9 February 2023

Victoria A. Espinel
President and CEO
BSA | The Software Alliance

John Stanton
Chief Executive Officer
Communications Alliance

By email: [redacted] and [redacted]

Invitation to respond and/or submit amended draft code – Hosting Services

Dear Victoria and John,

On 18 November 2022, I received a request from the six industry associations making up the Steering Group (**Steering Group**) to register the Consolidated Industry Codes of Practice for the Online Safety Industry (Class 1A and Class 1B Material) pursuant to section 140 of the *Online Safety Act 2021* (Cth) (**the Act**).

As presented, the Consolidated Industry Codes comprise a set of head terms, and eight separate industry codes that apply to different sections of the online industry. In the request for registration, Communications Alliance and BSA | The Software Alliance (collectively, the **Industry Bodies**) indicated that together they represent providers of hosting services, so far as those services host material in Australia and were responsible for developing the Hosting Services Online Safety Code (Class 1A and Class 1B Material) (**draft Hosting Code**).

Section 140 of the Act gives me, as the eSafety Commissioner, power to register an industry code. I have considered the relevant requirements under the Act, taking into account the Steering Group's submission and accompanying documents.

I have not yet made a decision whether to register the draft Hosting Code, but have formed a preliminary view. The **attached** statement sets out my preliminary views on the draft Hosting Code, and provides you with an opportunity to respond and/or submit an amended draft code before I finalise my decision. Separate letters will be sent to the relevant industry associations in relation to each draft industry code.

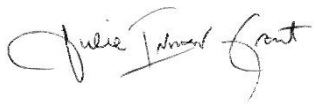
If I decide not register a code for a section of the online industry, I intend to determine an industry standard under section 145 of the Act for that section of the online industry.

Next steps

I invite you to provide a response to this letter and/or submit an amended draft Hosting Code by 5pm AEDT on 9 March 2023.

If you have any questions about this letter, please contact Morag Bond, Executive Manager, Legal MarComms and Research on [redacted], Vicki Buchbach, Co-Manager, Industry Codes Team, on [redacted], or the eSafety Industry Codes Team at [redacted]

Yours faithfully,



Julie Inman Grant
eSafety Commissioner

Statement of Preliminary Views – Hosting Services Code

Summary

On the information currently available, the eSafety Commissioner's preliminary view is that:

- the draft Hosting Code does not meet the requirement under s 140(1)(d) of the Act, because it does not provide appropriate community safeguards for matters of substantial relevance to the community (as identified in the Request for registration), namely Matters 1, 2, 4 and 11, and
- as a result, the eSafety Commissioner's jurisdiction to register an industry code under s140(2) is not enlivened.

The Industry Bodies are invited to provide a response to this Statement of Preliminary Views and submit an amended industry code addressing the areas of concern set out below.

Background

1. On 11 April 2022, the eSafety Commissioner (**eSafety**) issued a notice to the Industry Bodies, requesting the development of an industry code that applies to participants in the group consisting of providers of hosting services, so far as those services host material in in Australia (as defined under s 135(2)(f)).
2. The notice required an industry code dealing with specified matters to be submitted to eSafety by close of business on 9 September 2022. By variation issued on 24 June 2022, eSafety extended the due date for submission of the industry code to 18 November 2022.
3. By email dated 18 November 2022, the Industry Bodies submitted the draft Hosting Code to eSafety for registration. Accompanying the draft Hosting Code were a cover letter, an explanatory document titled 'Request for registration', and a submission log from the public consultation and industry associations' responses to public consultation.

Section 140 requirements

4. eSafety has reviewed the Industry Bodies' submission, including the accompanying documents. eSafety has also closely considered the draft Hosting Code in light of previous discussions with members of the Steering Group, as well as other factors including current industry practice, international approaches, the systems and technologies available to, and used by hosting providers, and the effectiveness and enforceability of the proposed compliance measures.
5. Section 140(1) of the Act sets out the conditions which must be met in order to enliven eSafety's discretionary power under s 140(2) to register a code. Based on the information currently available, eSafety is unlikely to be satisfied that all of the conditions in s 140(1) are met. Consequently, the power to register an industry code under s 140(2) of the Act would not be enlivened. The reasons for this are set out below.

Section 140(1)(d) requirement

6. Section 140(1)(d)(i) of the Act requires eSafety to be satisfied that to the extent to which the draft Hosting Code deals with one or more matters of substantial relevance to the community, the code provides appropriate community safeguards for that matter or those matters.

7. eSafety considers that the draft Hosting Code is unlikely to meet the requirement under s 140(1)(d)(i) of the Act, because it does not provide appropriate community safeguards for Matters 1, 2, 4 and 11 for the reasons outlined below.

Matter 1

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.

Matter 2

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of, class 1B material.

Matter 4

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.

8. The draft Hosting Code proposes minimum compliance measures (**MCMs**) 1-4 to deal with Matters 1 and 2, and MCMs 1-3 to deal with Matter 4.

