Submission from Telstra Limited

on the

Issues Paper – Statutory Review of the Online Safety Act 2021

5 July 2024

Contents

Introductory comments

1. Thank you for the opportunity to respond to the Issues Paper re the Statutory Review of the Online Safety Act 2021 (Cth) (the **Act**), and for the time granted to us for submission of our comments. We have also contributed to the submission made by the Communications Alliance (noting our views on certain issues may differ).

2. As a leading Australian telecommunications and technology provider, we work continuously to help keep Australians safe online. We see this as a key part of our purpose of providing a connected future that enables everyone to thrive. Like the Australian Government, we recognise that Australians want stronger protections for online activities, especially for children, and that industry needs to do more to ensure online safety, including in emerging technologies.

3. In this spirit, we comment below on those issues which we believe would enable the Act to focus more effectively on safeguarding Australians from online harms and promoting safer, more positive online experiences. Our comments arise from our industry leadership in online safety and digital wellbeing initiatives, our position in the industry as a telecommunications provider, and based on the lower risk of harm from the services we provide to our customers.

4. Importantly, the role of telecommunications services in the "connectivity stack" means that our connectivity services do not involve user-generated content in the same way as higher risk and online platform services, and are regulated under separate, telecommunications specific legislation with extensive consumer protections. The overseas experience demonstrates that online harms are not reduced when regulating telecommunications services in the same way as content platforms.

The scope and objects of the Act

5. The issues paper asks whether the current objects of the Act should be expanded. We strongly support the overall objects of the Act (ie improving/promoting the online safety of Australians), and believe that they remain current. We see an opportunity to expand these objects in line with our comments below to reduce the risk of online harm to children and all Australians through a sharper focus on higher risk services.

The UK and other comparable jurisdictions

6. The issues paper asks whether the Act should incorporate any international approaches, particularly from the United Kingdom's (**UK**) Online Safety Act[1], which includes a statutory duty of care, a "best interests of the child" principle, safety by design and stronger enforcement powers. We acknowledge Australia's extensive collaboration with the UK in online safety, and see the UK Online Safety Act as a strong online safety framework which focuses on regulating the services where children and adults can experience the highest risks of harm. We understand it does so by adopting a regulatory approach based on the risk represented by various types of services (with user-to-user platforms and regulated search services being regarded as highest risk, and telecommunications services being out of scope).

[1] *Online Safety Act 2023* (UK).

7. In terms of its regulatory approach, and by contrast with other jurisdictions like the UK, European Union (**EU**) and Canada, the Act, particularly in relation to Part 9 'the Online Content Scheme', focuses on certain types of material by classification (eg Class 1 or Class 2 material). In doing so, it is linked to the Australian classification scheme[2]. As a result, the Act (and subordinate instruments made under it, including the Industry Standards), adopts a fairly complex and inflexible approach to regulating online harms, with core obligations arising from the classification rating of material rather than the fundamental risk of harms inherent in certain service types.

8. We see this as resulting in an undue complexity in the volume and application of obligations (ie with obligations under the Act, separate industry codes required for different classes of material and industries, and supplementary regulation in the form of the Industry Standards BOSE Determination). There is overlap between some of these instruments, and instruments apply to all industry segments and services even where there is limited relevance or risk given the service type. For example:

    - both the *Online Safety (Designated Internet Services Standard – Class 1A and 1B Material) Industry Standard* 2024 (**DIS Standard**) and *Online Safety (Basic Online Safety Expectations) Determination* 2024 (**BOSE Determination**) regulate generative AI in different ways, and
    - the DIS Standard applies to all websites (irrespective of their use and purpose), with complex risk assessment and obligation matrices then required to work out how to apply obligations where they're fundamentally not needed.

