SUPPLEMENTARY EXPLANATORY STATEMENT

Approved by the eSafety Commissioner

Online Safety Act 2021

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

Purpose of the Supplementary Explanatory Statement

The eSafety Commissioner (**the Commissioner**) has made the *Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024* (**the Relevant Instrument**) under section 145 of the *Online Safety Act 2021*.

This Supplementary Explanatory Statement amends and supplements the initial explanatory statement to the Relevant Instrument in accordance with subsection 15J(1)(c) of the *Legislation Act 2003*.

Amendment to the explanatory statement for the Relevant Instrument

Statement of Compatibility with Human Rights

After the paragraph with the wording:

> Further, the Standard adopts an outcomes and risk-based approach. The requirements contained in the Standard are proportionate to the risk a service presents in respect of class 1A material and class 1B material, and this minimises the potential for illegitimate restriction of personal expression. This risk based approach is also consistent with the CRC General Comment which specifies that content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy.

Insert new paragraphs with the wording:

> eSafety recognises that class 1A and class 1B material pose different risks to different users, and that context is likely to be more important in determining what is class 1B material. eSafety has limited the measures for class 1B material accordingly, and has carved out class 1B material which has justification from being in scope of the Standard. Proactive detection requirements are limited to class 1A material, with providers only required to have and enforce terms of use in relation to class 1B material and respond to breaches. This reflects our understanding that scalable measures for class 1B material may be more challenging, and could potentially pose more risks to infringement of privacy and free expression if providers were subject to broad detection measures, and were to implement these in a manner that did not recognise context. There is nothing in the Standard that prohibits or requires proactive scanning to identify breaches of terms of use.
>
> While not required by the Standard, eSafety considers it is also best practice for industry participants to enable a user to appeal where their material has been removed or restrictions imposed on their accounts. Providers are encouraged to have accessible complaints and appeals processes, which can enable end-users to raise instances where a provider may have made an incorrect content moderation decision.
>
> To the extent that the Standard prescribes requirements that interact with rights relating to freedom of expression, qualifiers and limitations have been built into the Standard so that these rights are appropriately balanced with the other key rights that the Standard supports. For example, an 'appropriate' qualifier has been included for key requirements relating to the detection, removal, disruption and deterrence of child sexual abuse material and pro-terror material. This supports the rights to freedom of expression and privacy as, as detailed in the

Standard, whether something (including action) is 'appropriate' can include an industry participant's consideration of proportionality to the level of online safety risk to end-users in Australia, considering scale and reach of the service. Further, the matters detailed in the Standard that may be considered when determining whether something is appropriate are not exhaustive, and so industry participants can consider other matters when determining suitable compliance actions. The 'reasonably practicable' limitation may also encompass consideration of how human rights are impacted in the context of that service.

After the paragraph with the wording:

> For example, sections 19 and 20 of the Standard require providers of specific relevant electronic services to implement appropriate systems, processes, and technologies to detect and identify known child sexual abuse material and known pro-terror material and remove that material as soon as the provider becomes aware of it. The obligations do not require a provider to do something that is not technically feasible or reasonably practicable. Nor do they require a provider to proactively scan texts, emails, or messages for content other than material which has been verified as child sexual abuse material or pro-terror material. Additionally, providers are not required to implement or build a systemic weakness or systematic vulnerability into the service. For end-to-end encrypted services, providers are not required to implement or build a new decryption capability into the service or render encryption methods less effective. This is consistent with the preservation of privacy and allows providers to both protect the privacy of individuals by safeguarding encryption, while also minimising the harm caused by this kind of material. This is also consistent with the CRC General Comment which specifies that, where encryption is considered an appropriate means to protect children's privacy, States Parties should consider appropriate measures to enable the detection and reporting of child sexual exploitation and abuse or child sexual abuse material.

Insert a new paragraph with the wording

> The Standard makes no reference to where these interventions must take place on a service, such as in 'private communications'; instead taking a risk and proportionality-based approach, depending on what is appropriate on a given service.

Attachment A

Section 19 Detecting and removing known child sexual abuse material

After the paragraph with the wording:

> Subparagraph 19(3)(b)(ii) does not require a provider to use a system or technology if, in relation to an end-to-end encrypted service, to do so would require the provider to implement or build a new decryption capability into the service or render methods of encryption used in the service less effective.

Insert a new paragraph with the wording:

> If an end-to-end encrypted service already has a decryption capability, subparagraph 19(3)(b)(ii) still does not require a provider to use a system or technology if to do so would require the provider to render methods of encryption used in the service less effective.

After the paragraph with the wording:

> Subsections 19(4) and 19(5) provide that if the provider cannot implement a system or technology due to the exceptions listed in subsection 19(3), the provider must take appropriate alternative action. The factors which must be considered when determining if something is appropriate are outlined in section 11. The appropriate alternative action may

comprise a suite of additional steps, which when considered holistically in the context of the specific service, provide risk mitigations and appropriate safeguards in lieu of a system or technology.

Insert a new paragraph with the wording:

Appropriate alternative action taken by the provider under subsections 19(4) and 19(5) will not require the provider to implement or build a systemic weakness, or a systemic vulnerability, into the service or, in relation to an end-to-end encrypted service, implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective.

Section 20 Detecting and removing known pro-terror material

After the paragraph with the wording:

Subparagraph 20(3)(b)(i) does not require a provider to use a system or technology if to do so would require the provider to implement or build a systemic weakness, or a systemic vulnerability, into the service. This exception will only apply where the system or technology would require the provider to build an actual, not merely theoretical, systemic weakness or vulnerability.

Insert a new paragraph with the wording:

If an end-to-end encrypted service already has a decryption capability, subparagraph 20(3)(b)(i) still does not require a provider to use a system or technology if to do so would require the provider to render methods of encryption used in the service less effective.

After the paragraph with the wording:

Subsections 20(4) and 20(5) provides that if the provider cannot implement a system or technology due to the exceptions listed in subsection 20(3), the provider must take appropriate alternative action. The factors which must be considered when determining if something was appropriate are outlined in section 11. The appropriate alternative action may comprise a suite of additional steps, which when considered holistically in the context of the specific service, provide risk mitigations and appropriate safeguards in lieu of a technology or system.

Insert a new paragraph with the wording:

Appropriate alternative action taken by the provider under subsections 20(4) and 20(5) will not require the provider to implement or build a systemic weakness, or a systemic vulnerability, into the service or, in relation to an end-to-end encrypted service, implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective.