Explanatory Memorandum

For the

DRAFT (for public consultation)

Consolidated Industry Codes of Practice for the Online Industry

(Class 1A and Class 1B Material)

1 September 2022

Contents

1. Executive Summary

The Codes that are the subject of this consultation have been developed by industry under the *Online Safety Act 2021* **(the OSA**), following the guidance laid out in the Office of the eSafety Commissioner's 2021 Position Paper[1].

The Codes outline steps that online industry participants must take to enhance online protections by reducing access and exposure to **Class 1A** and **Class 1B** material, which are categories of content that have been defined by the Office of the eSafety Commissioner to include online material promoting child sexual abuse, terrorism, extreme crime and violence, crime and violence, and drug-related content.

Separate Codes have been developed for each section of the online industry identified by the OSA, including:

1. **social media services** (e.g. Facebook, Instagram, TikTok);
2. **relevant electronic services** used for messaging (including SMS and MMS) services, email, and online gaming services (e.g. Gmail,WhatsApp, services);
3. **designated internet services** that include websites and end-user online storage and sharing services (e.g. Dropbox, Google Drive);
4. **internet search engine services** (e.g. Google Search);
5. **app distribution services** used to download apps (e.g. Apple IOS and Google Play stores);
6. **hosting services** (e.g. Amazon Web Services, NetDC).
7. **internet carriage services** (e.g. Telstra, iiNet, Optus, TPG Telecom); and
8. **manufacturers and suppliers of any equipment that connects to the internet, and those who maintain and install it** (e.g. of modems, televisions, phones, tablets, smart home devices, e-readers etc).

The OSA requires that industry associations representing these sectors develop the Codes on behalf of the industry. A group of industry associations have been closely engaging with an extensive group of companies across these sectors with the technical know-how and experience in managing Class 1A and Class 1B material online.

These industry associations are the Australian Mobile Telecommunications Association (**AMTA**), BSA | TheSoftware Alliance (**BSA**), Communications Alliance (**CA**), Consumer Electronics Suppliers Association (**CESA**), Digital Industry Group Inc. (**DIGI**) and Interactive Games and Entertainment Association (**IGEA**) (**the Steering Committee**).

The Steering Committee has consulted extensively with industry and would now like to hear from a wider group of interested parties in Australia. The Committee encourages parties likely to be impacted by the Codes to share views and feedback, including:

- consumer groups
- civil society groups
- community legal and advocacy groups
- representatives from academia
- children and young people
- parents, carers, teachers and educators (including their representative groups)
- users of the services and devices (including content creators impacted by the codes)
- digital rights groups
- women's advocacy groups
- domestic and family violence groups
- groups representing sex workers
- groups representing the safety tech sector, and
- companies and organisations in each of the industry sections outlined above.

[1] https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper

Feedback will be used to refine the Codes before they are submitted to the eSafety Commissioner for approval and registration later this year. Upon registration by the eSafety Commissioner, the Codes will be enforceable by directions, civil penalties, enforceable undertakings and injunctions to ensure compliance. The Office of the eSafety Commissioner is widely accessible to receive complaints and investigate potential breaches of the Codes.

2. Background

a) The Online Safety Act

The new ***Online Safety Act 2021****,* which replaced the *Enhancing Online Safety Act 2015*, gives Australia's independent regulator for online safety, the eSafety Commissioner, greater investigative and enforcement powers and updates Australia's **Online Content Scheme**. Previously, Codes had been developed under the *Broadcasting Services Act 1992 (Cth)*. However, the online world has changed significantly since they were developed and new Codes are required to reflect this changed reality.

Under the updated Online Content Scheme, the eSafety Commissioner has asked the online industry to develop Codes that deal with the online treatment of **Class 1** and **Class 2 material**.

Class 1 and Class 2 material is defined by reference to:

a) the classification it has received by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995 (the Classification Act)*, where the material has been classified, or
b) the classification the material would likely be given by the Classification Board under the Classification Act, where the material has not been classified.

In very broad terms, Class 1 is comprised of materials that are or would be classified as Refused Classification (RC), while Class 2 is comprised of materials that are or would be classified as X18+ or R18+. Class 1 and Class 2 material includes online material depicting or promoting child sexual exploitation, terrorism, extreme crime and violence, crime and violence, drug use, and pornography.