9. We can see the review of the Act is considering a number of reforms consistent with the UK Online Safety Act, including the introduction of a duty of care and an industry funding model. We comment on some aspects of these issues below. If these elements are to be introduced, to be part of an effective package of legislation ameliorating online harms, and proportionate to harm, they should operate together with a recognition that different service types inherently pose a different level of risk of harm to users. To achieve this, we consider that the Act should focus key obligations on those service types which generate the most risk. This would be consistent with equivalent legislation in comparable jurisdictions.[3]

10. We note that telecommunications services (including email, SMS, MMS, telephone services and underlying connectivity) are not within the scope of the 'high risk' services regulated under the UK Online Safety Act[4]. The Canadian Online Harms Bill also excludes telecommunications services from scope, focusing on the services where harmful content is most commonly found, ie online platforms.[5]

---

[2] *Classification (Publications, Films and Computer Games) Act1995* (Cth).
[3] *Online Safety Act 2023* (UK); European Union, The Digital Service Act', *Strategy and Policy* (Web Page) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>. '); Online Harms Bill C-63 2024 (Can); *Harmful Digital Communications Act 2015* (NZ).
[4] *Online Safety Act 2023* (UK) Sch 1, Part 1 s 1-5.
[5] Online Harms Bill C-63 2024 (Can) Part 1 s2; see definitions of "regulated service", "social media service".

12. The EU adopts a four-tiered approach in its Digital Services Act[6], with telecommunications forming part of the lowest tier "intermediary services" – see Figure 1[7] below. Intermediary services are required to meet online safety obligations appropriate to their role including transparency reporting, enforcing terms of use, cooperating with enforcement agencies to remove content, and providing support (eg an avenue for complaints). Higher levels of regulation are applied to very large online platforms, online platforms, and hosting services.

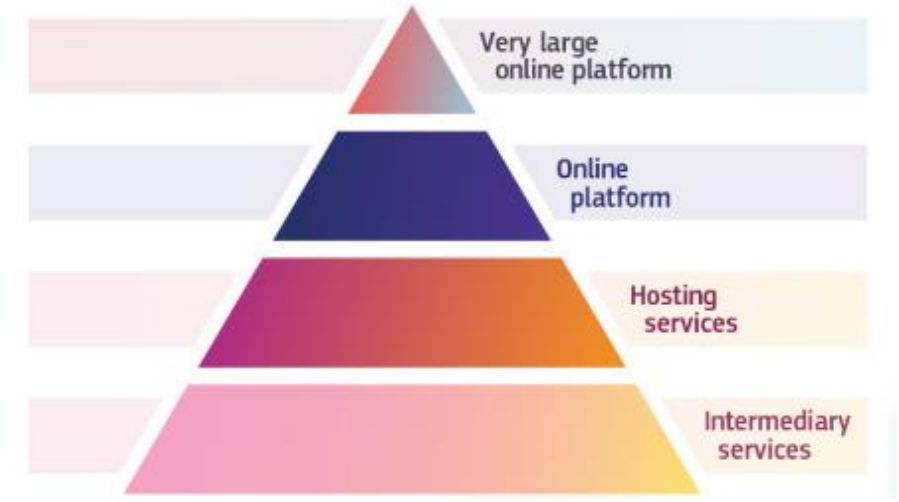

Figure 1: The EU online safety regulatory model

13. The predecessor UK online safety legislation[8] included telecommunications services within the scope of core online safety obligations, however, these services are now excluded under the UK Online Safety Act. We understand that this is attributable to the recognition of the limited role of these services in online safety risk, including the fact that telecommunication services:

    - do not involve user-generated content in the same way as online platforms, and
    - are regulated under separate, specific legislation with extensive consumer protection obligations (which is not the case for content platforms).

    Fundamentally, the UK regulatory experience demonstrates that telecommunications services are not the source of, nor the best vehicle to remedy, online harms (a position reflected in the Canadian and European online safety legislation).

14. We strongly believe that the Act would be more effective in ameliorating online harms if it adopted a similar approach to the UK and other jurisdictions, by focusing on high risk service types, including either taking telecommunications services out of scope (as do the UK and Canada) or treating them as forming the lowest risk tier of services reflecting their limited role in user-facing and content safety controls (as does the EU). Among other things, refocusing the Act could enable significant streamlining of what is currently a complex set of subordinate instruments.

---

[6] *Digital Services Act* 2024 (EU), see definition for 'Intermediary Services'; European Commission, 'The Digital Services Act' accessed 28th June 2024 at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en; See, eg European Parliament, EU Legislation in Progress Briefing, Digital Services Act, November 2022: "Second, the limited liability regime exempts 'online Intermediaries' from liability for the content they convey and host (ie the 'safe harbour' principle) if they fulfil certain conditions." p.2.

[7] Ibid.

[8] *Digital Economy Act 2017* (UK).

