Stakeholder roundtable

Summary of feedback from industry providers and associations on draft industry standards for Relevant Electronic Services and Designated Internet Services

March 2024

Australian Government | eSafetyCommissioner

eSafety.gov.au

This deidentified summary is based on a compilation of feedback received during a roundtable held with industry stakeholders on 7 December 2023, under Chatham House Rules[1].

Detecting known child sexual abuse material and pro-terror material

- Several stakeholders expressed concern about the **'technical feasibility' provision relating to detecting and removing known child sexual abuse material and pro-terror material**. The 'detect and remove' clause stipulates that a service provider is not required to use a system, process or technology to detect and remove child sexual abuse material or pro-terror material if it is not technically feasible. The 'technical feasibility' provision specifies certain matters to be considered when assessing what is technically feasible.
- Stakeholders highlighted that the draft standards only outline economic factors as a consideration that needs to be assessed in relation to technical feasibility. The stakeholders considered **whether it is technically feasible to implement a system, process or technology that is independent of potential investment**. They emphasised **actual technical and operational limitations** should be explicitly noted.
- A stakeholder requested greater guidance on **whether the standards expect 'completely new things' to be created in terms of technical feasibility**, as well as **what would be viewed as appropriate alternative action** if something is not technically feasible.
- A stakeholder highlighted **limitations in the capabilities of providers of email services to detect child sexual abuse material when emails are 'at rest'**. They noted that if there is an expectation in the standard to detect known child sexual abuse materials in emails that are in draft format, and as such are 'at rest', this would be a challenge, as **services have limited visibility over this content compared to their visibility when the message is transmitted**.
- A stakeholder noted **the definition of 'known material'** in the standards can only be established if the material is verified. They suggested **the standards should be clearer on which specific organisations are suitable authorities to verify** material under the standards.

[1] Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Application of Relevant Electronic Services Standard

- A stakeholder queried whether email services provided by carriage service providers (such as internet service providers) are considered closed communication relevant electronic services, and therefore subject to the 'detect and remove' provisions. The stakeholder noted there were legal[2] and technical impediments to the inspection of **every communication carried over a network. Compliance with 'detect and remove' provisions by carriage service providers would therefore not be possible.**
- Similarly, a stakeholder expressed concern about **the legality of monitoring an email service where provided by a carriage service provider**. The stakeholder was concerned with a lack of clarity around **what obligations were attached to which relevant electronic service categories**. They noted there are **different capabilities between messaging services provided by internet service providers and over-the-top messaging service providers, which was reflected in the different categories set out in the draft Relevant Electronic Services Industry Code.**

Application of the Designated Internet Services Standard to generative artificial intelligence (AI)

- A stakeholder queried **how the standard would address a scenario where a generative AI model satisfies more than one of the designated internet service categories**. For example, a model could be an enterprise designated internet service and machine learning model platform.
- A stakeholder raised concerns that the **draft standard could stifle open-source repositories**. They expressed the view that the requirements in the draft Designated Internet Service Standard may be **burdensome on open-source libraries which have limitations in their ability to know how the model will be used** once an end-user downloads it.

Compliance

- The draft standards require a service provider to **notify an enforcement authority as soon as practicable if they identify child sexual exploitation material or pro-terror material** on their service, and they believe in good faith that the material affords evidence of a serious and immediate threat to a person in Australia. A stakeholder

[2] Telecommunications Act 1997 (Cth); Telecommunications (Interception and Access) Act 1979 (Cth)

discussed the lack of specificity in the draft standards when provisions reference an 'enforcement authority'. They enquired as to whether that refers to only **Australian authorities or is inclusive of foreign authorities**, and asked whether the standards can specify the relevant enforcement authorities to ensure providers can comply with the standard.

- Stakeholders expressed concern with **variation in tests** between the registered industry codes and draft standards to determine which code or standard applies to a service. **Stakeholders raised concern that the draft standards' predominant functionality test could conflict with the industry codes' predominant purpose test** as set out in the Industry Codes Head Terms, and would create uncertainty when services assess which code or standard is applicable.
- The Industry Codes Head Terms defines the term 'appropriate' as a qualifier for obligations, meaning that obligations should be demonstrably reasonable. The draft standards include a more expansive definition of the term 'appropriate action' that includes proportionality and other measures to be considered. Stakeholders suggested **the difference in the definition of the term 'appropriate' in the standards compared to the codes will create confusion** for companies who have multiple services and are required to comply with different standards of appropriateness.
- A stakeholder was concerned **the draft standards address matters that were not identified as deficiencies in the Commissioner's statements of reasons for rejecting the two draft codes**. They advised there was an industry expectation that the standards would only address the weaknesses identified in those statements.
- A stakeholder suggested the draft standards **do not adequately reflect the work that industry** had undertaken and implemented to develop practical Head Terms and minimum compliance measures in the draft codes. A stakeholder expressed concern the **'conflict of law' provisions in the head terms of the draft codes is not reflected in the draft standards**.

Other issues

- A stakeholder queried the **inclusion of restricted content in the standards where it may not necessarily be related to class 1 material**. They suggested there are many reasons why material may be classified as restricted content due **to issues of morality as opposed to being child sexual abuse material**.
- Similarly, a stakeholder expressed the view that **the draft standards create new categories of content that are not linked effectively to the Classification Act**, which could lead to misalignment and inconsistency. They noted issues would arise if the classification framework was amended. The stakeholder proposed the draft standards

should refer directly to the definitions in the Classification Act rather than summarise the categorisation.

- Stakeholders expressed concern **about the obligations surrounding pro-terror material, given there are scenarios in which there are justifications for the material being accessed or stored** (for example, if a researcher or academic has pro-terror material hosted on an end-user managed hosting service). They suggested there were important aspects of the classification framework around consideration of contextual factors which should be addressed in the draft standards.