Supplementary Explanatory Memorandum

For the

REVISED DRAFT (for second round of public consultation)

Consolidated Industry Codes of Practice for the Online Industry

(Class 1A and Class 1B Material)

9 March to 23 March 2023

Contents

1. Executive Summary

The Codes that are the subject of this **second round of 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. 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.

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).

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**).

For further background on the requirements for registration of the Code please see *the Explanatory Memorandum for the Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* published on September 2022.[2]

The Steering Committee conducted an initial round of public consultation on the draft Codes in September 2022. On 18 November 2018, updated Codes were submitted to the Commissioner for registration, together with supporting documentation that included the industry's response to the public consultation. The Commissioner provided industry associations with a preliminary assessment of the Codes on 9 February 2023 requesting that additional feedback be considered by industry prior to the Codes being resubmitted to the eSafety Commissioner by 9 March to better address community expectations[3]. The industry associations requested an extension to conduct a second 30-day public consultation on the draft Codes to give the community and stakeholders an opportunity to express their views on the revised Codes following the Commissioner's feedback. A short extension

[1] https://www.esafety.gov.au/about-us/consultation-cooperation/industry-Codes-position-paper
[2] https://onlinesafety.org.au/
[3] The version of the Codes and the Commissioner's preliminary assessment are available at: https://onlinesafety.org.au/Codes/

was granted by the Commissioner and revised Codes are now due for resubmission to the regulator by **31 March 2023**. This allows for a **two-week period** of second public consultation.

The complexity of the subject matter and scale of the Codes' potential applications means that feedback is sought from a broad range of industry participants, community stakeholders and government agencies. **The Committee encourages parties likely to be impacted by the Codes to share views and feedback on the revised versions of the Codes, 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.

The revised drafts of the Codes are marked up to compare the version of the Codes submitted to the Commissioner for registration and the version that is the subject of this second round of public consultation. Given the brief time frame allowed by the Commissioner for the industry to revise and resubmit the Codes, we recommend that submissions focus on the changes made since the initial round of public consultation concluded in 2022.

2. Industry's approach to Revision of Codes for Class 1A and Class 1B materials

Industry has made material revisions to the Codes in response to the Commissioner's preliminary assessment of the Codes, communicated to industry associations on 9 February 2022. We have summarised some of the most significant changes below which stakeholders may wish to consider in making a submission.

a) Head Terms (common terms for all Codes)

- The definition of **Australian end-user** has been revised. **Australian end-user** now means an end-user in Australia.
- A definition of **known-pro-terror material** has been added which incorporates concepts used by non-governmental organisations operating to prevent terrorists and violent extremists from exploiting digital platforms, which are recognised as expert or authoritative in that context. This change impacts the pro-active detection measures in the Social Media Services Code and Relevant Electronic Services Code.
- Clause 5.2 now expands the obligations on relevant industry participants to notify their risk status under the Codes to require notification of how their service/device is categorised under the Codes.

b) Schedule 1 Social Media Services

- *Risk assessment:* The clauses in this Code concerning the approach to risk assessment by social media service providers have been strengthened. In particular, note the introduction of a requirement that where a

risk assessment indicates that the service may fall in one or more risk tiers, the provider must assess the risk profile of the service to fall into the higher risk tier (see clause 5.1(c)).

- *Proactive Detection of Pro-terror material*: Measure 9 has been strengthened to extend minimum compliance measures to proactively detect known pro-terror materials to all Tier 1 social media services (rather than very large social media services per the previous draft).
- *Investment to disrupt and deter CSAM/Pro-terror material*: This Code now contains specific obligations on industry to invest in solutions that aim to address child sexual abuse materials and pro-terror materials on their services. Measure 10 has been revised and now contains minimum compliance measures for all Tier 1 social media services to invest in systems, processes, and/or technologies that aim to disrupt and deter CSAM and pro-terror materials.