15. There remains an important role for telecommunications services in online safety, and we will keep fulfilling that role because it's the right thing to do as a responsible business and for our customers. We discuss that role in more detail below.

The role of telecommunications providers

16. The issues paper asks whether regulatory obligations should depend on a service provider's risk profile or their reach. We see online safety as a shared responsibility, with individuals, government agencies, law enforcement and various segments of industry including telecommunications providers each having a role. As well as meeting our fundamental obligation to deliver reliable, secure connectivity, telecommunications providers have a key online safety role, including in:
    - providing reasonable assistance to national security and law enforcement agencies
    - fulfilling our interception, blocking and security obligations, and
    - assisting our end user customers, including by providing avenues for reporting harmful and unlawful content[9], complaints handling and enforcing terms of use, education, and access to third party safety products.
17. While we are a conduit for services to be provided, our role in the "connectivity stack" (ie the technologies that enable users to interact online, see Figure 2 below) means that we do not create, control or have visibility of user transmitted content or the applications/platforms on which it is disseminated.

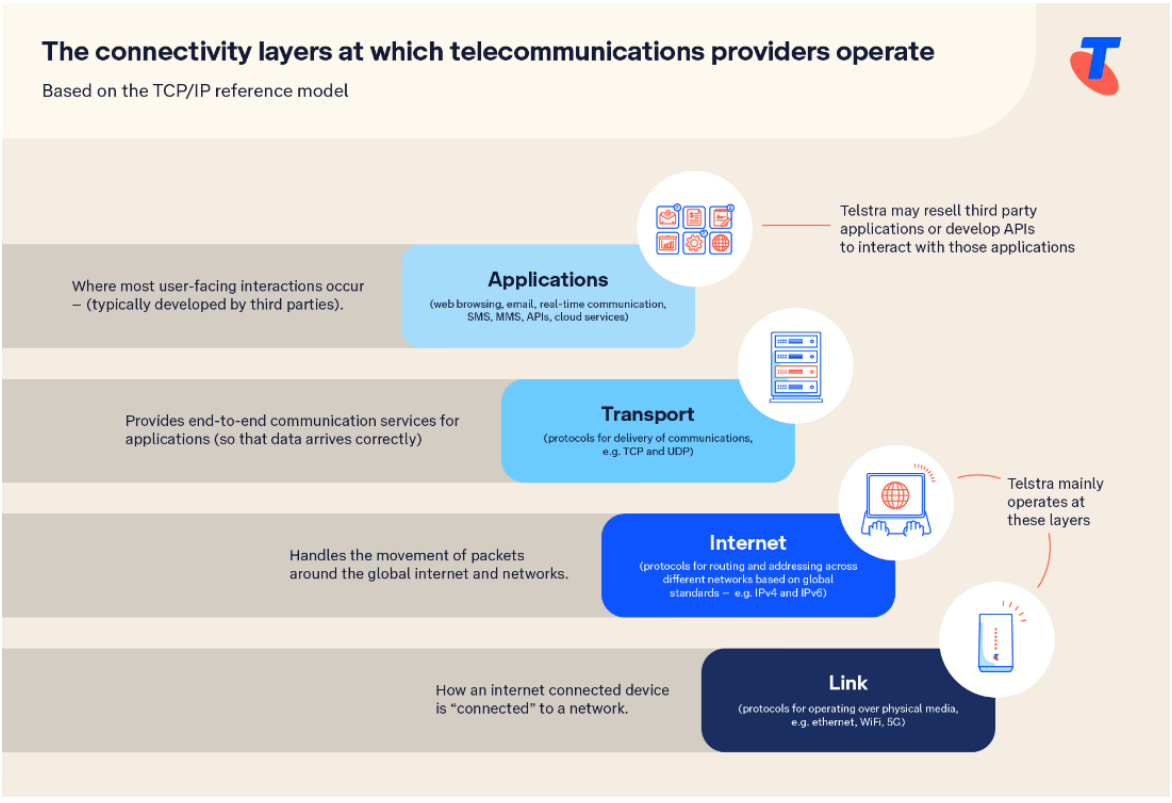

Figure 2: The connectivity stack

[9] See *Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard* 2024 s24-31 (RES Standard); *Online Safety (Designated Internet Services Standard – Class 1A and 1B Material) Industry Standard* 2024 (DIS Standard) s25-30; RES Standard; See also *Harmful Digital Communications Act 2015* (NZ), which focuses on user complaints about breaches of the digital communication principles.

