9 February 2023

John Stanton
Chief Executive Officer
Communications Alliance

By email: [redacted]

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

Dear 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, the Communications Alliance (the **Industry Body**) indicated that it represents providers of internet carriage services, so far as those services are provided to customers in Australia and is responsible for developing the Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material) (**draft ISP 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 ISP Code, but have formed a preliminary view. The **attached** statement sets out my preliminary views on the draft ISP 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.

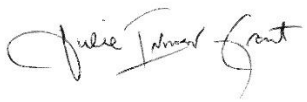
If I do not register a code for a section of the online industry, I intend to determine an industry standard under section 145 of the Act for that section of the online industry.

Next steps

I invite you to provide a response to this letter and/or submit an amended draft ISP 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, [redacted], or the eSafety Industry Codes Team at [redacted]

Yours faithfully,



Julie Inman Grant
eSafety Commissioner

Statement of Preliminary Views – Internet Carriage Service (ISP) Code

Summary

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

- the draft ISP Code does not meet the requirement under s 140(1)(b) of the Act, because the code is expressed to apply in respect of services provided to 'Australian end-users' rather than 'customers in Australia',
- the draft ISP 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 7, 10 and 11, and
- as a result, the eSafety Commissioner's jurisdiction to register an industry code under s 140(2) is not enlivened.

The Industry Body is 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 Body, requesting the development of an industry code that applies to participants in the group consisting of providers of internet carriage services, so far as those services are provided to customers in Australia (as defined under s 135(2)(g)).
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 Body submitted the draft ISP Code to eSafety for registration. Accompanying the draft ISP Code was 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 Body's submission, including the accompanying documents. eSafety has also closely considered the draft ISP Code in light of previous discussions with members of the Steering Group, as well as other factors such as current industry practices. eSafety has closely considered the effectiveness and the 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)(b) requirement

6. Section 140(1)(b) of the Act requires eSafety to be satisfied that an industry code submitted by a body or association referred to in s 140(1)(a) applies to participants in that section of the online industry and deals with one or more matters relating to the online activities of those participants.
7. The relevant 'section of the online industry' for the draft ISP Code is the group consisting of providers of internet carriage services, so far as those services are provided to customers in Australia, as defined in s 135(2)(g).[1]
8. The relevant 'online activity' for the draft ISP Code is providing an internet carriage service, so far as the service is provided to customers in Australia, as described in s 134(g).
9. Clause 2 of the draft ISP Code stipulates its scope applies only to 'entities that supply internet carriage services to Australian end-users'.
10. eSafety considers that 'customers in Australia' and 'Australian end-users' are materially different concepts, despite the likely overlap, because the former reflects an end user's geographical location, while the latter (as defined in the head terms) reflects the ordinary residency status of the end-user.
11. While some parts of the Act refer to 'Australians' and 'end-user' who is 'ordinarily resident in Australia', the provisions identifying the sections of industry and online activities subject to the proposed codes (ss 134-135) are not expressed in these terms. eSafety considers that the registration criteria in s 140 must be considered by reference to ss 134-135.
12. eSafety considers it unlikely the draft ISP Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(g), or to the relevant online activity, described in s 134(g).

Section 140(1)(d) requirement

13. Section 140(1)(d)(i) of the Act requires eSafety to be satisfied that to the extent to which the draft ISP 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.
14. eSafety considers that the draft ISP 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 7, 10 and 11 for the reasons outlined below.

Matter 7

Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.

[1] For the avoidance of doubt, eSafety is satisfied at this stage that the requirement under s 140(1)(a) that the Industry Body represents providers of internet carriage services, so far as those services are provided to customers in Australia, has been met. This Statement of Preliminary Views relates only to the scope of the draft ISP Code as submitted.