The scale of material that is available online is clearly immense, and while the classification scheme allows for consideration to be given to the context in which material appears offline (for example, its literary, artistic or educational merit and whether it serves a medical, legal, social or scientific purpose), this type of assessment is extremely challenging when looking to comprehensively achieve online prevention and storage of such material at scale**. While a range of measures can be introduced by industry participants that aim to improve online safety for Australians, consistent with the objects of the OSA, the Codes recognise these limitations.**

It is worth noting that the National Classification Scheme is currently under review, and adjustments may be required to the Codes in light of any changes made to the National Classification Scheme as a result of that review.

b) Parameters set out by the eSafety Commissioner's Position Paper

In September 2021, the Office of the eSafety Commissioner released the **Development of Industry Codes under the Online Safety Act Position Paper** (**the Position Paper**) to guide industry with the development of the Codes.

As expressed in the Position Paper, the Office of the eSafety Commissioner's core objectives for the Codes are to establish compliance measures for industry that broadly fall into three categories: (1) measures to create and maintain a safe online environment; (2) measures to empower persons to manage access to Class 1 and Class 2 material; and (3) measures focused on transparency and accountability. The Codes must apply across the online industry and aim to include the industry's responsibilities for dealing with Class 1 and Class 2 material.

As outlined in the Position Paper, under the National Classification Scheme, classification decisions are to give effect, as far as possible, to the following principles:

(a) adults should be able to read, hear, see and play what they want;
(b) minors should be protected from material likely to harm or disturb them;
(c) everyone should be protected from exposure to unsolicited material that they find offensive; and
(d) the need to take account of community concerns about:
(i) depictions that condone or incite violence, particularly sexual violence; and
(ii) the portrayal of persons in a demeaning manner.

The Position Paper sets out **11 policy positions** regarding the substance, design, development and administration of industry codes, as well as eSafety's preferred risk and outcomes-based model for the Codes. Under this model, each Code will include a common set of objectives and outcomes which, to a very large extent, mirror the positions set out in the Position Paper (see **Table 1** in the Annexure to this document for the Outcomes and Objectives used in each of the Codes) and industry has flexibility to develop tailored compliance measures in response to those objectives and outcomes, taking into account their unique context and other relevant factors. This is necessary to take account of the large variety of participants (global enterprises to very small companies), services and technologies covered by the Codes.

The Commissioner can refuse registration and impose alternative obligations on industry in the form of Standards if the Codes do not meet the Commissioner's requirements.

c) Material covered by the Codes

The Position Paper further classifies Class 1 and Class 2 material as **Class 1A, 1B, 1C, 2A** or **2B,** by grouping together materials based on eSafety's assessment of the harm they cause. Class 1A is intended to capture the most harmful materials, followed by Class 1B and so on.

The Codes that are the subject of this consultation deal only with Class 1A and Class 1B material. Industry participants have agreed with the eSafety Commissioner that additional Codes will be developed to deal with Class 1C and Class 2 materials.

Class 1 A is any material which[2]:

- promotes or provides instruction of paedophile activity ('child sexual exploitation');
- advocates the doing of a terrorist act, including terrorist manifestos ('pro-terror');
- describes, depicts, expresses or otherwise deals with matters of extreme crime, cruelty or violence (including sexual violence) without justification (for example murder suicide, torture and rape), ('extreme crime and violence'); or
- promotes, incites or instructs in matters of extreme crime or violence ('extreme crime or violence').

Class 1B is any material which[3]:

- describes, depicts, expresses or other wise deals with matters of crime, cruelty or violence without justification ('crime and violence');
- promotes, incites or instructs in matters of crime or violence ('crime and violence');

[2] p.23, Office of the eSafety Commissioner, *Development of Industry Codes under the Online Safety Act Position Paper*, Sept 2021
[3] p.23, Office of the eSafety Commissioner, *Development of Industry Codes under the Online Safety Act Position Paper*, Sept 2021

- describes, depicts, expresses or otherwise deals with matters of drug misuse or addiction without justification ('drug-related content'); or
- includes detailed instruction or promotion of prescribed drug use ('drug-related content').

d) Development process

Six industry associations have formed a Steering Committeeand are overseeing the development of the Codes. These are:

- Australian Mobile Telecommunications Association (**AMTA**),
- BSA | TheSoftware Alliance (**BSA**),
- Communications Alliance (**CA**),
- Consumer Electronics Suppliers Association (**CESA**),
- Digital Industry Group Inc. (**DIGI**), and
- Interactive Games and Entertainment Association (**IGEA).**

A concerted effort has been made to adopt the positions and follow the guidance set out in the Position Paper released by the Office of the eSafety Commissioner, including to design measures that are reasonable and proportionate to the service and harm type in question.[4] In developing the Codes, there has also been a need to ensure they do not result in conflicts with existing legal obligations for industry.