18. As Figure 2 illustrates, the telecommunications services which we provide are located 'underneath' the application and user interface technology with which users interact, and which they use to access and share content. We generally do not create the applications which users access (although we sometimes re-sell them)[10].

19. The options wholly within our control in relation to content and applications are fairly limited 'blunt instruments' – we can block user access to domains which host/transmit harmful or unlawful content on request (on a whole-of-domain basis), and we can cease supplying third party applications (cutting off user access to products). We can also seek to influence application vendors in relation to particular safety features or content outcomes, although we note that this opportunity is limited given the global market for applications and global standards for connectivity and routing of data[11].

20. We would like to again stress that telecommunications providers can and should enhance online safety by implementing safeguards appropriate to their role in communications and the online environment (which include the measures we have set out at paragraph 16). Where we do not own the end user relationship (eg for enterprise or wholesale services), we can support our customers with taking action.

21. Applying regulation to all industries, service types or provider types does not make for effective online safety regulation in practice because it ignores the role, scope, capacity and technical functionality of telecommunications services. In doing so, it creates burdensome and ineffective regulation, driving regulatory complexity, ambiguity and compliance uncertainty. Apart from avoiding ineffective and burdensome regulation of providers of low risk and irrelevant services, we consider that careful exclusion of telecommunications and other low risk services would also avoid the need to build in exemptions to specific obligations. Our experience has been that when obligations apply 'across the board' on a service-neutral basis, this has the undesirable effect of requiring exemptions to be built in when the obligations don't fit, leading to 'dilution' of obligations and the likelihood of reduced enforceability. For example, the *Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard* 2024 (**RES Standard**) now contains a technical feasibility and 'reasonable practicability' exemption to the obligation to detect/delete certain material, which we understand was (among other reasons) included because ISPs advised they would not be able to comply with the detect/delete obligation as drafted for ISP email platforms.[12]

22. Taking all of this into account, and with a view to the effectiveness of online safety regulation and telecommunications providers maintaining an appropriate, ongoing role in online safety, if telecommunications services are not taken out of scope (as in the UK and Canada) we strongly recommend the Review specifically consider exempting telecommunications providers from the application of content management and user-facing obligations when they're providing telecommunications

[10] Bigpond email is a third-party product typically accessed via third party interfaces (eg email applications, web browsers), which is re-sold by Telstra. SMS and MMS are also accessed using third party device applications.
[11] We provided the example of ISP email platforms during consultation on the RES Standard. As indicated in the footnote above, ISP email services are typically acquired from platform vendors. There is a limited ability to influence technology development as the vendor operates a global roadmap for feature development which is not necessarily responsive to Australian regulatory developments or requests from individual ISPs.
[12] RES Standard s12, s19(1), 20(1).

services[13]. Our view is that – irrespective of the regulatory approach ultimately adopted - the obligations under the Act need to be proportionately applied to those organisations best placed to manage the content, technology or the end user relationship (as relevant). We illustrate this in Figure 3 below.

	Provider owns technology	Provider does not own technology
Provider owns end user relationship	User safety and content management obligations should apply	General obligations should apply, eg user education, terms of use, transparency, reporting, complaints
Provider does not own end user relationship	User safety and content management facing obligations should apply (except enforcement of terms of use)	General obligations should apply (B2B/enterprise/resale scenario)

Figure 3: Proposed application of online safety obligations based on role of provider

Best interests of children and role of industry

23. Children and young people are "growing up digital" and their digital relationships and wellbeing online play a critical role in shaping their sense of belonging, self-esteem, and identity, as well as their longer-term mental wellbeing. We are passionately committed to supporting the wellbeing of children and young people online, and we have a wide range of initiatives and investments underway to achieve this, some of which we describe below.

