DIGI

Senate Standing Committees on Environment and Communications
By email: ec.sen@aph.gov.au

22 September, 2025

Dear Committee members,

The Digital Industry Group Inc. (DIGI) appreciates the invitation to provide a submission to the Senate Environment and Communication References Committee's (the Committee) 'Inquiry into the Internet Engine Services Online Safety Code and the under 16 social media ban' (the Inquiry).

DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's members are Apple, Discord, eBay, HelloFresh, Google, Meta, Microsoft, Pinterest, TikTok, Twitch, Spotify, Snap and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI is committed to improving and championing online safety in Australia. We support the eSafety Commissioner's efforts to progress the Government's online safety policy, as outlined in the Online Safety Act (2021) (the OSA). DIGI welcomes the Commissioner's recent decision to register the Phase 2 Online Safety Codes (including the internet search engine services code), marking a significant step forward by industry in making the internet safer for young Australians across a broad range of digital services and devices. DIGI is especially proud to have played our part in up-levelling the protections for AI companion chatbots which are generating considerable public concern around the world[1].

DIGI led the development of these codes on behalf of a consortium of peak industry associations. This was an intensive effort, which required industry associations to engage extensively with the Office of the eSafety Commissioner throughout the process. We also consulted with a broad range of industry and civil society stakeholders, as part of a robust public consultation process required under the OSA.

By way of background, the Phase 2 codes form part of the eSafety Commissioner's suite of regulatory tools regarding the management of harmful and age -inappropriate online content under OSA, which passed parliament in 2021. The codes are legally enforceable, with civil penalties ranging up to AU $49.5 million. Their focus is on material identified under the National Classification Scheme as in-appropriate for Australians under the age of 18, including pornography, extreme violence, and content promoting or instructing in suicide, self-harm and eating disorders. They regulate a wide range of service providers and technology organisations that make services available to Australian end-users covering social media platforms, messaging services, online games, search engines, app stores, internet service providers, hosting providers, and even device manufacturers, suppliers and maintenance and installation providers.

[1] For example, on September 17 the United States Senate Judiciary Subcommittee on Crime and Counterterrorism w convened a hearing "Examining the Harm of AI Chatbots. See 'Critical Questions for Congress in Examining the Harm of AI Chatbots 'Liana Keesing, Isabel Sunderland, *Tech Policy Press*, Sep 16, 2025 available at https://www.techpolicy.press/critical-questions-for-congress-in-examining-the-harm-of-ai-chatbots/. See also information about the risk to children posed by AI companion chatbots provided by eSafety available at https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people.

The measures in the Phase 2 codes are tailored to the different online industry services that are in scope of the OSA and were designed to respect privacy and human rights, as well as delivering on the key expectations contained in eSafety's position paper on code development. Some key measures include:

- **Risk Assessments**: Services that are likely to have a variable risk profile – such as Social Media Services and certain websites – are required to conduct risk assessments to ensure that their compliance obligations are proportionate to risk of users being exposed to online pornography, self-harm material or high-impact violence material. Following the risk assessment process, services must abide with a stringent compliance framework of the relevant code.
- **Privacy**: The codes contain privacy protections such as requiring services not to use or disclose user's personal information in a way that would be in breach of privacy law.
- **Age Assurance requirements**: The codes contain targeted age assurance measures for:
    a. Social Media Services that allow online pornography, self-harm material or high-impact violence material. These services must restrict under 18's from accessing this material.
    b. Search Engine Services must age assure user accounts in order to filter out pornography and high impact violence material for logged -in users under 18.
    c. App Distribution Services (app stores) must ensure apps are appropriately rated and restrict under 18's from accessing 18 +rated apps.
    d. Adult websites that make online pornography available, and self-harm sites that promote or instruct in suicide, eating disorders and self-harm, must restrict access to their services by under 18's.
    e. Where AI companion Chatbots generate pornographic or self-harm content, they must implement age assurance mechanisms.
    f. Simulated gambling apps must restrict access to their services by under 18's.
- **Parental controls**: Where feasible, the codes require parental control mechanisms (for example, on mobile devices) to filter inappropriate material for child users.

In general, the codes adopt a flexible approach to age assurance, encouraging seamless, privacy protective approaches such as using age inference from existing data.

DIGI is conscious that search engines, in particular, are fundamentally different from other online services. Search engines do not host or publish user-generated content but rather index publicly available third-party content and return links in response to user queries. Search is user-initiated, intent-driven, and supports access to information, a fundamental human right under the International Covenant on Civil and Political Rights. In addition, privacy expectations are high for search, as users typically expect to search anonymously without logging in or sharing personal data. This is why the search engine services code allows users to search in a logged-out state, without needing age assurance.

DIGI is committed to collaborating with the Commissioner to ensure clear public communication and education about the codes and their impact. DIGI considers there is a need for public awareness of the Phase 2 codes and their practical implications, —particularly the application of age assurance requirements. There is a risk of public misunderstanding when these requirements come into force, as seen in other jurisdictions[2].

