Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

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

Re: Digital Duty of Care

5 December 2025

TABLE OF CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

1.1 The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

1.2 For questions on this submission, please contact Deputy CEO Christiane Gillespie-Jones, c.gillespiejones@austelco.org.au.

1.3 This is submission is provided on behalf of our carrier and carriage service provider (C/CSP) members.

2. INTRODUCTION

2.1 The ATA welcomes the opportunity to provide a submission to the Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (Department) in response to its public survey on the proposed digital duty of care (DOC) under Australia's *Online Safety Act 2021* (OSA),

2.2 The ATA supports the overall objective to protect Australians, especially the most vulnerable online participants and children, from harmful online content and to promote online safety more broadly.

2.3 In addition to member-specific initiatives to enhance user safety and promote online safety, our members comply with the requirements of the OSA and its subordinate instruments, i.e. the

a) Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) (Class 1 Codes),

b) Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) (Class 2 Codes),

c) Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024 (DIS Standard),

d) Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 (RES Standard), and

e) Online Safety (Basic Online Safety Expectations) Determination 2022 (BOSE)

2.4 Against this background of a complex regulatory environment, it would be helpful to understand whether it is proposed that the DOC operate in parallel to the existing OSA and its subordinate instruments, or whether it is intended to revise the OSA in line with the recommendations of the Report of the *Statutory Review of the Online Safety Act 2021* conducted by Delia Rickard PSM (Rickard Report) and establish the DOC as part of a revised OSA.

2.5 The current regulator landscape in relation to online safety is already complex, confusing and creates significant compliance challenges for our members. We are very concerned that the introduction of a DOC to operate concurrently with the existing OSA and subordinate instruments (i.e., sitting 'over the top') would create even further complexities for regulated entities. It is also likely that doing so would add complexity and limitations to the revision of the OSA, i.e. without a very clear path and understanding of a future, revised OSA and its instruments, there is a risk that a DOC developed 'over the top' at this stage will limit the range of options further down the track.

2.6 Given the existing OSA and subordinate instruments, it is not quite clear what 'gap' the proposed DOC is

seeking to fill. Therefore, it would be helpful to gain a better understanding of the additional harms or protections that the government is striving to address in order to form a view on how to best introduce a DOC.

2.7 In the absence of further information on the interaction between the OSA and the DOC, but highlighting our concern above, we will assume that the DOC, at least initially, is intended to operate concurrently with the existing OSA and its subordinate instruments listed above.

2.8 We support the objective of gathering feedback from the public on some of the basic premises of the DOC through an online survey.

2.9 While we also completed the online survey, we do not believe that the survey format provides sufficient opportunity for entities potentially regulated under a new DOC to submit their feedback with the requisite detail and granularity.

Given it is unclear whether and, if so, how and when further consultation with our sector would occur, we take this opportunity to comment on the proposal, noting that more detail on the planned DOC and the proposed consultation process would be welcome.

2.10 Therefore, we urge the Department to publish an Position Paper with concrete proposals and alternatives for the various aspects of the DOC, for example, the interaction with other regulation, scope of services covered, scope of material and harms covered, risk focus, and when in-scope providers would be deemed compliant with the DOC etc. Subsequent further consultation with relevant stakeholders could be used to guide the development of an exposure draft of the legislation for public consultation.

2.11 Only carrier and carriage service provider (C/CSP) members participated in the development of this submission. However, we note that other non-C/CSP members have also highlighted their concern with the consultation process, as apparent so far.

Individual members may make additional submissions.

3. PRINCIPLES FOR A DUTY OF CARE

3.1 In our view, the DOC ought to operate as a duty on certain providers to ensure that they take steps/care to protect vulnerable online users from online harms, including by limiting access and distribution of harmful content.

3.2 The online environment consists of a plethora of different types of services and organisations. The OSA attempted to categorise those service types into eight different online sections. Unfortunately, in doing so, the OSA fails to apply a risk-based approach to online services and also considers technical capabilities and legal constraints to a limited or insufficient extent. For example, with very limited exceptions, C/CSPs are not permitted to intercept communications or to analyse their content for harmful material without a warrant.

3.3 These deficiencies of the OSA have already led to substantial complexities and, as we argued in previous submissions, over-regulation in that services are burdened with regulatory requirements despite having a very low risk profile for causing online harms and/or no visibility or control over the content deemed to be harmful.

