a risk assessment for the purposes of s 26A should cover all other reasonably foreseeable risks, regardless of whether or not such risks are related to online safety at all. This paragraph should be redrafted to narrow the scope of the risks to be covered by a risk assessment for the purposes of the DDOC framework so it is only related to online safety.

Delegated powers

We are concerned that a significant number of provisions in Schedule 2[3] allow the Minister or Commissioner to determine scope, impose new obligations, or compel action from providers, by legislative instrument or written notice without sufficient guardrails to ensure the proper exercise of these powers. **Given the practical consequences these powers can have on an entity, especially for resourced constrained smaller ISPs, we recommend:**

- **a consistent requirement to undertake consultation in relation to each of the relevant delegated powers – publicly or directly with the relevant entity, as applicable – with any consultation period to be held for at least 30 days, modelled after the consultation process requirements set out under s 47 of the OSA;**
- **the inclusion of parameters and considerations the Minister or Commissioner must have regard to prior to exercising its discretion.**

Additionally, several of these provisions[4] also express the scope of the Minister or Commissioner's powers as being "without limitation" or similarly unlimited, which we do not consider appropriate. **We recommend the Minister and Commissioner's delegated powers to be clearly and appropriately scoped.**

Privacy Act Amendments

We are concerned about the implications of the research and data access scheme under proposed Part 14 and the proposed addition of the Commissioner as an 'enforcement body' for the purposes of the *Privacy Act 1988* (**Privacy Act**). Noting ISPs already operate under complex and extensive data-retention and disclosure obligations under the *Telecommunications (Interception and Access) Act 1979* and the Privacy Act, we have not been able to fully assess the privacy impacts of the proposed reforms for end users, nor the compliance implications for ISPs due to time constraints.

[3] Proposed ss 26A(2)(f), 25B(2), 25G(2), 26(4), 26A(4), 26F(3), 192C(3), 192M(1) and (3), 199, and 229A(2).
[4] Proposed ss 192D(1), 192M(2) and (3), 205B(2), 205C(3) and 205K(1)-(2).

Commencement Timeframe

We understand the Exposure Draft proposes for DDOC obligations under this Part 2 to commence 12 months following Royal Assent. We submit that this commencement timeframe is far too short, and does not appropriately reflect the operational realities of particularly smaller ISPs with respect to new regulation.

Given the scale of the new compliance obligations, we recommend that the proposed commencement timeframe be extended to 18 months following Royal Assent. Furthermore, we recommend a staged commencement timeframe based on the online service category, and size and/or revenue thresholds. We consider this more appropriate to reflect the comparatively low level of risk that smaller ISPs pose to the online safety of Australians.

SCHEDULE 3 – REPEAL OF ONLINE CONTENT SCHEME INDUSTRY CODES AND STANDARDS

We understand that the existing co-regulatory framework under Division 7 of Part 9 of the OSA is to be replaced by the proposed DDOC framework. In principle, we appreciate the legislative intent to repeal the codes and standards so as to prevent duplicative online safety frameworks in the event the DDOC is established. However, we submit that the DDOC framework could be established under a co-regulatory model instead of the prescriptive framework as currently drafted. Co-regulation has the benefit of being designed by the industry participants who have the technical and operational expertise to ensure effective and practicable regulation.

IAA reiterates our concern about the lack of engagement with the sector in relation to this proposal, and it is unclear why a co-regulatory model was deemed unfit to pursue more stringent DDOC objectives. This is highly concerning given that many of these codes and standards were only reviewed, consulted on and registered very recently. The first set of industry codes addressing class 1A and class 1B illegal material (**Phase 1 Codes**) only commenced in late 2023, while codes addressing class 1C and class 2 material only came into effect in December 2025. Furthermore, review of the Phase 1 Codes is currently ongoing, with public consultations only closing in July 2026. There was no indication by the Commissioner nor Minister that this co-regulatory approach has been inadequate. Under the OSA, the Commissioner has, and indeed has previously exercised powers to reject an industry Code, where a Standard was deemed necessary to ensure effective regulation over a segment of the Internet sector.

Furthermore, we take this opportunity to reiterate points raised in respect of the consultation approach, and the broad scope of the DDOC, particularly in relation to providers of the Internet carriage service. **In the event that the DDOC framework is established, we support the repeal of the industry codes and standards. However, we maintain our position that the DDOC should be amended so that ISPs are only subject to a lighter set of obligations, proportionate to the nature of the Internet carriage service in the context of online safety. Furthermore, IAA respectfully requests greater engagement with the sector to consult on the relevant obligations for ISPs under the proposed DDOC, and the feasibility of a co-regulatory framework for the DDOC.**

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the *Online Safety Amendment (Digital Duty of Care) Bill 2026*. We take this opportunity to reiterate our commitment to working with the Government in the development of a fit-for-purpose legislative framework that will ensure the safety of Australian end-users. To that end, we respectfully request for further consultation on the Bill to ensure the legislation will champion online safety while not unduly burdening industry. We look forward to working with the Government, regulators, industry, and other stakeholders to develop an effective regulatory framework that is proportionate, practicable and reflective of the Internet ecosystem it seeks to regulate.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (**WAIA**), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our public policy work is guided by the following principles:

We stand for an internet for the common good

We stand for an open internet platform

We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.