24. Through the Telstra Foundation, we partner with impactful non-profits to improve the digital skills, digital safety and wellbeing, access and connectivity of children and young people. We also enable children and young people to have their say in shaping their digital world. Our work focuses on underserved and vulnerable children and young people, and (relevantly) includes partnerships with:

    - ReachOut to Co-Chair the Technology & Wellbeing Roundtables to engage civic leaders and share youth and technology insights (including about online safety and digital skills)
    - The Smith Family to enhance digital literacy for low-income families
    - The ARC for the Digital Child and UNICEF to better understand and advocate on issues that will improve the online experiences of children and young people
    - Alannah & Madeline Foundation's online safety and cybersafety education programs and parent resources
    - Project Rockit to support their work to build a world where kindness and respect thrive over bullying, hate and prejudice, and
    - Orygen Digital to offer digital mental health resources tailored to young people, such as the Mello app,
    - Young people to amplify their voices and provide opportunities for them to shape their digital world – via the Telstra Foundation Youth Advisory Council.

    among others.

[13] Where a telecommunications provider is also supplying a service other than a telecommunications service then obligations corresponding to the provider's role in the technology and the end user relationship would apply (assuming the service was of a regulated risk type). See Figure 3.

25. We are currently designing a new Family Hub on Telstra.com.au (aiming to launch later this year) aimed at both parents and children. The Family Hub will provide resources on the real issues on which parents and children need support, including Online Safety, Mental Health and Wellbeing, Digital Education, Responsible Tech and more. We have a range of other online safety projects which we are in the early stages of exploring, including working through how we can incorporate Safety by Design principles into our CX Design Standards and designing a game for our Retail (and digital) channels aimed at teaching kids how to become digitally safe.

26. The issues paper highlights a potential, new approach under the Online Safety Act which incorporates a requirement to act in the best interests of the child, together with a statutory duty of care. We note that the former element is an existing obligation under the BOSE Determination[14], as recently amended. From the perspective of our significant and ongoing investment in online safety for children and young people, we support the critical need for additional protections for children and young people online, and for continued development of tools and resources to assist parents and children with navigating their online lives.

27. Acting in the best interests of children in the digital space can be a complex proposition, given the very broad nature of children's rights and the diversity of viewpoints (for example, there are clear findings from research on the importance of digital connectivity for education, improving mental health, wellbeing and loneliness). To be effective as a principle, either clear guidance is needed for industry about how this principle applies to various service types, or each industry segment should have a broad discretion to determine the application of this principle to its services. If the best interests of children are to be the primary consideration in the design of a service (as the BOSE Determination now requires[15]), it should be clear that this requirement applies to services which are designed for use by children or where use by children is to be expected in the ordinary course (ie other than where use is inadvertent).

28. We would support the Review bringing in the "voice of the child" to the reforms being contemplated, including to understand the types of protections and rights that children and young people would like to see, and to design the Act in a way which best envisions the future they would like to see for themselves.

Age verification

29. The issues paper asks how age verification measures can prevent and mitigate harms to children online. We support age verification measures for services where they reduce the risk of harm to children in view of the types of content involved. Age verification technologies will effectively mitigate online harms where they are applied to appropriate tiers of service based on risk service types, where it is in the best interests of children to apply those controls, and where it is left to a service provider to determine the appropriate technology solution, consistently with the approach taken under the UK Online Safety Act.

30. In prescribing age verification requirements, consideration should be given to not requiring solutions which materially increase privacy risk by requiring the collection of

[14] *Online Safety (Basic Online Safety Expectations) Determination* 2022 (BOSE Determination) s6(2A).
[15] Ibid.

additional data from individuals,[16] and to avoiding imposing obligations which overlap with existing regulatory regimes requiring identity or age verification. For example, telecommunications services are subject to existing identity requirements where the account holder's identity must be verified.

Enforcement – ombudsperson, duty of care, penalties

31. The issues paper asks whether additional statutory duties are necessary to mitigate online harms, including regarding the effectiveness of current dispute resolution processes in ensuring a safe online experience for Australians and the potential need for supplementary safeguards, such as an ombudsperson or appropriate penalties. We consider that introducing an ombudsperson or similar scheme and a statutory duty of care in relation to online safety across all service types and industry segments would not be effective for assisting individuals in the context of the services we supply.

32. In a telecommunications context, there is a significant ecosystem of telecommunications specific consumer protection, privacy and security obligations. Telecommunications customers also have a range of remedies under telco-specific consumer protection obligations, in addition to those found under the Australian Consumer Law, including the ability to submit complaints to the Telecommunications Industry Ombudsman (TIO). Without appropriate differentiation between service types, we consider that introducing an additional ombudsman and statutory obligations like a duty of care in relation to online safety for services provided by telecommunications providers would be disproportionate and costly (a cost which consumers would ultimately bear in part through increased service charges).