3.4 Consequently, the proposed DOC ought not to replicate the previously chosen approach. Instead, at a minimum, all of the following threshold criteria ought to be satisfied to bring a service in scope for the DOC:

a) Significant risk of harm emanating from access to and distribution of regulated (harmful) content through the service;

b) Visibility and editorial or other control over the content or its distribution; and

c) No legal prohibitions to obtain visibility of the content and/or to exert control over the content

3.5 We also highlight that the term 'digital duty of care' does not appropriately characterise what we believe is the intention of the proposed DOC. Instead, and in line with the language used in the Rickard Review, a DOC of online services appears to be what ought to be contemplated.

While the term 'online' has not been defined in the OSA (nor in the Rickard Report), we argue that the common meaning of the term implies transmission of material via the internet and/or for the purpose of accessing the material on the internet. At the highest level, this appears to be the intended scope for the DOC, noting that only those online services that meet the respective threshold criteria ought to be in scope for an online DOC.

The term 'digital' is broader, and could include material made available in electronic form or via electronic means but without the use of/access to the internet.

4. THE ROLE OF C/CSP SERVICES

4.1 C/CSP members provide the following services that are currently in scope, or could be argued of being in scope, of the OSA:

a) SMS/MMS, i.e. 'traditional' texts and multimedia messages sent by users by means of a carriage service. (For iOS users, SMS appear as green messages.) Note that these services do not include other messaging services that are provided 'over the top' (OTT), such as WhatsApp or iMessage or other Rich Communication Services (RCS). (For iOS users, iMessages appear as blue messages.);

b) Email services provided as part of a contract for carriage services, e.g. Optus Webmail or Bigpond. Note that these services do not include email services that run 'over the top' by means of a carriage service, e.g. they do not include gmail, Hotmail etc.;

c) Internet carriage services (ICS), i.e. access to and connectivity via the internet. Note that these services do not include any services that use internet connectivity to be delivered;

d) Certain business/enterprise services;

e) Certain apps or websites for the management of the C/CSP services; and

f) Resale of services (e.g. entertainment services) and equipment.

SMS/MMS

4.2 SMS/MMS are relevant electronic services within the meaning of the OSA and could, as such, potentially be considered in scope of a DOC.

4.3 The inclusion of SMS/MMS in the definition of relevant electronic services is unfortunate and, in our view, inappropriate. The inclusion has led to substantial uncertainty and complexities for the drafting of, and compliance with, regulatory instruments subordinate to the OSA, e.g. the registered Class 1 and Class 2 Codes, the RES Standard, and the BOSE. In fact, even the OSA itself struggles with the inclusion of SMS/MMS and contains provisions in relation to relevant electronic services (e.g. section 110 and section 114, removal notices) that are unenforceable as providers of SMS/MMS cannot comply with them as they are unable to remove content.

4.4 These complexities and compliance issues arise due to an unfortunate conflation of telephony communications services, i.e. services that are transmitted via carrier telephony networks (e.g. SMS/MMS over 4G/5G)) and services that enable such communication online, i.e. over the internet.

4.5 The issues also arise as the OSA fails to apply an appropriate risk lens and/or insufficiently considers technical and legal limitations of carriage services.

SMS/MMS are not online services

4.6 The Rickard Report recognises these issues and recommends (Recommendation 2) that:

> *"current definitions of the online industry sections should be simplified to online platforms, online search and app distribution services, online infrastructure services and equipment and operating system services. These should be included in the Act to better reflect online safety risks and future proof the Act."*[1]

and proposes a definition of online platforms as

> *"Online platforms*
>
> *This first category includes services where the majority of harmful content or conduct occurs. It would capture those services that enable:*
>
> - *Online social interaction or messaging; and/or*
> - *The provision of online content – including content that is user-generated, directly provided or generated by a service, or recommended by a service (such as by an algorithm)."*[2] [emphasis added]

4.7 The recommendation and proposed definition make clear that only online services ought to be the within scope of the definition of online platforms (which includes, albeit not exhaustively as we argue, relevant electronic services).