The Steering Committee represents a broad cross-section of companies spanning each of the eight sectors of the online industry. Since October 2021, the Steering Committee has undertaken intensive industry consultation with broad outreach to industry participants in each applicable section of the online industry, including outside of the membership of each association. Those industry participants have formed working groups with extensive participation, and the associations have kept a wider group of industry participants and the associations' members informed and provided multiple opportunities for input on draft versions of the code. Many companies to whom the Codes will apply are not members of any of the above industry associations, and their participation has been proactively sought by the association in attempts to run an open and representative process. Participating associations and companies have engaged in the drafting process in good faith.

The Steering Committee is responsible for overseeing the public consultation of these Codes and will subsequently work with industry to refine the Codes before submitting them to the eSafety Commissioner for registration.

3. Industry's approach to Codes for Class 1A and Class 1B

a) Structure of Codes

The **Consolidated Draft of Industry Codes (Phase 1)** contains eight separate industry codes that apply to different sections of the online industry. Each code has been developed by one or more industry bodies or associations that represent the relevant section of the online industry.

- **Code 1:** Social Media Services
- **Code 2:** Relevant Electronic Services
- **Code 3:** Designated Internet Services
- **Code 4:** Internet Search Engine Services
- **Code 5:** App Distribution Services
- **Code 6:** Hosting Services

[4] p.6, Office of the eSafety Commissioner, *Development of Industry Codes under the Online Safety Act Position Paper*, Sept 2021

- **Code 7:** Internet Carriage Services
- **Code 8:** Equipment

The Codes establish obligations on the whole of the online industry in respect of Class 1A and Class 1B material. As per the Position Paper developed by the Office of the eSafety Commissioner, they include a mix of (**mandatory**) 'minimum compliance measures' and (**discretionary**) 'optional compliance measures'. Minimum compliance measures aim to hold industry to account and lift the standard of minimum protections in place for Class 1A and Class 1B materials. Many companies may already go beyond or choose to go beyond the minimum measures that are now required to be implemented by a certain class of participants, as set out by the measures.

Under some Codes, companies will need to undertake a risk assessment of their service or product, as different compliance measures are prescribed based on their risk profile. For example, services with a higher risk profile may have minimum compliance measures that lower or medium risk services are not subject to. However, a risk assessment is not always necessary, as it is more appropriate in some sectors for obligations to apply to all industry participants equally.

b) Different requirements based on functionality of industry sectors

Industry has developed separate Codes for the eight online sectors to reflect the different role that various online sectors must play in reducing access and exposure to Class 1A and Class 1B materials, due to the different role they play in the digital ecosystem. The diverse nature of the service-types, purposes, audience and business model in scope for these codes means there is a need for proportionate responses based on the level of risk presented by the service. For example, social media services, relevant electronic services and designated internet services generally include a more direct interface between online material and end-users than exists for internet search engine services or app distribution services. Similarly, hosting services, internet carriage services and applicable equipment support access to material only in conjunction with another online service, and have different relationships with end-users and control over end-user interfaces.

The Codes recognise that all eight sections of the internet industry have a role to play in improving online safety and that this role will vary between sectors, depending on how direct a relationship a service is with the ultimate end-user, and the extent to which it may have control of individual items of content. For example, it may be more appropriate for an app owner with direct control of content on their app to delete an item of Class 1A or Class 1B material, rather than to require an app store to disable access to the app. In drafting the Codes, industry has considered what and where interventions will be most effective and proportionate, depending on the service and the nature of the content in scope. Child sexual abuse and exploitation material, for instance, will warrant a heightened level of safety measures.

Consideration has also been given to designing measures that will not impact competition by creating undue barriers for new industry entrants. For example, some compliance measures may be limited in their application to companies of a certain size. Tools that are currently accessible to only a few companies (for example, certain AI technologies) are also not specified as minimum compliance measures, as that would be unachievable for many smaller companies.

c) Requirement for proactive detection of Class 1 materials

Outcome 1 of the Position Paper requires industry to take "Proactive steps to detect and prevent access or exposure to, distribution of, and online storage of Class 1A material". This includes child sexual exploitation and pro-terror material, but also including material describing, depicting or otherwise dealing with extreme violence and crime.

