20 December 2023

To: Julie Inman Grant, eSafety Commissioner

Submission on the the draft Designated Internet Services Standard and Relevant Electronic Services Standard for class 1A and class 1B material

The OPTF is a non-profit organisation founded in 2018 whose mission is to provide education and awareness around digital rights, privacy, and safety; and building and maintaining a portfolio of secure and privacy-enhancing technologies for open use. The outcome of our work enables Australians and people around the world to enjoy privacy and safety in the digital world.

General Remarks

The OPTF welcomes the opportunity to provide a response to the draft Relevant Electronic Services Standard for class 1A and class 1B material. We recognise the seriousness of the challenge which we collectively face in protecting the safety of vulnerable groups online.

As a foundation which advocates for a free, open, and secure internet which promotes respect and dignity, we call for safeguards for encryption and user privacy to be included in all applicable legal or regulatory frameworks in Australia, including the codes currently being drafted by the eSafety Commissioner.

We are primarily interested in ensuring the standards, in particular the Relevant Electronic Services Standards, sufficiently consider the technical realities and limitations of modern technology; do not have unintentional, adverse effects on the rights of Australians; and do not unnecessarily stifle technological development and business in Australia.

Defining and applying ‘technical feasibility’

The OPTF notes that, while some Sections reference limitations of technical feasibility, other Sections where such limitations may be relevant do not make similar allowances. Additionally, how we come to understand what may or may not be considered technically feasible under the Standard is not clear.

Defining technical feasibility

The given definition of technical feasibility refers inclusively to financial cost to the provider, but does not specifically provide for the actual technical challenges providers may face.

The OPTF recommends that this definition be expanded to safeguard specific technologies, such as end-to-end encryption, which protect the rights and safety of Australians.

For example, in a case where an intervention is only possible by undermining or removing end-to-end encryption, the intervention should not be considered technically feasible. More broadly, this definition should provide for limitations of a technology's architecture such as it contributes to the technology's essential purpose.

Sections with limitations on what is technically feasible

Some sections make reference to actions which may have limitations of technical feasibility, but other Sections do not make allowances. Section 22 refers to disrupting and deterring CSAM and pro-terror material, making specific suggestions of hashing, keyword detection, and machine learning or artificial intelligence systems.

While these suggestions may be appreciated by some providers, it is worth noting they are each in their own way incompatible with, for example, an end-to-end encrypted service. Additionally, machine learning and artificial intelligence are in their relative beginnings, with unresolved concerns pertaining to user and data privacy, data traceability, and outcome verification, and they are likely not appropriate for use by the average platform or company subject to this Standard.

Moreover, subsection (2) places a burden of effectiveness on the provider, potentially implying an additional expectation the 'suggested' technologies in subsection (3) be utilised, and that providers which are technically unable to utilise them may be more heavily scrutinised.

The OPTF recommends clarification be provided that subsection (3) does not require the provider to implement the systems, processes, and technologies if it is not technically feasible.

Finally, it is imperative to recognise the technical and operational constraints associated with verifying reports of abhorrent material in end-to-end encrypted environments. As content cannot be first-party verified by the provider, third-party reports from users must be relied upon. However, the means for verifying that a) the content exists on the service; b) the content was solicited, generated, distributed, or accessed by a particular user either does not exist or places an extreme technical burden on the reporting user.

Highly punitive reporting systems deployed in global contexts are at risk of abuse by malevolent state-actors, hackers, or other malicious parties making false or dishonest reports against innocent or good faith users.

Studies have demonstrated how even pro-privacy legislation, such as the European Union's GDPR, may be misused by malicious parties to target individuals. It should be considered how this Standard may similarly provide for systems which are vulnerable to abuse.

The OPTF recommends a more material measure of verification for detected or reported content than 'good faith', especially within reporting systems which carry risk of misuse.

Broadly speaking, it is important to consider the technical feasibility of any requirements placed on providers. Additionally, the Standards should refrain from requiring technologies which, in some contexts, may reduce online safety.

End-user registration requirements

There is a pre-existing 'data economy', wherein personal information of value is collected, stored, and shared among various parties. While this data may be of use in some situations, it also creates increased risk to user privacy due to potential breaches or unauthorised sharing of personal data.

Millions of Australians have recently been impacted by data breaches—9.8 million in the Optus breach, 14 million in the Latitude breach, 9.7 million in the Medibank breach—and introducing onerous requirements of personal data collection and storage on providers elevates the risk of further such breaches impacting Australians.

Large-sized companies such as Optus, Latitude, and Medibank were unable to sufficiently secure citizens' personal data, and it is likely smaller-sized providers will lack the required resources to design and maintain secure and privacy-preserving data collection and storage protocols.

In industry, it is considered best practice to avoid unnecessarily collecting personal data, yet the draft Standard places an artificial necessity for data collection.

The OPTF recommends the requirement for registration via collection of personal data such as phone number, email address, or other identifier be removed from the Standard.

Privacy considerations in framework for detection

Detection of abhorrent material in encrypted environments is currently a challenge faced by both industry and regulators around the world. Scanning technology has been widely criticised as a non-privacy preserving solution, and the concerns which have been raised in dialogue over the UK's Online Safety Bill and the EU's Chat Control proposal also apply in the Australian context.

The OPTF echoes these concerns and **broadly recommends** the flaws and limitations of scanning technologies are fully considered before their use is mandated.

Self-determination of providers

It is critical for providers to have the capacity to improve and change their services for the benefit of Australians and global users. Section 35 of the draft Standard requires the Commissioner be provided notice whenever a provider adds a new feature to their service which may increase the risk the service will be used to solicit, access, distribute, or store class 1A or 1B material. It is not clear this would not be exhaustively required for every proposed feature which may be added to a given service, particularly in the case of Tier 1 Relevant Electronic Services.

This risks placing an enormous burden on providers, inviting an asymmetrical system wherein Australians are not 'shipped' new technologies as they are created. Furthermore, it is not clear what the purpose of the notice is, whether it will be reviewed by the Commissioner, whether the Commissioner will propose changes or or whether a consultation process may be required.

The OPTF recommends altering Section 35 such that notice of changes to services may be optionally made at the discretion of the provider.

Similarly, while the requirement for providers to supply simple and accessible mechanisms for end-users to make complaints about breaches of the Standard to the Commissioner is justified, the requirements provided for in Section 28 Subsection (3) may present as problematic depending on the interpretation of "in service". Further, the "in service" requirement creates artificial restraints on how this mechanism is supplied; providers may be able to provide more full, accurate, and educational information through other means.

The OPTF recommends removing the "in service" requirement from Section 28 Subsection (3).

Conclusion

We thank you for the opportunity to participate in this consultation. We are available for any clarification or queries in relation to the feedback we have provided, and hope to be of further assistance in this important process.

Alex Linton
Director of the OPTF
[redacted]