Submission from Telstra Limited 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

Introductory Comments

Thank you for the opportunity to comment on the:

- draft *Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024* (**RES Standard**), and
- draft *Online Safety (Designated Internet Services Standard – Class 1A and 1B Material) Industry Standard 2024* (**DIS Standard**),

together the **draft Standards**, and for the extension granted to Communications Alliance members in relation to the submission of our comments on the draft Standards.

As Australia's leading telecommunications and technology company, we are committed to helping to keep Australians safe online. We would like to strongly emphasise that we support the need for stronger measures to limit the proliferation of class 1A and class 1B material, and for the communications industry to play a role in this. With the Communications Alliance, we have played an active role in the review and development of the Online Safety Codes, and we will continue to work with industry, the Office of the eSafety Commissioner (**eSafety**), our suppliers and our customers to find solutions which limit prohibited material and to comply with our obligations.

We understand eSafety's reasons for making the draft Standards in place of the proposed industry codes for relevant electronic services (**RES**) and designated internet services (**DIS**), and we will support their implementation as far as possible. However, there are changes we believe should be made to the draft Standards before they are finalised to make them effective in improving online safety for Australians in respect of class 1A material and class 1B material. In this spirit, we have contributed to and endorse the submission made by the Communications Alliance (subject to our comments on specific issues as described in this document, where our position may differ). We also note the submission made by the Digital Industry Group Inc (**DIGI**). Many of the issues raised by DIGI are also relevant to the communications industry and to Telstra.

We set out suggested amendments below which we believe would enable the draft Standards to effectively reduce the risks associated with the proliferation of Class 1 material in the services carriage service providers (**CSPs**) like Telstra provide to our customers. Our suggestions include:

- an improved definition of technical feasibility to better recognise the state of currently available technology and alternatives, explicitly referencing the availability of technological solutions, the effectiveness and reliability of the technologies, the proportionate impact of the technology on legitimate communications, and a recognition that feasibility depends in part on the role of a provider in the technology supply chain
- an implementation period of 2 years to enable technical solutions to be investigated, developed and implemented
- building in some regulatory forbearance for the development and testing of new solutions such that a provider which is in good faith seeking to implement appropriate alternative action (but has not yet done so, including because it is testing or seeking to verify or improve the effectiveness of technology) is not regarded as non-compliant
- accountability for taking action under the Standards being more clearly aligned to providers at various levels of the supply chain, with services supplied to enterprise customers (including government and business) and wholesale customers being exempt, recognising that government data requires special consideration and that providers in the middle of the supply chain can typically neither impact the technical solutions nor the end user relationship, and

- additional protections to protect legitimate Australian users against the unintended consequences of implementing the Standards, including re resilience, security and privacy risks.

We suggest that an industry deep dive would be a useful next step, where Telstra and other CSPs could discuss with eSafety the technologies that are currently available to them, and the actions which can be taken by CSPs, in an attempt to bridge the gap between the Standards as they apply to the CSPs and the measures that industry had proposed in the rejected Codes.

Technical feasibility of the draft Standards

The primary obligations under the draft Standards require providers to detect and remove certain kinds of known Class 1A material on certain types of RES and DIS, and disrupt and deter its transmission, essentially on the understanding that technology is available which would enable searching for certain images/words and deleting the relevant material from communications or the content of services. If that is not technically feasible (as defined), providers are required to take appropriate alternative action aligned with the object of the Standards. Our view is that the understanding of available technology and the concept of technical feasibility reflected in the draft Standards will not enable effective action as it does not reflect a full view of the current state of technology, specifically of technology available to be implemented by a CSP like Telstra. Among other things, 'technical feasibility' under the draft Standards does not take into account whether:

- technology is commercially available, technically feasible to implement, or likely to be effective and reliable
- implementing the requirements of the draft Standards will disproportionately impact legitimate communications, or
- relevant measures can be implemented by a provider given its role in the supply chain.

It's important that the primary detection/removal obligation and the concept of technical feasibility be amended to address these issues, as the draft Standards pre-define the way in which the systems, processes or technologies have to work in a way which cannot be implemented by some providers and may not be the best solution as technology develops over time.

Our technical feasibility comments below are relevant to the RES Standard in connection with email (and SMS and MMS[1]) services, with our comments about new technology and technology development, false positives and reseller providers applying to both Standards.

- No viable commercially available solution: Telstra has been evaluating technological measures to assist with managing a range of unlawful content including Class 1A material for some time. We are aware of commercially available technologies (including image hashing technologies) which exist and could be implemented by some providers to locate images[2] verified by a third party as having certain characteristics. We are not aware of a commercially available technology which Telstra could integrate with our email (or SMS or MMS platforms) which could work as required by the RES Standard. There are alternative solutions available (eg DNS/domain blocking technology), which we use today in other contexts which could potentially be adapted for Class 1A and Class 1B material. We discuss these further below. However, these solutions do not work in the way specified under the detect/remove sections of the draft Standards.

[1] We understand that it was not intended for SMS and MMS to be captured under s20, however, the definitions of closed communication relevant electronic service and pre-assessed relevant electronic service do not explicitly exclude those technologies, so this is not clear or beyond doubt.

[2] In our view technologies that search for particular words versus images are not viable as a means of detection as they will likely generate overwhelmingly high volumes of false positives, disproportionality impacting legitimate communications.

Telstra notes that as a CSP supplying email we are in a different position to some other providers, for example, providers of over the top email solutions. Our internet email systems have been built to decades-old global internet technologies and standards, for agnostic use across and integration with other platforms and services. Our email platform is not modifiable or customisable in the same way as more recent email technologies. Similarly, SMS technology does not allow modification of communications as it is developed based on legacy standards.

We further understand that email (and SMS and MMS) are not the principal means of distribution of Class 1A and 1B material (which is generally distributed via alternative communications platforms in order to avoid detection by law enforcement, among other things). This means that in our view there is a significant disproportionality between the technical requirements to implement the primary detection and deletion obligations under the draft Standards in relation to email (and SMS and MMS) – which would require a re-build of relevant systems over many years – and the outcomes that would be achieved by implementing these measures.

- Development of new technologies: Overall, we don't object to the concept in the draft Standards of providers of our scale implementing programs to develop systems, processes or technologies to combat Class 1A material over time (as appropriate for their role in the technology supply chain). In our experience this will be a longer term research, development and investment process (as with all R&D activities), as we have to ensure that new technology can be integrated with our existing systems and services, will deliver services to our customers and minimise adverse customer impact. To be effective, the Standards shouldn't require providers to implement untested, unreliable new technology. In our view 'technical feasibility' must be defined to preclude implementation of technology which is untested, unreliable in detecting/deleting relevant material, or which would be likely to disproportionately affect legitimate communications. As a final point, we note that at the industry roundtable in December last year the Office of the eSafety Commissioner indicated in discussions that building new technology would not be required; however, this comment was later withdrawn. We suggest this demonstrates that there is uncertainty about the nature and extent of technology development required under the draft Standards which should be clarified.

- False positives, interruption of legitimate communications and proportionality: Telstra considers that there is a significant risk of false positives with technology solutions of this type. Specifically, all technologies Telstra considers it could investigate in connection with the Standards will likely block or affect a significant amount of legitimate and essential communications with high customer impact (unacceptably high in our view if additional protections are not built into the draft Standards). We are not familiar with the basis on which eSafety has concluded that there is a low risk of false positives. This may relate to technologies that can be implemented on a home or small enterprise basis (rather than for medium to large enterprise businesses or at a network level). [redacted]

[redacted] To address this, in addition to education (discussed below), technical feasibility should be defined under the Standards to expressly recognise a requirement that the systems, processes or technologies implemented must be proportionate to the risk of harm to innocent users of RES and DIS services and take into account the risk of false positives. We make some additional suggestions about required legal protections for legitimate communications below.

- Original suppliers vs resellers: Telstra operates in a complex technology ecosystem. We put together solutions for our retail consumer and enterprise and wholesale customers using a broad range of technologies sourced from a number of suppliers, and in compliance with global standards. The draft DIS Standard generally requires action by a 'provider', without identifying which provider is required to take the relevant action (eg the creator of the technology or its reseller, or the owner of the end user customer relationship). In many cases, Telstra will not be able to implement the relevant measure required under the draft Standards because it will not own or be able to alter the technology, or because as a supplier to enterprise or wholesale customers including government customers, it will not own the end user customer relationship. The draft Standards would be more effective if they were specific regarding which provider in a chain was required to implement particular measures.

Overall, as we have outlined above, we suggest that technical feasibility under the draft Standards should explicitly reference the availability of technological solutions, the effectiveness and reliability of the technologies, the proportionate impact of the technology on legitimate communications, and a recognition that feasibility depends in part on the role of a provider in the technology supply chain. We also suggest that sufficient time to investigate solutions is allowed through a longer implementation period, together with clearer recognition of the acceptability of alternative technological solutions in the form of forbearance during the period required to develop them. These amendments would assist providers in developing and implementing effective and technically feasible measures. We discuss this further below.