It is also important to acknowledge that detailed input from the Office of the eSafety Commissioner throughout the development process has significantly influenced the outcome of the Phase 2 codes. Under the OSA, the Commissioner holds the ultimate authority to determine if industry codes contain appropriate community safeguards and qualify for registration. The complete versions of the eight Phase

[2] CNBC 'Why a new UK internet safety law is causing an outcry on both sides of the Atlantic' Aug 12, 2025.https://www.cnbc.com/2025/08/12/why-the-uk-age-verification-law-has-led-to-backlash.html

2 codes are available on the Office of the eSafety Commissioner's website in the register of codes[3]. Further information about the code development process is set out on the online safety.org.au website, published by industry associations. Each registered code comprises Head Terms which govern all the codes, and a schedule which sets out the measures for the relevant industry section as set out in Appendix B. The Head Terms set out a number of key principles which require regulated businesses to balance privacy, safety, human rights when implementing obligations under the codes. Appendix B also includes details of the industry associations that were involved in the drafting of each code.

DIGI's role and engagement with the Phase 2 codes drafting process has given us unique insights on the operation of the codes, which we have detailed in this submission. The submission provides additional background around the code measures and code development process which we hope will assist the Committee's inquiries. As the codes and this submission of necessity use a range of technical terms, we have included for the Committee's reference, a table of terms in Appendix A of this submission, which we encourage you to review.

We thank you for your consideration of the matters raised in this submission. Should the Committee have any questions, please do not hesitate to contact DIGI, and we look forward to further contributing to the Inquiry.

Yours sincerely,

[redacted]

Dr Jennifer Duxbury
Director Policy, Regulatory Affairs and Research
Digital Industry Group Inc. (DIGI)

[3] https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards

Table of contents

Background to development of Phase 2 industry codes

Parliament intended that industry develop codes under the Online Safety Act

The Phase 2 industry codes, including the internet search engine services code, have been drafted by industry in accordance with the Australian Parliament's intent and the requirements of Part 9 of the OSA. Section 137 (1) of the OSA says:

> *The Parliament intends that bodies or associations that the Commissioner is satisfied represent sections of the online industry should develop codes (**industry codes**) that are to apply to participants in the respective sections of the industry in relation to their online activities.*

This co-regulatory scheme has some parallels with those in the Broadcasting and Telecommunications legislation. The eSafety Commissioner has a broad remit under the Act to request industry associations representing different parts of the industry to develop codes to deal with "matters relating to the online activities" of industry participants. The Commissioner is empowered to issue notices under s141 to relevant industry associations, which specify the matters to be dealt with in the codes for each of eight different sections of the online industry. If industry associations do not comply with the request outlined

in a notice, or fail to meet timing requirements, the Commissioner may instead determine an industry standard. If the Commissioner is satisfied that industry codes contain appropriate community safeguards, they are registered by the Commissioner and become enforceable regulatory instruments.

The Commissioner announced in 2021 that industry would be tasked with developing two sets of eight codes that would be advanced in two phases – with the first phase addressing certain. illegal and high-end harmful content (Class 1 materials) and the second addressing fetish pornography (Class 1C) and content unsuitable for under 18's (Class 2 materials). Phase 1 focused on providing community safeguards, across "the technology stack' (the eight sections of the industry described in the OSA), against "Class 1 material ", the most harmful online material based on the criteria of the National Classification Scheme. This includes illegal material such as child sexual abuse material and pro-terror content, as well as certain extreme crime and violence material and drug-related content. The Commissioner accepted six of the Phase 1 codes for registration in 2023, while rejecting two others. In response to the rejected codes, the Commissioner developed two standards. These standards, which came into force last year, cover measures for messaging services and online games (relevant electronic services), and websites, apps, and user-managed hosting services (designated internet services).

In the case of the Phase 2 codes, a key objective of the Government was to limit the exposure of children to pornographic material online.[4] This was informed by the report of the House of Representatives Standing Committee on Social Policy and Legal Affairs, following their inquiry into age verification for online wagering and pornography[5]. We have provided a timetable below that summarises the process for developing the Phase 1 and Phase 2 codes over the past four years, alongside related policy programs.

Timetable for Phase 1 and Phase 2 code development and implementation in context

Date	Event
September 2021	eSafety published an initial position paper to guide the industry in developing the Phase 1 codes. Code development by industry associations commences.
April 11, 2022	The eSafety Commissioner issued notices to six industry bodies requesting the development of Phase 1 codes.
June 16, 2023	Industry-developed Phase 1 codes for five industry sections (social media services, app distribution services, equipment, hosting service providers, and ISPs) were registered.
September 16, 2023	A sixth industry code for internet search engine services was registered.