c) Schedule 2 Relevant Electronic Services

- This Code has undergone significant revisions, including a restructure of the previous approach to risk assessment. Because of the extensive changes a clean and revised version have been published on the onlinesafety.org.au website.
- *Services that do not need to assess risk:* The approach of this Code has been revised so that most (if not all) known categories of services that fall within the definition of relevant electronic services under the OSA are not required to undertake a risk assessment and will be required to comply with specific compliance measures allocated to them under the Code. This provides clarity about how the Code regulates these services. Those categories are:
    - closed communication relevant electronic services.
    - dating services.
    - encrypted relevant electronic service.
    - enterprise relevant electronic services.
    - gaming services with communications functionality; and
    - gaming services with limited communications functionality,
- *Services that need to assess risk:* The Code requires some services to assess their risk. This is particularly relevant for future services that may not fall into the existing categories set out by the Code. The provisions regarding risk assessment have been strengthened. Note the introduction of a requirement that where a risk assessment indicates that the service may fall in one or more risk tiers, the provider must assess the risk profile of the service to fall into the higher risk tier.
- *New definitions for services that are capable of assessing and reviewing materials and not capable of reviewing materials and services that are capable of removing materials and not capable of removing materials:* These concepts have been introduced to ensure that the minimum compliance measures under the Code take into account differences in the technical and legal capacity of different types of providers to review, assess and or remove materials in accordance with the requirements of the Classification Scheme. This provides greater clarity regarding the measures that are applicable to different types of relevant electronic services. See also corresponding revisions to measure 3, measure 4, measure 12 and measure 13. Also note the inclusion of a new obligation in clause 5.3 that requires providers to report to eSafety if they are capable of reviewing and assessing material or capable of removing material.
- *Notification of CSEM and pro-terror materials:* Measure 2 has been broadened to cover a broader range of services including gaming services with limited communications functionality.
- *Proactive detection of known CSAM:* Measure 9 extends this obligation to a broader range of service categories i.e., Tier 1 relevant electronic service, an open communications relevant electronic service that is not a carriage service provider; dating services, and a gaming service with communications functionality.
- *Proactive detection of known Pro-terror material*: Measure 10 was previously limited to very large Tier 1 relevant electronic services. The obligations in this measure now extend to all Tier 1 relevant electronic services and all open communications relevant electronic services.

- *Actions to deter and disrupt CSAM and pro-terror materials*: This Code now contains specific obligations on those industry participants to invest in solutions that aim to address child sexual abuse materials and pro-terror materials on their services. Measure 11 has been revised and now contains minimum compliance measures for a broad range of services to invest in systems, processes, and/or technologies that aim to disrupt and deter CSAM and pro-terror materials. This measure applies to a Tier 1 relevant electronic service; a dating service; an open-communications relevant electronic service; closed communications relevant electronic service; or an encrypted relevant electronic service.

d) Schedule 3: Designated Internet Services

- *Risk assessment:* The clauses in this Code concerning the approach to risk assessment by designated internet service providers have been strengthened. Note the introduction of a requirement that where a risk assessment indicates that the service may fall in one or more risk tiers, the provider must assess the risk profile of the service to fall into the higher risk tier (see clause 4.1(d)).
- *New definitions for services that are capable of assessing and reviewing materials and not capable of reviewing materials and services that are capable of removing materials and not capable of removing materials:* These concepts have been introduced to ensure that the minimum compliance measures under the Code that are applicable to end-user hosting services take into account differences in the technical and legal capacity of different types of providers to review, assess and/or remove materials in accordance with the requirements of the Classification Scheme. This provides greater clarity regarding the measures that are applicable to different types of end-user hosting services (examples of end-user-managed hosting services include online file storage services, photo storage services or other online media hosting services). Also note the inclusion of new obligations in clause 4.5 that require providers of end-user hosting services to report to eSafety if it is capable of reviewing and assessing material or capable of removing material.
- *End-user hosting services:* Changes to this Schedule principally strengthen the measures in the Code that are applicable to services for file storage and management. See revisions to measure 3, measure 4, measure 5, measure 11 and measure 12.

e) Schedule 4: Search Engine.

- *Algorithmic Optimisation:* The minimum compliance measures in measure 1 concerning algorithmic optimisation has been clarified and strengthened so as to require search engine service providers to adjust ranking algorithms to elevate authoritative, relevant and trustworthy information and reduce the risk that class 1A material is accessible or discoverable in search results by Australian end-user.

f) Schedule 5: App Distribution Services

- *Engagement with Third Party App Providers:* Changes have been made in measure 1 to strengthen obligations on app distribution service providers to review apps before release and to enforce agreements with third party app providers with the aim of reducing the risk of access or exposure to, distribution of, or online storage of class 1A material via third-party apps.

g) Schedule 6: Hosting Services

- *Enforcement of policies:* Measure 2 has been strengthened.

h) Schedule 8: Internet Service Providers

- *Provision of information about filtering products:* Measure 4 has been strengthened to ensure this information is provided by ISPs to customers at or close to the point of sale.

- *Reporting:* The reporting obligation on ISP's to report to eSafety has been strengthened so that ISPs must additionally report about complaints by end-users about Class1A and Class1B materials and Code complaints

i) Schedule 9: Equipment

- *Gaming devices*: The revisions to this Schedule generally aim to strengthen measures applicable to gaming devices that enable end-users to play online games. See new definition of gaming device, revisions to measure 5 and new measure 6(d) that requires manufacturer of gaming devices to develop and implement appropriate tools that allow Australian end-users to help reduce the risk of harm to children when using those devices.

3. Next steps

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

The Steering Committee encourages 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 from **9 March to 23 March 2023.**

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.