9. MCMs 1 and 2 are of particular importance for each of these matters. MCM 1 requires providers to have policies or contractual terms 'in place' prohibiting unlawful content (including class 1A and class 1B material) and MCM 2 requires providers to have policies or terms 'in place' to enforce breaches of policies and terms concerning class 1A and class 1B material, respectively.

10. eSafety considers that MCMs 1 and 2 are unlikely to provide appropriate community safeguards in their current form. Although MCM 1 sets out a requirement to have clear contractual terms and/or policies with regard to unlawful content, MCM 2 does not require that relevant terms and policies be enforced, applied or adhered to by the hosting service provider. A requirement that these terms and policies be 'in place' may potentially be met by a service provider having these documents prepared, published and/or executed as applicable.

11. eSafety is concerned that a hosting service provider will be able to establish that it has complied with its obligations if it can demonstrate that it has published and/or executed relevant terms and policies regarding class 1A and class 1B material (MCM 1) and has also published policies or executed terms which set out the procedures for considering reports and enforcing such policies (MCM 2) without requiring the service provider to actually apply or enforce those policies and/or terms.
12. eSafety notes that requiring hosting service providers to apply or enforce their own policies and terms does not remove service providers' ability to exercise discretion, nor does it mean the service provider would be required to take certain action in all circumstances (such as terminating the provision of a service). Service providers remain able to design these terms and policies to allow appropriate and proportionate responses to potential breach scenarios.
13. eSafety considers it unlikely that measures which fail to require a hosting service provider to adhere to, apply or enforce their terms or conditions where their service is being used to store class 1A or class 1B material would provide appropriate community safeguards.

Matter 11

Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.

14. The draft Hosting Code proposes MCM 8 to address this matter, which requires service providers (on request) to submit a report to eSafety outlining the steps they have taken to comply with MCMs in the Hosting Code and an explanation as to why these measures are appropriate.
15. Under this MCM, the report must be submitted within 6 months of receiving the request, although any request that would otherwise be due within the first 12 months after the code comes into effect is not due until 12 months after the code comes into effect. The head terms further provide that a code does not come into effect until 6 months after registration. This means that no reports would be due to eSafety until 18 months after registration at the earliest.
16. eSafety has concerns that the timeframe for responding to requests for reports under MCM 8 will impact eSafety's ability to consider a service provider's compliance with code commitments, as well as eSafety's ability to provide constructive input into the first review of the Hosting Code. Without an effective review process, the capability of the Hosting Code to provide appropriate community safeguards may be compromised.
17. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 8 is likely to prevent this MCM from providing appropriate community safeguards in relation to this matter, and suggests that a reasonable response timeframe of 2 months would be appropriate.
18. eSafety also considers that the reporting requirements under MCM 8 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many cases a hosting service provider will not regularly receive reports of class 1A and class 1B material, eSafety considers that service providers should collect further information, for inclusion in a report to eSafety which could include:

- number of reports received for class 1A and class 1B material;
- number of complaints received in respect of the handling of class 1A and class 1B material;
- number of complaints related to code compliance;
- an explanation of the appropriateness of those measures and responses; and
- data and information on safety innovations, investments and third-party engagements etc.

Enforceability of the code

19. In order to provide appropriate community safeguards under s 140(1)(d) of the Act, the head terms and the specific provisions in each industry code, when read as a whole, must be capable of being implemented and being enforced. This means ensuring service providers, eSafety and other parties have sufficient certainty and clarity about the obligations under the codes. At the same time, eSafety recognises the importance of a balance between flexibility and ensuring compliance can be assessed and enforced.

20. eSafety has identified provisions in the head terms which are phrased and structured in ways that risk rendering the proposed compliance measures ineffective, or potentially impractical to measure and enforce. The following example is not exhaustive:

    Limitation clause in the head terms

    - Clause 6.1 (e)(iii), (h), (i) and (j) and clause 6.2 each limit the codes from requiring industry participants to take action or engage in conduct that would violate other laws. As previously communicated to the Industry Bodies, eSafety considers that the blanket exclusions are not desirable and it would be more appropriate for service providers to communicate specific concerns to eSafety when a specific issue arises as to how compliance with a code requirement may breach a law and/or explore alternative approaches to meeting the minimum compliance measures of the code while still meeting other legal requirements.

Next steps

21. The Industry Bodies are invited to respond to the Statement of Preliminary Views and submit an amended code addressing all the following:

    (a) MCM 2 should be amended to require that relevant policies or contractual terms be applied or enforced to ensure that MCMs 1 and 2 are effective in practice; and

    (b) MCM 8 should be amended to require reporting on a broader range of metrics, with a shortened response timeframe of 2 months, to ensure that eSafety is appropriately informed and able to carry out its functions effectively, based on timely information.

22. If Industry Bodies decide not to submit an amended code but wish to provide further information, the information should clearly explain how the existing MCMs will provide appropriate community safeguards despite the express concerns identified above.

23. Any submission and revised code will need to be provided to eSafety by 5pm AEDT on 9 March 2023, in order for the eSafety Commissioner to take it into account before making her final decision. For the avoidance of doubt, eSafety makes no representations that an amended code addressing the above concerns will be registered by default.