15. The draft ISP Code proposes minimum compliance measures (**MCMs**) 4 and 5 to deal with Matter 7.

16. eSafety's preliminary view is that, while the proposed MCMs are positive steps towards providing people with a range of technical tools and/or information, the commitments as currently drafted are insufficient to provide appropriate community safeguards under Matter 7 for the following reasons:

    - **Timing and availability of information** – as eSafety has previously communicated to industry, eSafety considers the information to be provided under MCMs 4 and 5 important and, in order to help safeguard end-users, ISPs should provide this information at or close to the point of sale. While industry has raised concerns that this may lead to 'information overload', eSafety considers that a commitment to provide information on filters *'at, or close to the time of sale'* is sufficiently flexible to avoid the risk of information overload at sign-up. Clear communication with links to more detailed information may also help address the risk of information overload. eSafety considers it important to provide information 'at, or close to the time of sale' as this is the time when end-users are likely most interested, and most motivated to explore the adoption of a filter. eSafety also considers it important that, in ensuring this commitment remains effective, the information remains easy to navigate to and accessible on the ISP's website.

    - **Monitoring the development of filtering and other user-safety tools** – The draft ISP Code does not contain any commitment requiring ISPs to invest in, or monitor the development of, filters or other technology designed to increase user safety. eSafety notes previous comments made by the Industry Body that ISPs have limited expertise in filtering products, and that there are significant costs related to developing filtering products. However, eSafety considers monitoring developments in filtering technology or other tools designed to protect users is important to help ensure there are technologies and systems available to remove, disrupt and/or restrict class 1A and class 1B material. eSafety considers it reasonable and appropriate that the ISP code contain such a commitment from large ISPs (for example, those ISPs with over 1 million end-users in Australia).

<u>Matter 10</u>

Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material; and Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.

17. The draft ISP Code includes MCM 9 which requires ISPs to make information on online safety in respect of class 1A and 1B material accessible to end-users, including information for parents/carers about how to supervise and control children's access and exposure to class 1A and 1B material, and to provide end-users with information about the role and functions of eSafety.
18. eSafety considers that the information required to be provided by ISPs should be easily accessible and understandable in order for this commitment to operate effectively and 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.

19. The draft ISP Code MCM 10 requires ISPs to submit an annual report upon request by eSafety which contains:
    - information on the steps the ISP has taken to comply with the MCMs of the ISP Code; and
    - any explanation regarding the appropriateness of these steps.
20. Under MCM 10, ISPs are required to submit a code compliance report to eSafety upon request. ISPs are not required to submit a report more than once in any 12-month period.
21. 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.
22. eSafety has concerns that the timeframe for responding to requests for reports under MCM 10 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 ISP Code. Without an effective review process, the capability of the ISP Code to provide appropriate community safeguards may be compromised.
23. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 10 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.
24. eSafety also considers that the reporting requirements under MCM 10 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many cases an internet service provider will not regularly receive reports of class 1A and class 1B material, eSafety considers that service providers should collect further relevant information, for inclusion in a report to eSafety that could include: the:
    - 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

25. 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.

26. 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 examples are 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 Body, 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

27. The Industry Body is invited to respond to the Statement of Preliminary Views and submit an amended code addressing all the following:

    (a) the scope and application of the draft ISP Code should align with the language of the Act where the relevant section of the online industry and relevant online activity are described by reference to 'end-users in Australia';

    (b) MCM 4 and MCM 5 under Matter 7 should be expanded to ensure that there is both:

        (i) a commitment by ISPs to provide information on filtering products at or close to the point of sale; and

        (ii) clarification on how ISPs should monitor the development of filtering and other user-safety tools, and

    (c) MCM 9 under Matter 10 should be clarified/amended to ensure safety information is to be provided in in an easily accessible manner, similar to the approach taken in other Industry Codes; and

    (d) MCM 10 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.

28. If the Industry Body decides not to submit an amended code but wishes to provide further information, the information should clearly explain how the MCM will, despite the express concerns identified above, provide appropriate community safeguards.

29. 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.