

Summary of Reasons – Internet Carriage Services Code

31 May 2023

eSafety decision

The eSafety Commissioner (**eSafety**) has decided to register the *Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)* (the **ISP Code**). The ISP Code meets the statutory requirements set out in section 140 of the *Online Safety Act 2021* (Cth) (the **Act**).

Background

The Act permits eSafety to register an industry code that has been developed and submitted by a body or association that represents a particular section of the online industry. To register an industry code, eSafety must be satisfied that it meets the requirements under section 140 of the Act, including that it provides appropriate community safeguards for any matters of substantial relevance to the community.

On 11 April 2022, eSafety gave a notice to the Communications Alliance Ltd (the **Applicant**) under section 141 of the Act requesting that they develop an industry code dealing with certain matters (the **Notice**).

On 18 November 2022, the Applicant submitted a draft of the ISP Code to eSafety pursuant to the Notice. In February 2023, eSafety gave a statement of preliminary views on this draft to the Applicant, and invited the Applicant to submit a final version addressing feedback from that statement.

On 31 March 2023, the Applicant submitted the ISP Code to eSafety for registration, with a covering document entitled “request for registration of online safety codes” (the **Request**).

Scope of the ISP Code

The ISP Code applies to entities that supply internet carriage services to end-users in Australia.¹ The ISP Code contains measures to address, minimise and prevent harms associated with access and exposure to the most harmful forms of online material accessed through internet service providers.

¹ ‘Australian end-users’ is used throughout the industry codes but is defined in clause 2 of the Head Terms as an end-user in Australia to align with the language and scope of the Act. Both terms are used in this document.

Material covered by the ISP Code includes:

- **class 1A material**, which is comprised of child sexual exploitation material, pro-terror material, and extreme crime and violence material, and
- **class 1B material**, which is comprised of crime and violence material and drug-related material,

in each case as described in Annexure A to the ISP Code Head Terms, which reflects the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (**Classification Act**) and related instruments.²

These types of material are subcategories of class 1 material under the Act, which is material that has been or would be refused classification under the Classification Act. Serious harms are associated with these kinds of material whenever it is produced, distributed or consumed.

A future industry code or industry standard will be developed to address class 2 material under the Act, which includes material that has been or would be classified X 18+, R 18+, Category 1 Restricted or Category 2 Restricted under the Classification Act.

eSafety assessment of the ISP Code

The ISP Code only applies to providers of retail internet carriage services (**internet service providers** or **ISPs**), so far as those services are provided to customers in Australia. This covers those ISPs which have both retail and wholesale or reseller activities, but the requirements in the code apply only to their retail activities. Given the role of wholesale and retail ISPs, this approach is reasonable. Retail ISPs, and the retail arms of vertically integrated ISPs have a direct relationship with Australian end-users. They are accordingly well placed to engage with end-users regarding online safety.

The ISP Code sets out a range of minimum compliance measures for ISPs that the Applicant submits provide appropriate community safeguards in relation to the matters identified in the Request.

eSafety agrees that the matters identified by the Applicant in their Request, which are materially the same as those matters identified by eSafety in the Notice requesting a code, are matters of substantial relevance to the community.

eSafety found that the ISP Code provides appropriate community safeguards in relation to each of those matters by requiring ISPs to:

1. create and maintain a safe online environment for Australian end-users
2. empower people to manage access and exposure to class 1A and class 1B material, and
3. strengthen transparency of, and accountability for, class 1A and class 1B material.

² Importantly, the nature of the material, including its literary, artistic or educational merit, and whether it serves a medical, legal, social or scientific purpose, is relevant to the assessment of class 1B material – see section 11 of the Classification Act. Material only falls within class 1B if there is no justification for the material.

Creating and maintaining a safe online environment for Australian end-users

Specific obligations relating to the first of these objectives require ISPs to:

- if requested by eSafety, join and sign the Online Crisis Protocol governing the blocking of certain class 1A material under Part 8 of the Online Safety Act
- inform Australian end-users that they must not produce online material that is in contravention of any Australian law, and
- notify hosting service providers if the ISP becomes aware of alleged class 1A material being hosted.

Empowering people to manage access and exposure to class 1A and class 1B material

The ISP Code places specific obligations on ISPs which aim to empower users to manage access and exposure to class 1A and class 1B material. These include obligations on ISPs to:

- ensure Australian end-users are advised on how to limit access to class 1A and class 1B material by providing, easily accessible information available on filtering products at or close to the time of sale
- ensure Australian end-users are advised of the existing Family Friendly Filter program
- ensure Australian end-users are informed of their right to make complaints about class 1A and class 1B material to content providers and eSafety, and the procedures for doing so
- link to eSafety's complaints reporting process, and
- respond to complaints.

Strengthening transparency of, and accountability for, class 1A and class 1B material

Specific obligations relating to the third of these objectives require ISPs to:

- provide Australian end-users with easily accessible plain-language information on online safety, and
- submit reports to eSafety setting out steps they have taken to comply with the ISP Code, an explanation as to why those steps are appropriate and the volume of reports received about class 1A and class 1B material on their service.

eSafety considers that these obligations will, together, create effective and meaningful obligations that reflect the role of ISPs in the online safety ecosystem in addressing the risks of class 1A and class 1B content.

Next steps

The ISP Code will shortly be published on the eSafety Commissioner's Register of industry codes and industry standards for online safety. The ISP Code will come into operation six months thereafter.