[4] *Government response to the Roadmap for Age Verification* (Australian Government, August 2023) p.3
[5] *Protecting the age of innocence,* (Commonwealth of Australia 2020).

December 16, 2023	The first five registered Phase 1 codes came into effect.
March 12, 2024	The Phase 1 search engine services code came into effect.
June 21, 2024	eSafety developed and registered standards for Relevant Electronic Services and Designated Internet Services (due to non-registration of industry codes).
July 1, 2024	The eSafety Commissioner issued section 141 notices to five of the six industry bodies involved in drafting the Phase 1 codes, requesting they begin drafting the Phase 2 codes. eSafety also published a supplementary position paper outlining expectations for Phase 2 codes.
September 12, 2024	Industry associations consulted with representatives of the pornography industry, including via a roundtable also attended by eSafety representatives.
October 22, 2024	The legislatively mandated public consultation on the Phase 2 codes commenced and was publicised with a wide range of stakeholders including digital rights and child advocacy groups.
November 22, 2024	The legislatively mandated public consultation period for the Phase 2 codes concluded.
November 29, 2024	The Online Safety Act 2021 was amended to require in-scope "age-restricted social media platforms" to prevent Australians under 16 from having an account.
December 15, 2024	The s141 notices were varied to require the Industry Associations to provide copies of submissions received, summaries of submissions, and a second preliminary draft of each code by December 19, 2024, and were given an extension until February 28, 2025, to submit the codes.
December 19, 2024	Industry associations provided details of the submissions to the public consultations, summaries of the Associations responses to submissions, and a second preliminary draft of each Phase 2 codes to the Commissioner.

December 2024	The Standards for the Phase 1 Relevant Electronic Services and Designated Internet Services took effect.
December 2024	The Commissioner granted extensions for submission of the Phase 2 codes until February 28, 2025.
February 28, 2025	Industry Associations provided the Commissioner with further drafts of the Phase 2 codes.
June 27, 2025	The Commissioner registered the Phase 2 codes for Hosting Services, Internet Search Engine Services, and ISPs.
July 29, 2025.	The Minister made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 (the Rules), specifying services that are not age-restricted social media platforms under the OSA.
September 1,2025	The Age Assurance Technology Trial report was published.
September 9, 2025	The Commissioner registered the Phase 2 codes for Relevant Electronic Services, Social Media Services, Equipment Providers, Designated Internet Services, and App Stores.
September 16, 2025	The Commissioner publishes regulatory guidance on the reasonable steps required to comply with the social media minimum age restrictions under the OSA.
December 10, 2025	The social media minimum age restrictions will come into force under Part 4A of the OSA.
December 27, 2025 (Anticipated)	The first three Phase 2 codes including the Internet Search Engine services Code will come into force under the OSA.

March 12, 2026.(Anticipated)	The five Phase 2 codes registered on September 9, 2025, will come into force under the OSA

How the Phase 2 codes supplement the OSA legislative scheme for protecting children

The Phase 2 codes are intended to complement a range of existing measures in the OSA that require or encourage services to adopt age assurance as a child protection measure:

- The **Restricted Access Declaration** requires social media services, designated internet services, relevant electronic services, and Australian hosting service providers that provide or host "Restricted Material" to restrict children's access to R18+ content (i.e. a subset of class 2 material) online, upon receiving a notice from eSafety.
- **The Basic Online Safety Expectations Determination** (BOSE) sets out expectations for all social media services, relevant electronic services (including messaging, email and gaming services), and designated internet services (including websites). Section 12 emphasises the core expectation that providers will take reasonable steps to implement measures – technological or otherwise – to prevent children accessing class 2 material. The BOSE specifically mentions that reasonable steps to comply with section 12 could include 'implementing age assurance mechanisms.' The BOSE also gives eSafety powers to obtain information from service providers about how they meet these expectations.
- The **social media minimum age restrictions** set out in part 4A of the OSA (SMMAR), require age-restricted social media services to take reasonable steps to prevent under 16's from accessing their platforms, which will require implementation of age assurance measures. These requirements will take effect on December 10, 2025.

We also note that the **Children's Online Privacy Code,** is currently under development by the Office of the Australian Information Commissioner (OAIC) as passed by parliament in the Privacy and Other Legislation Amendment Bill 2024. These reforms are expected to address whether entities need to take reasonable steps to establish an individual's age with a level of certainty that is appropriate to the privacy risks to users under 18, such as by implementing age assurance. This code is due to be finalised in December, 2026.

eSafety Commissioner's positions on development of Phase 2 codes

The Commissioner's expectations on the development of the Phase 1 and Phase 2 codes are outlined in two position papers that were published in 2021 and 2024[6] (Position Papers). These Position Papers explain how industry associations should ensure codes include appropriate community safeguards, specifying examples of the types of measures eSafety considers appropriate and necessary to protect the community from Class 1 and Class 2 material.

[6] These are published on the eSafety Commissioner's website at esafety.gov.au.