33. The appropriate alternative, in our view, is to consider whether an ombudsperson type arrangement or statutory duty of care[17] is requisite for other sectors, and to supplement the existing TIO regime and telecommunications law if required.

34. We are particularly mindful of other cases where general laws are made which overlap with existing, telecommunications-specific legislation, creating uncertainty and requiring complex legislative 'clean up' exercises where one set of obligations is 'paused' while the other is reconciled and phased in/out. One example is security obligations introduced by the *Security of Critical Infrastructure Act* 2018 (Cth) including for the telecommunications sector, sitting alongside existing, overlapping telecommunications sector specific security obligations under the *Telecommunications Act* 1997 (Cth) (*Telecommunications Act*).

35. Similarly, when considering augmentation of the penalties regime, we would like to see a strong link between the application of penalties to the role of a service provider and the ability of a service provider to mitigate the online harm. This suggests a tiered approach to penalties based on the severity of harm, and threshold questions of application of penalties based on whether there has been a failure of a service provider to implement controls in relation to its end users or in relation to its technology where that would have prevented the harm.

[16] Australian Government, 'Government response to the Roadmap of Age Verification' (31 March 2023)..
[17] In place of a duty of care, we note consideration should be given to the alternative proposal of an organisational accountability standard (as described in the submission from the Communications Alliance).

36. The consultation questions also ask if 'business disruption' penalties should be available more broadly; that is, whether eSafety should be able to issue a notice to a business requiring it to cease providing a particular type of service. Business disruption penalties are a very serious measure which should only be used as a very last resort and when all other options (including court ordered sanctions, remediations and penalties) have failed. Given the seriousness of their impact (which could put many smaller companies into insolvency), we consider they are best reserved to the jurisdiction of the courts, and should not be available as a direct enforcement measure. In the telecommunications context, business disruption could involve a provider (who is an intermediary for the services driving online harms) being required to cease providing a telecommunications service (ie this could result in interrupting connectivity for millions of innocent customers due to the actions of a few). This would not be a proportionate response, particularly given the intermediary services which would be involved in the online harm or transmission of content.

Balancing security, privacy and other human rights

37. The issues paper asks what considerations are important in balancing innovation, privacy, security, and safety, and specifically whether the right approach is to address risks raised by specific technologies or remain technology neutral. We believe the Act should expressly include the same types of security, proportionality and reasonableness protections that apply in the context of telecommunications interception to protect legitimate communications, the security of data and privacy.

38. The RES and DIS Standards were amended following consultation to expressly recognise that providers should not be required to implement a systemic weakness or vulnerability into detection/deletion solutions (protections expressly captured under the *Telecommunications Act*), or to require decryption[18]. We would like to see the Act expressly recognise these protections as we consider these to be critical measures to ensure that cybersecurity is not compromised as online safety solutions are implemented to meet core obligations.

39. The Act should also incorporate the remaining protections from the Telecommunications Act and specifically exempt providers from having to implement measures which are not reasonable or proportionate[19]. These protections were not recognised in the RES or DIS Standards[20], however, we consider them to be particularly important for online safety where new or emerging technology is not reliable and could affect significant volumes of legitimate communications, as well as to protect rights and freedoms under Australian law.[21]

[18] DIS Standard s20(3)(b)-21(5)(b); RES Standard s19(3)(b)-20(3)(b).
[19] A protection expressly captured under the *Telecommunications Act 1997* (Cth) s 317JC and s 317RA.
[20] We note that the RES and DIS Standards now include a requirement that measures not be taken if they are not 'reasonably practicable' however, in our view this does not protect communications to the same extent (and is more a test of feasibility). For relevant DIS Standard ss15(3), 20(3)(a), 21(5)(a), 32(1)(a); RES Standard ss15(2)(a), 19(3)(a), 20(3)(a), 24(2)(a), 28(3)(a), 33(1)(a), 36(3)(f), 37(3)(c).
[21] For example, there is a potential impact on the implied freedom of political communication under s7, s24 of the Australian Constitution if technological measures are required to be implemented which cannot effectively distinguish legitimate from unlawful communications. Some consideration should also be given to the GDPR impact of additional communications surveillance legislation for Australia as a destination country for EU data.