Alternative technology solutions and options potentially available for consideration

There are alternative technology solutions potentially available which would enable Telstra to take effective steps in line with the objective of the Standards. Telstra would need to further explore and develop these solutions over time.

- DNS Blocking: Telstra currently undertakes domain name server (**DNS**) blocking in relation to sites distributing Class 1A material, including on the basis of advice from Interpol. DNS blocking is effective and technically feasible as it operates on the basis of advice from expert third parties who identify specific domains distributing the relevant material which can then be blocked by a technical solution/software working together with the network/platform technology.

  Telstra is currently trialling the feasibility of linking DNS blocking solutions to SMS (ie to suppress SMS that reference particular domains). We note that this technology is not yet reliable and

[redacted]

would involve detecting the impugned domain and blocking communications that reference it (rather than detecting and removing material from communications). It requires a third party to specifically identify the domains/websites which need to be blocked, and would need to be developed and explored further.

- Other SMS/MMS solutions: It could also be feasible for Telstra to implement "campaign based" solutions, which – if a provider is advised that a particular series of communications contains relevant material - would enable us to identify and suppress that series of communications containing the particular characteristics of those communications (ie the "campaign").
  [redacted] This will not enable CSPs to detect particular images or words or vet communications at scale, and will rely on initial reporting of the campaign and material (ie by a third party or customer).

Developing alternative technology solutions takes time (as well as a significant investment of resources). Telstra believes it could develop solutions over time if the draft Standards supported that by:

- (as discussed above) amending the concept of 'technical feasibility', including so that Telstra could explore and implement appropriate effective alternative technologies
- extending the implementation period under section 2 so providers have the time to explore and implement technology, and
- building in regulatory forbearance such that a provider that is in good faith seeking to implement appropriate alternative action (but has not yet done so, including because it is testing or seeking to verify or improve the effectiveness of technology) is not regarded as non-compliant.

DIS Standard, providers and AI

The draft DIS Standard does not distinguish between a developer/supplier and a reseller/supplier providing a third party developed solution to customers. To take the example of an AI DIS, the reseller of the AI DIS may be able to take a range of steps to educate or assist its customers, but will not control or be able to change the AI DIS model itself (including to ensure it detects or removes material). The reseller will also not be able to control the training data or the use of the service by the end users (the domain of the enterprise customer). We suggest the DIS Standard concept of a "provider" needs refinement to more clearly distinguish between the responsibilities of the originator of a technology (who has the technical ability to control its content and functionality), and a reseller of such technology. The Standard should also clarify where the responsibility for managing the end users falls.

We also support the comments in the DIGI submission on the need to holistically consider regulation of online safety as it applies to high impact generative AI DIS and machine learning platforms under the DIS Standard as well as under the BOSE Determination and the very recently announced 'AI Safety Standard' to be developed by the National AI Centre in collaboration with industry. We believe an integrated and holistic approach to the regulation of AI safety is critical to the long-term development of effective online safety technology, particularly as in our view many AI services could be captured under the DIS Standard as a 'high impact generative AI DIS'.

Government data and enterprise customer issues

The draft Standards require CSPs to detect and remove known CSAM and pro-terror material from customer communications and data, as well as to enforce terms of use against end customers (including restricting, suspending or terminating services). The draft Standards do not currently differentiate between different types or classes of customers to which services are supplied, for example, retail vs wholesale, enterprise vs consumer or government customers.

[redacted]

These issues could be addressed in part by more clearly differentiating between the roles of various providers in a supply chain (as suggested above), but would be best addressed by the Standards exempting a CSP provider from complying with a requirement where a service is supplied to an enterprise (business and government) or wholesale customer (ie where is it not supplied to an end user). Thought should be given to whether government communications should be exempt.

Protecting legitimate communications from interception and inspection by having appropriate safeguards and protections in the draft Standards

The draft Standards make a significant shift to the Australian communications, privacy and human rights landscape by, ultimately, requiring telecommunications companies to look inside the content of communications and to restrict, suspend or terminate services breaching terms of use in relation to prescribed material. Whether or not this is characterised as 'monitoring' or 'intercepting' communications, the reality is that there is no way to detect whether or not particular, known Class 1A material is present without using technology to examine the content of a communication or data held in a service. This has the unintended consequence of potentially introducing vulnerabilities into these services.