The 2024 Position Paper made very clear that the Phase 2 codes must incorporate a range of age assurance measures across the technology stack:

> *The measures outlined in this position paper highlight the importance of implementing age assurance, as it is essential for industry participants to recognise when an end-user is a child to activate appropriate protective measures*[7]

The 2024 Position Paper proposes a range of minimum compliance measures be included in the codes for achieving eSafety's preferred outcomes including age assurance measures across various devices used by children such as mobile phones and tablets, and across services such as search engine services, social media services, apps and pornography websites and messaging and email services[8].

The Position Papers also state that the Age Assurance Technology Trial would inform industry's approach to age assurance under the Phase 2codes. However, the Trial did not conclude until after the deadline for submission for the Phase 2 codes set by eSafety, which meant that industry associations drafting the codes were unable to take into account its results. Further, the Trial only tested a limited sub-set of the participating age assurance technologies on users of a 'laboratory' social media site, rather than the broad range of services in scope of the Phase 2 codes.

The Commissioner has recently produced *Social Media Minimum Age Regulatory Guidance* to guide the implementation of the SMMAR. In this guidance, the Commissioner encourages age-restricted social media services to consider:

> *the findings of the trial, which can help them to understand the technologies on offer in the current market. This includes their readiness for deployment in the Australian context, some of their strengths and weaknesses, opportunities for improvement and how they align with current and emerging international standards*[9].

This guidance, while not directly applicable to the Phase 2 codes, adopts a flexible and iterative approach to age assurance measures which DIGI supports, recognising that the technology is continuing to evolve. This flexibility is consistent with the approach to implementation of age assurance outlined in the Phase 2 codes. The *Social Media Minimum Age Regulatory Guidance* contains detailed recommendations concerning the implementation of age assurance under the SMMAR, including the steps age-restricted social media services should take to protect user privacy and enable users to appeal decisions on age assurance e.g. where a user is incorrectly blocked from using a service. The Commissioner plans to issue additional guidance concerning the compliance of regulated providers under the Phase 2 codes, which we anticipate will build on the *Social Media Minimum Age Regulatory Guidance*.

The process for development of the Phase 2 codes

The five industry associations tasked with developing the Codes engaged in an intense collaborative process that involved a broad range of industry participants, and ensured diverse participation beyond the associations' memberships. This process enabled the associations to harness knowledge and expertise across the tech stack, identifying the specific needs of different industry sections and their users. To achieve this:

---

[7] *Development of Phase 2 Industry codes under the Online Safety Act eSafety Position Paper July 2024*p.4
[8] *Ibid* p54-82.
[9] Office of the eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance, September* 2025 p.4

- Industry associations invited their members to participate in the drafting effort.
- Non-members were invited to participate at no cost or membership requirements, addressing any membership gaps. This included participants from the Phase 1 process and additional identified participants from the adult industry.
- Relevant industry participants either directly engaged in the drafting of the codes or were given the opportunity to contribute issues and suggestions.

In accordance with the OSA requirements, the industry associations held a 30-day public consultation on the draft Phase 2 codes from October 22 to November 22, 2024. Drafts of the codes and a detailed Discussion Paper, outlining the approach and submission process, were published on the Online Safety.org.au website which we established for code development. The five Industry associations developing the codes extensively promoted the public consultation through:

- Newsletter updates to industry, government, and civil society organisations.
- Updates on social media channels and association websites.
- A media alert, which generated 123 print and 80 radio stories (including syndications), raising awareness and explaining the code development approach to facilitate stakeholder participation.

The associations proactively contacted over 250 stakeholders from relevant consultation categories, as outlined in eSafety's discussion paper, inviting their submissions. Additionally, the industry associations convened a virtual expert stakeholder roundtable.as part of the public consultation. All the public submissions and industry's responses are published on Onlinesafety.org.au together with a record of the roundtable.

DIGI believes that meaningful and ongoing consultation with key stakeholders on safety should not be confined to regulatory processes. We note that in addition to these formative consultation processes, the Phase 2 codes require certain services including internet search engine services to engage on an ongoing basis with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to age inappropriate material under the codes. For example, providers of an internet search engine service must consider information obtained through such engagement.

Key measures and principles governing implementation of the codes

The Phase 2 codes deliver a range of additional safeguards for all Australians, with targeted measures to limit the exposure of under 18's to pornography, high impact violence, and material that promotes or instructs on suicide, self-harm, or eating disorders. Regulated businesses implementing measures are required to take into account a common set of principles which are set out in the Head Terms including:

- the importance of the applicable online safety objectives specified in the codes;
- where relevant, the risk profile of the industry participant;
- the importance of protecting and promoting human rights online, including the right to freedom of expression, the right not to be subjected to arbitrary or unlawful interference with privacy, the right to protection from exploitation, violence and abuse, and the rights and best interests of children, including associated statutory obligations. Note: In this context, the rights of children include the rights recognised in the United Nations Convention on the Rights of the Child;
- the product or service in question, including its function, purpose, size/scale and maturity as well as the capacity and capabilities of the industry participant providing the product or service;

- whether the steps taken are proportionate to the level of risk to online safety for end-users in Australia as a result of the material[10].