40. As part of our submission in relation to the RES and DIS Standards[22] we raised an additional telecommunications specific issue in relation to the requirement to protect the confidentiality of communications.[23] Online safety obligations[24] are asking, for the first time in Australia and in direct contrast to the existing prohibitions on doing so, that telecommunications providers look inside the content of communications without a warrant or other law enforcement power, and then enforce the law in relation to that content by removing the relevant offending content and/or restricting, suspending, or terminating services. In our context, this currently applies predominantly to email services. Telstra considers that providers should not be placed in a position where they comply with online safety requirements in good faith but are then exposed to an allegation that they have breached the prohibition on accessing the content of communications (or other relevant laws). Certainty on this point is important, as telecommunications confidentiality obligations are offences with substantial penalties. Telecommunications laws[25] need to be amended to clearly exempt measures taken by telecommunications providers to comply with online safety requirements to place this issue beyond doubt. More broadly, section 221 of the Act needs to be expanded to better protect providers from all potential liabilities.

Innovation and generative AI

41. At Telstra, our vision is to be a leader in responsible AI adoption. We have been involved at the earliest stages of development of responsible AI frameworks in Australia and globally:

    - Over five years ago we made a commitment to responsible AI when we helped design Australia's AI Ethics Framework, and then committed to the Australian AI Ethics Principles (2019).
    - In 2022 we co-authored The AI Ethics Playbook for the global mobile industry through our work with the GSM Association.
    - We are the first Australian organisation, and the sixth globally, to join the United Nations Educational, Scientific and Cultural Organization (UNESCO)'s Business Council to promote the implementation of its Recommendation on the Ethics of Artificial Intelligence.

42. The issues paper asks whether additional arrangements are warranted to address online harms relating to generative AI. Generative AI is a subset of AI technologies that creates new content in response to prompts. We recognise its uniqueness as a technology tool has captured public interest in AI adoption and acceleration globally, and its powerful transformative potential.

43. We can see that Australia will only reap the benefits from AI if supported by appropriate safeguards, including to build public trust and confidence in the technology and its uses. In addition to existing frameworks like Australia's AI Ethics Framework, we have recently seen the augmentation of the BOSE Determination to

---

[22] Telstra Limited, Submission to the Office of the eSafety Commissioner (eSafety) on the draft *Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard* 2024 and *the draft Online Safety (Designated Internet Services Standard – Class 1A and 1B Material) Industry Standard* 2024, 22 January 2024.
[23] *Telecommunications Act 1997* (Cth) Part 13; *Telecommunications (Interception And Access) Act* (Cth) 1979 Part 5-1A. Requires all service providers that collect and retain telecommunications data under the data retention scheme to comply with the *Privacy Act 1988* (Cth) in relation to that data.
[24] DIS Standard s20-22; RES Standard s19-21.
[25] Ibid n22, at p8.

add new expectations in relation to the safe use of generative AI services. In parallel, the Australian Government will shortly release an online safety standard and associated guidance material.

44. From our leadership position in responsible AI, we have a strong belief that legislative intervention should be saved for those areas where there are clear regulatory gaps to ensure that innovation isn't interrupted before it can occur. This concern has been noted by the UK Parliament when considering legislative approaches to AI:

    "… legislating too soon could stifle innovation, place undue burdens on businesses, and shackle us from being able to fully realise the enormous benefits AI technologies can bring."[26]

45. We do see an emerging issue of ensuring simple, targeted and proportionate regulation, and regulatory coordination, as legislators in Australia and globally face into the challenge of trustworthy AI. We are concerned that the regulation of generative AI as used by and in our industry risks becoming very complex, de-coupled from harms and the risk of innovation, or diffused across various legislative regimes and poorly aligned across jurisdictions (limiting interoperability).

46. The adoption of responsible AI by business, including the prevention of online harms, does not inherently require the making of new laws. As our strong support of Australia's AI Ethics Principles and international frameworks demonstrates, existing frameworks and legislative regimes encourage the rollout of trustworthy AI.

47. We consider that safe use of AI in Australia would, however, benefit from additional, context or service specific guidance, for example to clarify the application of existing laws like the BOSE Determination. AI specific guidance material could provide a more dynamic and flexible solution to addressing online safety risks and harms, tailored to address specific industries or applications.