4.8 While the term 'online' has not been defined in the OSA (nor in the Rickard Report), we argue that the common meaning of the term implies transmission of material via the internet and/or for the purpose of accessing the material on the internet (as opposed to the term 'digital', which is broader, and could include material made available in electronic form or via electronic means but without the use of/access to the internet)

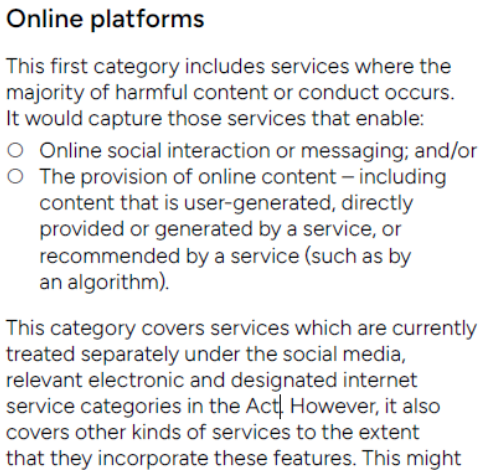
4.9 SMS/MMS are not online services. SMS/MMS are telephony services which are transmitted via mobile networks but do not use or make the transmitted material accessible on the internet.

SMS/MMS do not meet the risk threshold

4.10 In addition to existing precedents that have deliberately or inadvertently included C/CSP services into the scope of online safety regulation, we note with great concern that the Rickard Report also does not appear to address this issue. To the contrary, it appears to aggravate our concerns given the far-reaching additional requirements (e.g. DOC) that are to be placed on services that are, or ought to be, the actual target of the DOC and revised OSA.

4.11 The Rickard Report (p. 40) proposes four new online sections:

[1] Delia Rickard. 2025 (p. 21). *Report of the Statutory Review of the Online Safety Act 2021*
[2] Ibid (p.40)



Online platforms

This first category includes services where the majority of harmful content or conduct occurs. It would capture those services that enable:

- Online social interaction or messaging; and/or
- The provision of online content – including content that is user-generated, directly provided or generated by a service, or recommended by a service (such as by an algorithm).

This category covers services which are currently treated separately under the social media, relevant electronic and designated internet service categories in the Act. However, it also covers other kinds of services to the extent that they incorporate these features. This might

4.12 The above highlights the need to more clearly differentiate within proposed categories, in particular messaging services, and to clarify the role, risk profile, harms vector and capabilities of such services.

4.13 While the Rickard Report states an intention to apply a risk-based lens to the future OSA, it also appears to conflate 'reach' and 'risk'. This is concerning given that C/CSP services have an almost 100% 'reach' amongst Australians but only pose very limited risk.

4.14 We argue that SMS/MMS also do not meet the risk threshold, i.e. the likelihood that these services are being used to access or distribute the harmful content is limited. Where such distribution may occur, the distribution is usually through one-to-one communication as opposed to one-to-many group chats of OTT messaging services.

SMS/MMS do not have visibility of and control over content

4.15 C/CSPs do not have visibility of the content of communications and are prohibited by the provisions of the Part 13 of the *Telecommunications Act 1997* from intercepting communications without an appropriately authorised warrant.

4.16 C/CSPs are also technically unable to remove content from an SMS/MMS.

4.17 We note that the analysis and blocking of scam messages by C/CSPs is technically not comparable to the inspection and analysis that would be required to assess SMS/MMS for harmful content. We also highlight that the former (scam analysis) is permitted by statute (within strict confines) while the inspection of SMS/MMS for other purposes is not.

4.18 Against the background of

- SMS/MMS not being online services (and, consequently, not being in the envisaged scope of the OSA or a DOC);
- the low risk that emanates from SMS/MMS; and
- the lack of visibility of and control over content being transmitted by SMS/MMS, and
- the legal limitations associated with the inspection of and interference with communications,

we submit that SMS/MMS ought to be specified as exempt from the scope of the DOC (and a revised OSA).

EMAIL SERVICES

4.19 Email services are relevant electronic services within the meaning of the OSA and could, as such, potentially be considered in scope of a DOC.

4.20 The email services offered by C/CSPs are different to over-the-top (OTT) email services, such as gmail, Hotmail or other email services that are not offered by C/CSPs but travel across the infrastructure provided by C/CSPs in their capacity as internet carriage service providers.

4.21 Some C/CSPs provide residential consumer email services as part of fixed-line internet carriage services that they offer.[3] Fixed-line internet carriage services are not being offered to children, arguably one of the most vulnerable user groups.

4.22 Email services provided by C/CSPs (as opposed to those offered OTT or by academic institutions) are also not likely to be accessed by children. This is because the service, i.e. the email address, is usually coupled to the name of the contracting adult. C/CSP email services are typically used by an older demographic.

4.23 Importantly, the share of C/CSP email services in the overall residential consumer (i.e. not business/enterprise) email services market is very small. Many large internet carriage service providers have phased out their offerings or have announced their intention to do so.

4.24 Therefore, C/CSP email services do not meet the risk threshold for a DOC to apply.

4.25 Similar arguments with respect to a lacking visibility of, control over and legal limitations in relation to content contained in emails apply as for SMS/MMS above.

4.26 It should be noted that tools to detect spam messages are technically not suited to detect specific types of content. Instead such tools screen for certain technical characteristics or patterns that suggest that an email may be spam. Some external, specialised providers of filtering software may be able to filter for some types of content with varying degrees of success.

4.27 **Consequently, we submit that email services provided by C/CSPs ought to be specified as exempt from the scope of the DOC (and the revised OSA).**

INTERNET CARRIAGE SERVICES

4.28 ICS are regulated as one of the eight online sections in the OSA and could, as such, potentially be considered in scope of a DOC.

4.29 The Rickard Review envisages ICS form part of a newly defined category of 'online infrastructure services' (reproduced below). We agree with that classification on the basis that ICS only provide access and connectivity to the internet (often referred to as 'the dumb pipe'). These services are distinct from any services delivered using the internet or are being facilitated by use of the internet.

[3] Some C/CSPs may also permit customers to maintain an email service even if they no longer subscribe to a fixed-line internet carriage service provided by the C/CSP.

Online infrastructure services

Similarly, services in this third category would be expected to take actions regarding illegal content when it is reported to them, and to comply with lawful requests and notices from the regulator. All online services depend upon 'infrastructure' services to allow them to be securely located and accessed online, including:

- Hosting services, which provide 'real-estate' (both physical and virtual) for online services – such as the storage of a service's data on physical servers
- Domain name services and registrars, which provide services with an 'address' – enabling users to easily access the service
- Internet service providers, which provide a 'transport' service to users, allowing them to access services online; and
- Other services providing infrastructure support and security. This could include services providing content delivery network services, virtual private networks, distributed denial-of-service (DDoS) attack protection and other cybersecurity support.

Services should undertake proactive and ex ante steps where possible, but may not always be able to proactively monitor or moderate the content or activity on services for which they provide infrastructure support. However, once made aware of illegal or seriously harmful content and activity on a service they enable access to, they are generally capable of removing this material (in the case of hosts) or blocking access to the service (in the case of internet service providers and domain name system services). It is important that these services are defined in the Act, to cover all infrastructures services to the extent they support services which are provided to end-users in Australia. This would cover, for example, hosting service providers which host services provided to end-users in Australia, regardless of where the hosting service is located.

4.30 We also agree with the principle that online infrastructure services, including ICS, only ought to take action regarding illegal content, i.e. not all harmful content, upon an appropriately authorised request from a regulator or other lawful request.

4.31 ICS do not have any visibility of the content that travels across their networks and they are prohibited from intercepting such traffic without a lawful warrant, i.e. ICS neither have visibility nor control over specific pieces of content.

4.32 As ICS are unable to remove content, the only alternative action lies in the blocking of entire domains through the ICS, i.e. ICS cannot block individual sub-pages, posts, or pieces of user-generated content on a platform, but instead can only block access (to all users) to the domain that hosts content that is deemed illegal. For example, ICS cannot block a specific user's Facebook page but instead would need to block all of Facebook.

4.33 It is worth noting that ICS already comply with blocking requests under different legislative requirements, including section 313 of the *Telecommunications Act 1997*, Part 8 of the OSA, section 115A of the *Copyright Act 1968*, and section 127A of the *Tertiary Education Quality and Standards Agency Act 2011*.

4.34 ICS also comply with additional requirements under the Class 1 and Class 2 Codes. Such requirements include the promotion of filtering products and education of users how to stay safe online.

4.35 **Consequently, we argue that ICS ought not be considered in scope for the DOC (and the revised OSA). If they were considered in scope, compliance with appropriately authorised blocking requests ought to constitute a fulfilment of the DOC.**

BUSINESS / ENTERPRISE SERVICES

4.36 Some services that C/CSPs provide to enterprises may be considered social media services, relevant electronic services or designated internet services within the meaning of the OSA and could, as such, potentially be considered in scope of a DOC.

4.37 We believe that any services provided by C/CSPs to enterprises (e.g. business-focused unified communications and cloud services and business email platforms for resale to enterprise customers) do not meet the risk threshold (and potentially also not the other thresholds of visibility/control, legal limitations) for inclusion in a DOC.