The Table in Appendix C contains a summary of the key measures for different industry sections. Please note that this is not a comprehensive list. For example, all the codes contain additional measures that require relevant providers to undertake risk assessments, complaints handling, and provide transparency reports to the eSafety Commissioner.

Approach to content in scope of the Phase 2 codes

The s141 notices by the Commissioner require that the Phase 2 code measures be directed at preventing children and enabling adults to manage access to 'class 1C and class 2 materials'. This scope of content is very broad and is based on the National Classification Scheme in accordance with the OSA. DIGI's experience is that it is very challenging to manage online content based on the National Classification Scheme because it was developed for classifying individual items of professionally produced content before commercial release to the public. This same challenge was acknowledged in report of the recent independent review of the Online Safety Act: [11]

> *This nuanced framework is not workable as the basis for a regulatory regime designed to apply to vast volumes of online content, that as eSafety suggest in their submission, is dynamic, fluid and even ephemeral. What is needed is clear rules to determine whether certain material is illegal or harmful in order to trigger rapid removal, appropriate regulatory action and efficient compliance by online services*[12].

The classification process required by the scheme, requires fine, context-based judgments of materials, which are very difficult for online service providers to do accurately because of the vast range and diversity of online material at scale. These difficulties are magnified in the case of class 2 materials which are lawful for adults, but unsuitable for children. Following the suggestions in the July 2024 Position paper, we defined a series of 'high priority content types' for the Phase 2 codes to make the management of age restrictions and other measures practically feasible. These high priority categories included pornography, high impact violence and self-harm material (inc material that promotes or instructs in suicide, eating disorders and self-harm). By better defining the content in scope of the codes we hope to improve the ability of providers to accurately target age-inappropriate materials while protecting freedom of expression.

Approach to age assurance in Phase 2 codes

The approach for age assurance in the Phase 2 codes was developed with detailed input from eSafety, drawing upon the eSafety Commissioner's Position papers, industry knowledge of best practice approaches and international developments including the *code of Practice for Online Safety for App Distribution Services* issued by Infocomm Media Development Authority in Singapore, the Draft *EU Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online* pursuant to Article 28(4) of Regulation (EU) 2022/2065 and the safety measures recommended by Ofcom in the *Protection of Children codes* under the Online safety Act (UK) as well as *Ofcom's Guidance on highly effective age assurance*. By implementing best practice approaches from comparable jurisdictions that

[10] See section 5.2 in the *Consolidated Industry codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms*.
[11] See recommendation 29 of the *Report of the Statutory Review of the Online Safety Act 2021* Delia Rickard PSM October 2024, p120-134.
[12] Ibid, 121.

have codified protections for children from harmful materials, DIGI hopes that the Phase 2 codes can help promote greater regulatory parity across like jurisdictions, which will enable stronger compliance by industry.

As noted in the recently published Age Assurance Technology Trial Report, a wide range of approaches to age assurance exist, but there is no one-size-fits-all solution for all contexts. As every service type presents a different risk profile and requires a risk-proportionate response, providers need to be empowered to tailor age assurance techniques to their service. Industry is pleased to see that the eSafety Commissioner's recently published *Social Media Minimum Age Regulatory Guidance* concerning acceptable age assurance methods, under the SMMAR reflects the report's finding that there is no one size fits all approach and that there is a need for flexible approaches to implementation.

Implementation of Phase 2 Codes: User privacy and key considerations

The drafting of the Phase 2 Codes emphasises that services in scope of age assurance measures should minimise data collection in the implementation of age assurance under the Phase 2 codes. This is especially critical for services like search engines, where users expect a high degree of privacy and anonymity.

The Head Terms of the Phase 2 codes provide that service providers required to implement age assurance should take into account a range of additional, specific considerations:

- the technical accuracy, robustness, reliability, and fairness of the solution for implementing the age assurance measure;
- appropriate age assurance measures must include reasonable steps to assess whether an Australian end-user is at least 18 years of age;
- whether age assurance measures have been designed to comply with Privacy Laws and whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives specified in the codes;
- the interaction between measures which require age assurance in this code, and other applicable Australian laws which may require age assurance for the same product or service, including how to best achieve the online safety objectives of the codes whilst minimising the collection of personal information.

The effect of the Head Terms that is that service providers subject to the Phase 2 codes must comply with Privacy Act obligations when using personal information of their users for the purpose of complying with the various age assurance measures .