Cost sharing

48. The issues paper asks if Australia should consider introducing a cost recovery mechanism for online service providers in relation to regulating online safety functions (and what this should look like). We appreciate that regulatory schemes and cost sharing may be necessary to maintain a safe online environment for Australians. A well-designed fee model will foster a safer online environment without hindering responsible businesses or those with a limited role in driving online harms. It would do that by considering factors including proportionality, service type, and risk.

49. We would like to see any cost sharing arrangements apply on a tiered, and risk/service specific basis, including to recognise:

    - the role of particular service types in driving online harms and risk into the ecosystem
    - existing funding arrangements (for example, telecommunications companies currently fund the TIO and pay the telecommunications industry levy to the

[26] Michelle Donelan, 'Publication of AI Regulation White Paper Consultation Response', *Written Questions, answers and* Statements (Web Page ,6 February 2024) <https://questions-statements.parliament.uk/written-statements/detail/2024-02-06/hcws247>.

Australian Communications and Media Authority in relation to the services they provider), and

- the need to avoid undue consumer price impacts,

as well as the scale and role of providers in the ecosystem. Specifically, organisations which derive revenue from the provision of services and hosting of content which create online safety risk should carry the responsibility for funding oversight of the risks. This should not, in our view, extend to organisations providing the underlying connectivity.

50. The UK Online Safety Act has an existing framework for cost sharing under which services meeting a revenue threshold must notify Ofcom and pay annual fees (which we understand are still being determined for implementation in 2025/26). The UK Government has identified three overarching principles to which Ofcom should have regard when developing their fee guidance: proportionality, transparency and stability. The most relevant of these principles to the design of any Australian regime is the principle of proportionality, ie fees should be applied in a proportionate way to the range of regulated providers, considering revenue earned from the services that drive risk into the ecosystem and other relevant factors.

51. Applying the proportionality principle requires designing any fee arrangements to consider not just the revenue of a regulated entity, but also the range of providers in scope and the types of services they supply (in line with a risk-based regime where the highest risk services are subject to higher regulatory requirements). Any fee regime should have the following characteristics:

    - Proportionality: Fees should be applied considering the number of relevant services in scope and the functions of the provider in the ecosystem.
    - Service Differentiation: Fees should be differentiated based on service types to recover costs for essential regulatory oversight for the highest risk services.
    - Risk Assessment: Rather than burdening all providers irrespective of their role, we propose linking fees to risk. Companies like Telstra, which are not primary risk drivers in the ecosystem and do not earn a return from online platforms, should not bear the cost of regulation to address online safety harm.

52. We consider that this type of approach to fees, centred around proportionality and contribution to risk, would ensure fairness and avoid unnecessary strain on providers.

Concluding comments

53. We believe the issues we have raised in our submission will enable the Act to focus more effectively on safeguarding Australians from online harms and promoting safer, more positive online experiences. In particular, and for the reasons we have outlined above, we believe the Act would be a more effective, flexible and targeted regime if it was amended to align:

    - in scope with equivalent legislation like the UK's Online Safety Act and the EU's Digital Services Act, specifically excluding telecommunications services and/or focusing core content and end user obligations on the highest risk services (and not on services which are out of scope of equivalent overseas legislation like telecommunications services)

- online safety obligations to the role of providers in the ecosystem, including minimising content and end user facing obligations where there is a low risk of online harms inherent in the services and where providers do not own the technology or end user relationship
- the best interests of children and age verification requirements with the risks associated with specific service types, with the former to apply to services which are directed at children and the latter case to services which carry content of a type where age verification is needed to mitigate the risk of harm
- generative artificial intelligence (**AI**) regulation with other regulatory initiatives in the AI space ,limiting over-regulation in lower risk settings to avoid stifling innovation, and
- enforcement reforms and cost-sharing with the relative contribution of industry segments and service types to online harms, and recognising that new elements like an ombudsperson and duty of care are not required for services like telecommunications where well-established consumer protection and complaint mechanisms already exist.

54. Irrespective of the direction taken by the review of the Act, our investment in and commitment to the ongoing improvement to the safety of Australians online will remain strong.

55. We look forward to continuing to work with the Department, the Office of the eSafety Commissioner (eSafety), the Communications Alliance, our industry peers, our suppliers and our customers to find solutions which enrich the experience of Australians online, limit prohibited and harmful material, and to comply with our obligations.