4.38 **Consequently, we submit that business and enterprise services provided by C/CSPs ought to be specified as exempt from the scope of the DOC (and the revised OSA)**

APPS OR WEBSITES FOR THE MANAGEMENT OF C/CSP SERVICES

4.39 C/CSPs may provide websites or apps designed to allow customers to manage their services, including prepaid services, which may be purchased by children. Such services are designated internet services within the meaning of the OSA.

4.40 These services also do not meet the risk threshold (and potentially also not the other thresholds of visibility/control, legal limitations) for inclusion in the DOC.

4.41 **We submit that the use of such services for the purposes of facilitating telephony services equally ought to be specified as exempt from the scope of the DOC (and a revised OSA) as they are directly related to relevant telephony services that ought to be specified as exempt.**

RESALE OF SERVICES AND EQUIPMENT

4.42 C/CSPs may resell social media services, relevant electronic services, or designated internet services, for example gaming subscriptions, or entertainment services, such as television and music streaming services (where these services contain social features which enable users to post or share content like shared playlists, group watching features, or content recommendations).

4.43 C/CSPs may also resell equipment and, depending on definitional aspects, may be considered 'manufacturers' of equipment where they re-brand equipment but do not take part in actual manufacturing (in the ordinary use of the term) of the equipment.

4.44 Under these arrangements, C/CSPs have limited control over the provision of the service, which is managed by the relevant provider. Typically, the role of C/CSPs in these services is limited to facilitating access to and billing of those services. In the case of the resale or 'manufacturing' of equipment, C/CSPs have no control over the equipment. Instead, the control either rests with the actual manufacturer of the equipment or, most likely, with the provider of the operating system of the equipment.

4.45 **We submit that the resale of such services by C/CSPs ought to be specified as exempt from the scope of the DOC. We also submit that the resale and 'manufacturing' of equipment in cases as described above ought to be excluded from the scope of the DOC. Instead, any DOC ought to be placed, if at all, on the controllers of the operating system.**

5. INTERNATIONAL APPROACHES TO TELECOMMUNCIATIONS SERVICES

5.1 Australia is an active participant in a global economy. Therefore, it will be useful to consider international approaches to online safety most notably those embedded in the United Kingdom's (UK) *Online Safety Act 2023*, which contains a statutory DOC (amongst other additional safeguards).

5.2 We acknowledge Australia's extensive cooperation with the UK in online-safety matters and regard the UK *Online Safety Act 2023* as a robust regulatory framework that targets the service categories where the greatest risks to adults and children materialise. Our understanding is that the UK adopts a risk-graduated model, in which user-to-user services and regulated search services are treated as highest risk, while telecommunications services fall outside the regime's scope.

5.3 We recognise that the government is considering reforms aligned with elements of the UK model, including

the introduction of a DOC. The effectiveness and proportionality of such reforms will depend on a clear recognition that different service types present fundamentally different risk levels. To ensure coherence and to reflect practices in comparable jurisdictions, the DOC (and a revised OSA) should focus on those service categories most closely associated with online harms.

5.4 **We highlight that under the UK *Online Safety Act 2023*, telecommunications services – including SMS/MMS, email services, telephony, and ICS – are expressly excluded from the category of 'high-risk' services and the DOC.**

5.5 **Canada's *Online Harms Bill* (C-63) similarly omits telecommunications services** and focuses instead on platforms where harmful content proliferates most readily.

5.6 **Under the EU *Digital Services Act 2022*, telecommunications services fall into the lowest regulatory tier**, i.e. 'intermediary services'. These services must comply with obligations appropriate to their limited role, such as transparency reporting, enforcement of terms of service, cooperation with regulators for content removal/blocking, and provision of user-complaints mechanisms. Higher-risk categories (hosting services, online platforms, and very large online platforms) are subject to more stringent obligations.

5.7 **We therefore consider that the DOC and a revised OSA would more effectively reduce online harms if it mirrored the UK, EU, and Canadian approaches by targeting high-risk service types. This could be achieved either by removing telecommunications services from scope altogether (our preferred approach), or by designating them as the lowest-risk tier with obligations calibrated to their limited involvement in user-facing content controls.** Such a recalibration would reduce regulatory duplication and enable a significant rationalisation of the currently complex suite of subordinate instruments.

Ends

Australian
Telecommunications
Alliance

Level 25 / 100 Mount Street
North Sydney NSW 2060

T 02 9959 9111
E info@austelco.org.au
W austelco.org.au

ABN 56 078 026 507