The OAIC is the regulator responsible for implementing Australia's privacy laws including ensuring regulated entities follow the Privacy Act and other laws when handling personal information, including sensitive information. This can involve conducting investigations and handling complaints by users of online services. Reforms passed by parliament in the Privacy and Other Legislation Amendment Bill 2024 are intended to strengthen legislated privacy protections, impacting how organisations implement and use age assurance and manage associated information. The OAIC has powers for enforcing the Privacy Act particularly concerning interferences with individual privacy as defined in subsections 63F (1) and (3) of the Privacy Act. Online service providers under the Codes must also consider privacy related guidance issued by the OAIC.

The Phase 2 Codes are designed to ensure age assurance is implemented on different services in a manner that is proportionate to the risk of under 18's encountering class 2 materials. For example, where

the principal purpose of the service is the dissemination of one or more types of 'priority types' of Class 2 materials i.e. pornography, high impact violence or self-harm materials (suicide, eating disorders and self-injury), the service must implement effective age assurance to prevent under 18 year-olds accessing the service[13]. As such, all pornography websites and services that have the purpose of promoting or instructing in self-harm are required to ensure that only users over 18 access their sites.

Age assurance measures are included at other key online access points to high priority materials by under 18's such as app stores, social media services, designated internet services, and search engines. Additionally, the codes contain measures that require providers to implement less intrusive measures where these are an effective alternative to age assurance.[14] For example, there are requirements on services that carry films and computer games which are classified as 18 + or X18+ under the National Classification Scheme (Classified DIS) to implement parental controls.

In some cases, the age assurance measures in the codes were strengthened to accommodate additional requests by eSafety. For example, the Designated Internet Services (DIS) code was updated after the public consultation to include measures restricting access by under 18's to AI companion chatbots that have a medium to high risk of generating high impact sexualised material or self-harm materials. However, while we carefully considered eSafety's expectations as outlined in their Position Papers and additional detailed feedback they provided on successive drafts of the codes, we did not adopt all of their suggested measures. For example, while industry shares eSafety's concern to protect under 18 year-olds from exposure to Class 2 material, we are mindful of ensuring that any restrictions or barriers to vital communication tools are an appropriate, and provide a proximate response to the risk of harm to young users while also adequately protecting users' rights including privacy In particular, we found the views of the eSafety Youth Advisory Council on this issue to be helpful:

> *Messaging platforms, such as WhatsApp, Messenger, iMessage and Discord, should not be included in age verification reforms. Social media platforms and messaging apps are distinctive from each other. While social media platforms have an undefined set of users accessing and interacting with content from all other users, messaging apps have a definite pre-defined list and destination of who the messages will go to. Their differing risk profiles should be considered[15].*

Consequently, the measures in the codes concerning email and messaging services do not require providers to implement age assurance or otherwise restrict users' access to materials sent as part of private communications between users but aim to prevent unintentional exposure of users to pornography and other unsolicited materials[16].

Age assurance requirements on social media services under the Phase 2 Codes and the Social Media Minimum Age Restrictions

We thought it might be helpful to the Committee to outline the interaction between the Phase 2 Codes and the SMMAR. This raises some specific privacy-related issues, for social media services of which the Committee should be aware.

---

[13] See *Protection of Children Codes under the Online Safety Act UK.*

[14] See draft EU draft guidelines under Article 28(4) of the *Digital Services Act* (DSA) published on 13 May 2025 p14. These include, for example, measures that require detection and removal of priority material on social media services that prohibit that material where this is an effective alternative.

[15] eSafety Youth Council, *Submission to the Joint Select Committee on Social Media and Australian Society,* 2024

[16] We note that the *UK Protection of Children codes* do not apply to email services.

The Phase 2 Social Media Services (Core Features) code requires services to implement age restrictions to protect under 18's from accessing online pornography, or self-harm material where the service allows such material to be posted by users under applicable terms of use. A complicating issue for these services is that s63F of the OSA prohibits age-restricted social media services from re-using data obtained to comply with the SMMAR for any other purpose including compliance with the Phase 2 codes, without the user's consent. In effect, this means relevant social media services that must age assure users under the SMMAR will need to collect additional data to comply with the age assurance requirements in the Phase 2 Codes. The code drafters were conscious of this issue and have dealt with it in s 5.1 (c) (iv) of the Head Terms which provides that:

> service providers must consider the interaction between measures which require age assurance in this Code, and other applicable Australian laws which may require age assurance for the same product or service, including how to best achieve the online safety objectives specified in section 4 of this Code whilst minimising the collection of personal information;

Additionally, all social media services will aim to meet the expectations of the Commissioner outlined in the *Social Media Minimum Age Regulatory Guidance.* This guidance makes clear that the Commissioner expects providers to take a layered approach to age assurance to minimise end-user friction. This is consistent with the data and findings of the Age Assurance Technology Trial and our understanding of the technical capabilities of the technology. It is easier to use age assurance technology to identify if a user is under 18 than under 16. Not only will users under 18 often hold relevant ID, but the technology has been most commonly developed and tested for use on this age demographic. The use of the technology to identify the age of under 16's is more novel, and this demographic is less likely to hold relevant ID. Further, as teenagers mature at different rates, it can be harder to estimate their age with technologies like facial estimation. While it is not yet clear how many layers of age verification must be used to meet the requirements of the SMMAR, it seems reasonable to conclude that more personal information must be collected by social media services to verify if a user is under 16, then they would need to collect to verify if a user is under 18 under the Phase 2 social media services code.