The vast majority of Australians have no role in the distribution of this material, and have a fundamental expectation that their communications will be secure and private, except where there is a legitimate law enforcement requirement (and then they expect oversight and that the measures being used don't make networks or communications more vulnerable).

While eSafety has indicated in explanatory material that monitoring of communications or the introduction of vulnerabilities would not be required, the draft Standards do not currently reflect that, particularly in the definition of technical feasibility. The draft Standards also do not reflect the protections and experience built into what we think is the closest equivalent regime, telecommunications interception[4]. In our view, there are some critical protections missing from the regime proposed under the draft Standards. For example, the telecommunications interception regime:

- is based on powers granted to law enforcement agencies to access telecommunications either where they have a warrant or where another power has been granted to them;
- requires a specific request to the communications provider, and
- includes a range of exceptions to protect individuals.

The draft Standards require providers to undertake 'surveillance by default', ie for the first time we are being asked to look inside the content of all 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 that context, we consider that the draft

[4] Part 13 Telecommunications Act 1997 (Cth); *Telecommunications (Interception and Access) Act* 1979.

Standards should include the security, proportionality and reasonableness protections that apply in the context of telecommunications interception to protect legitimate communications. The concept of 'technical feasibility' under the Standards does not provide this protection.

We would like to see the draft Standards expressly recognise that providers should not be required to implement or build:

- a systemic weakness or systemic vulnerability (a protection expressly captured under the *Telecommunications Act* 1997 (Cth), s317ZG)
- measures which are not reasonable or proportionate (a protection expressly captured under the *Telecommunications Act*, s317JC and s317RA), which we think is particularly important in cases like these where new or emerging technology is not reliable and could affect significant volumes of legitimate communications.

Including these protections in the draft Standards would expressly recognise the interests of the public in privacy and cybersecurity, and assist in resolving other potential legal issues arising from the Standards.[5]

Legal issues with accessing communications

We would like to better understand the basis on which eSafety considers that there is no issue arising from implementation of the Standards under section 276 of the *Telecommunications Act* 1997 (Cth) (the prohibition on use of the content of communications), or under sections 7 and 108 of the *Telecommunications (Interception and Access) Act* 1979 (Cth) (which prohibit interception of communications and access to stored communications, respectively).

In our view, the exception to s276 under s280(1)(b) of the Telecommunications Act (permitting use of the content of communications if authorised or required by law) is not sufficiently certain when applied to measures implemented under the Standards, for example, because it could be argued that the 'use' we have made of the contents of a communication was not specifically 'required' (for example, because a different measure was available). Unlike in the case of, for example, the requirement to comply with a specific law enforcement request, providers must to some extent choose the measures they implement.

Telstra considers that carriers/CSPs should not be placed in a position where they comply with the Standards in good faith, but are exposed to an allegation that they have breached telecommunications laws. Certainty on this point is important, as carriers/CSPs risk committing offences with substantial penalties when complying with the Standards (as drafted), and this should be placed beyond doubt.

A clearer position would be for the Telecommunications Regulations to clarify that any measure taken by a carrier/CSP in good faith to comply with the Online Safety Codes and Standards is taken to be required by law, and for the draft Standards to specify that providers are not required to implement any measures which they reasonably consider unlawful. We consider that the clearest position would be to include clear exemptions under the relevant parts of the Telecommunications Act and the Telecommunications (Interception and Access) Act specifically exempting measures taken by carriers/CSPs to comply with Online Safety Codes and Standards.

Public education

Finally, we would be interested in understanding the public education planned by eSafety to raise awareness of what the new Standards will require service providers to do. The consultation has taken

[5] For example, the potential impact on the implied freedom of political communication under 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).

place over or just before the summer holiday period, and the timeframe eSafety is working to (tabling the Standards in March for commencement in April) gives limited opportunity for the public to understand the measures being proposed and for the draft Standards to be adjusted to implement the outcomes of the consultation. Public education is, in our view, particularly important given the Standards ultimately require CSPs to restrict, suspend or terminate services.

We would welcome the opportunity to discuss our views with you further. We will reach out to the Office of the eSafety Commissioner and propose that Lyndall Stoyles, Telstra's Group Executive for Sustainability, External Affairs, Legal, Risk & Compliance and Group General Counsel, meet with the eSafety Commissioner to discuss these issues and our suggested amendments to the draft Standards.

We would like to re-iterate our commitment to improving online safety for Australians, and our strong to desire to collaborate with eSafety to arrive at draft Standards that best promote that aim.

We are happy for our submission to be shared publicly, with the exception of the information we have marked as 'confidential' above, which we request is redacted from any published version.