The approach broadly taken across Codes is to give priority to measures that require the highest risk, public and semi-public platforms to proactively detect known child sexual exploitaition or pro-terror material. The industry considered whether the Code should include measures that would require providers to proactively monitor or scan users' private file storage and private communications (for example, emails and text messages). The industry concluded that the extension of proactive detection measures could have a negative impact on the privacy and security of end-users of private communications and file storage services, including services used by businesses and government enterprises.

Industry has also considered what it can do to detect first-generation child sexual abuse material. Some very large companies have invested in technology that can detect first-generation child sexual material (i.e. material not previously identified and stored in an appropriately maintained NGO database), however this technology is still in an early stage of development. While the accuracy of technology to enable detection of first-generation material is improving, it is generally accepted that it is not as accurate as technology for the detection of known CSAM and requires greater human review of detected materials. The proactive detection of online materials has therefore been limited to the detection of known child sexual abuse material.

Industry participants involved in the Code development process to date are of the view that the identification and removal of other types of Class 1A and Class 1B materials, such as crime and violence or drug-related material, should largely be dealt with by robust policies, end-user reporting and enforcement mechanisms. While effective technology exists and is deployed by some companies to proactively detect child sexual abuse material (for example, PhotoDNA and CSAI Match), comparable technical solutions do not exist across the other Class 1A and Class 1B categories, and there may not be community acceptance for the level of monitoring required to conduct proactive detection for these types of content. The proactive detection of this material through technical solutions is also not always practical as context around how and where the material appears is required for these kinds of assessments, which is not possible at a large scale. For example, showing crime and violence may be permissible where the intention is to bear witness to atrocities or as part of public-interest journalism, and portrayal of drug misuse or addiction that some may find objectionable, may be permissible in public health messaging. Therefore, while companies may choose to develop and adopt proactive measures for such content, the Codes do not require this; instead, they require companies to enable their users to flag such content so that it can undergo human review with attention to context, and prompt removal where necessary.

Industry would like to hear from interested parties during the consultation on the appropriateness of the approach, including:

1. **Are the measures in the Codes reasonable and proportionate to the harm posed by different types of Class 1A and Class 1B material?**
2. **Do measures across Codes include an appropriate level of protection in respect of Class 1A and Class 1B material?**
3. **Do you think the Codes strike an appropriate balance between user privacy, freedom of expression and online safety, particularly around services used for private communication and storage of material?**
4. **Are there any inconsistencies across Codes that should be addressed?**
5. **How will the Codes impact different in-scope businesses across the eight industry sectors (e.g. start ups, companies without a presence in Australia, new entrants to different online markets)?**

4. Next steps

Online safety is a priority for all parties involved in the drafting of the Codes and there are a range of experiences that have been considered in the development of this Draft. It is expected that feedback from the broader community and stakeholders provided during the public consultation, plus ongoing dialogue with the Office of the eSafety Commissioner, will help to further refine the Codes.

a) Key submission dates and information

The Steering Committee of industry associations invites interested parties to submit views and information to assist our development of the industry Codes.

The Steering Committee encourages general feedback from a wide range of stakeholders including young people, parents, educators, civil society groups, private individuals, the business community – including businesses of different sizes and at different stages of maturity –, the sex industry, researchers and academics, and any other stakeholders to whom the online world is relevant for their business or who has a personal experience that is relevant to share in the context of the Codes.

Individuals and organisations that would like to make a submission can **lodge a submission at www.onlinesafety.org.au**. Submissions will be accepted between September 1 and October 2, 2022.

Should you have any questions, you can contact the industry associations at **hello@onlinesafety.org.au**.

APPENDIX

Table 1: Online safety objectives and outcomes used in each of the Codes

Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for end-users in Australia.
● **Outcome 1:** Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material. ● **Outcome 2:** Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material. ● **Outcome 4:** Industry participants take reasonable and proactive steps to prevent or limit hosting of class 1A and 1B material in Australia. ● **Outcome 5:** Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material. ● **Outcome 6:** Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and 1B material, including complaints
Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.
● **Outcome 7:** Industry participants provide tools and/or information to limit access and exposure to class 1A and 1B material. ● **Outcome 8**: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and 1B material. ● **Outcome 9:** Industry participants effectively respond to reports and complaints about class 1A and 1B material.
Objective 3: Industry participants will strengthen transparency of, and accountability for class 1A and class 1B material.
● **Outcome 10:** Industry participants provide clear and accessible information about class 1A and class 1B material. ● **Outcome 11:** Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.