Concluding Remarks

In conclusion, DIGI would like to reinforce our commitment to online safety regulation that keeps pace with technology to foster safe, equitable digital spaces for the Australian community. The extensive work DIGI has done in conjunction with eSafety to develop codes, that we believe will achieve a demonstrable uplift in online safety across the technology stack, is evidence of this commitment. We hold a long track record of directly engaging in the development of regulation that is effective in its goals and can practically be implemented by industry. We appreciate the opportunity to contribute to this inquiry.

Appendix A: Summary of Key Terms used in Phase 2 codes

Category	Term	Definition / Description
Classes of Material	Class 1C Material	The category of fetish pornography material identified in the Position papers that is deemed offensive, but not necessarily illegal, and is rated as unsuitable for children and adults in accordance with the National Classification Scheme.
	Class 2 Material	Material that is restricted to over 18-year-olds in accordance with the National Classification Scheme., typically involving more severe content like high impact online pornography or self-harm material. This category includes further sub-classifications developed for the purposes of developing the Phase2 codes.
	High Impact Online Pornography	A specific type of graphic image based, or video-based pornography developed for the purpose of the Phase 2 codes that is considered highly inappropriate for under 18's.
	Self-Harm Material	Material that promotes or instructs in self-harm including suicide and eating disorders.
	High Impact Classified Material	Specific types of classified material (films, publications, computer games) that would be classified X18+ or R18+ under the National Classification Scheme due to their content, and self-harm material.
Industry Associations	Australian Mobile Telecommunications Association Communications Alliance, Consumer Electronics Suppliers' Association	Industry associations that were the subject of the s141 notices

	Digital Industry Group Inc, Interactive Games and Entertainment Association	
Categories of Services and Equipment Providers regulated by the Phase 2 codes	Social Media Services (SMS)	Platforms designed for the purpose of enabling social interaction as defined in the OSA.
	App Distribution Services	Services that distribute third-party applications (apps), such as app stores as defined in the OSA.
	Equipment Providers	Includes manufacturers, suppliers, installers, and maintenance providers of equipment, including operating system providers for certain devices.
	Hosting Service Providers	Services that host stored material online. The Phase 1 and Phase 2 codes distinguish "First-Party Hosting Services" (hosting their own content) and "Third-Party Hosting Services" (hosting content for other services). The Hosting Services code deals with Third Party Hosting Services.
	Internet Carriage Services (ISPs)	Includes providers of internet connectivity to end-users (retail ISPs). They act as a conduit for online content.
	Relevant Electronic Services (RES)	A broad category of online services under the OSA that includes dating services, messaging services, email services, gaming services with communications functionality, and SMS, and MMS.
	Designated Internet Services (DIS)	A very broad category under the OSA that encompasses most apps and websites accessible in Australia, from retail and entertainment sites to online bookstores and educational platforms, to adult websites and generative AI services. This category includes several sub-categories based on purpose and risk profile.

	Internet Search Engine Services	A category of services that has the sole or primary purpose of enabling end-users to search the service's index of material on the WWW for relevant results in response to the end-user's queries as further defined in the Phase 1 and Phase 2 Internet search engine services codes.
	High Impact Class 2 DIS	A type of Designated Internet Service defined under the codes whose main purpose is to provide access to high impact online pornography and/or self-harm material.
	High Impact Class 2 Generative AI DIS	A type of Designated Internet Service that uses AI to generate high impact online pornography.
	Classified DIS	A Designated Internet Service that makes available content classified under the Classification Act, with specific measures depending on whether it includes high impact material.
	End-User Managed Hosting Service	A type of hosting service where the end-user has primary control over the hosted material.
	OS providers	Operating system providers which are a type of provider of operating systems for equipment under the Equipment Code.
Other Key Terms	OSA	Online Safety Act.
	Phase 1 codes / Phase 2 codes	Refers to different stages of industry codes developed under the Online Safety Act, with Phase 2 building on Phase 1.
	Age Assurance Measures	Measures required under the Phase 2 codes that require the use of technologies or processes used to verify that users are over 18.
	Access Control Measures	Measures required under the Phase 2 codes that require the use of tools or settings that restrict access to certain content or services, often based on age.
	Risk Assessments	The process of evaluating the potential for harm to users under the codes, especially children, from

		material on a service, leading to a "risk profile" (e.g., Tier 1, 2, or 3).
	Family Friendly Filter (FFF) Program	A program that certifies internet filters designed to make online content safer for families and children.
	Simulated Gambling App	A third-party app that contains or provides access to computer games classified as R18+ due to simulated gambling.
	Technology stack	The eight sections (categories) of the industry regulated by the OSA.

Appendix B: Structure of Phase 2 codes

Title	Code structure	Section of the online industry to which the code applies	Industry representative
Hosting Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 1	Providers of hosting services, so far as those services host material in Australia	• Australian Telecommunications Alliance (formerly Communications Alliance) (**ATA**) • Digital Industry Group Inc. (**DIGI**)
Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 2	Providers of internet carriage services, so far as those services are provided to customers in Australia	• ATA
Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 3	Providers of internet search engine services, so far as those services are provided to end-users in Australia	• Australian Mobile Telecommunications Association (**AMTA**) • ATA
Social Media Services (Core Features) Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 4	Providers of social media services, so far as those services are provided to end-users in Australia	• ATA • DIGI
Social Media Services (Messaging Features) Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 4A	Providers of social media services, so far as those services are provided to end-users in Australia	• ATA • DIGI
Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 5	Providers of relevant electronic services, so far as those services are provided to end-users in Australia	• ATA • DIGI • AMTA • Interactive Games & Entertainment Association (**IGEA**)

Title	Code structure	Section of the online industry to which the code applies	Industry representative
Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 6	Providers of designated internet services, so far as those services are provided to end-users in Australia, but excluding OS providers (as defined in Schedule 8)	• ATA • DIGI • AMTA • Consumers Electronic Suppliers' Association (**CESA**)
App Distribution Services Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 7	Providers of app distribution services, so far as those services are provided to end-users in Australia	• ATA • DIGI • IGEA
Equipment Online Safety Code (Class 1C and Class 2 Material)	Head Terms + Schedule 8	Persons who manufacture, supply, maintain or install equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service (in each case in connection with the service) OS providers (as defined in Schedule 8)	• AMTA • ATA • CESA • DIGI • IGEA

Appendix C: Key Measures in Phase 2 codes

Industry Section	Age Assurance Measures	Measures that require other Tools/ systems and processes to limit/restrict exposure
Social Media Services that permit high priority Class2 materials	Yes. To access online pornography and/or self-harm material (inc suicide and eating disorder materials) if permitted by the service's policies and to access AI Companion Chatbot features where there is a medium to high risk that that they will generate this material.	Yes e.g interstitial notices. blurring, halting autoplay, filters, delisting or deprioritising materials.
Social Media services that do not permit Class 2 materials	Yes to access AI Companion Chatbot features as above	Yes. Services must detect and remove online pornography, self-harm material and high-impact violence material, and to continuously improve systems, processes and technologies used for this purpose.
Relevant Electronic Service Providers (inc messaging, email services, online games, dating services, SMs, MMs services)	Yes. To access a relevant electronic service with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material. To access 18+games such as Simulated Gambling Apps To access AI chatbot features as above	Yes. For example, messaging and email services and dating services must have appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material . Messaging /chat type services must enable users to block other users and leave a group chat.

Industry Section	Age Assurance Measures	Measures that require other Tools/ systems and processes to limit/restrict exposure
Designated Internet Services	Yes: pornography sites (High Impact Class2 DIS) must restrict access to pornography to those under 18 . In addition, medium to high risk generative AI services (High Impact Class 2 Generative AI DIS), such as many companion chatbots, to either prevent the generation of, or restrict under 18s from pornography, high-impact sexually explicit material, self-harm material, high-impact violence material, and violence instruction material	Yes. For example, services that carry 18+ and X18+ films or computer games(High Impact Classified Materials) will need to offer parental controls on their services.
Equipment Providers	No	Yes. Certain providers of interactive equipment commonly used by children such as mobile phones and tablets and OS providers must implement a range of measures, including specific requirements on OS providers to enable parents or guardians to set up child profiles with appropriate default safety settings. These measures provide a supplementary level of protection for child users to the other codes. The Equipment code also enables the sharing of age assurance information from OS providers among their related services (e.g., app stores) to minimise unnecessary data sharing. Where technically feasible and reasonably practicable, relevant providers must take appropriate steps to further develop and improve the safety tools, features and/or settings

Industry Section	Age Assurance Measures	Measures that require other Tools/ systems and processes to limit/restrict exposure
ISPs	No	No. Instead ISP's must promote family friendly filters to customers and use best efforts to address compatibility issues of proprietary filters, and, where technically feasible and reasonably practicable, ensure compatibility of filters and the internet service. In addition, ISPs providing proprietary filters must, where it is technically feasible and reasonably practical, continuously update their filters, including the product's parental controls, and, where updates have occurred, provide information on such updates to end-users in a timely manner.
Hosting Services. (Third Party Hosting Services)	No	No. Instead hosting services must require and take steps to enforce code requirements via their contracts with hosted services such as adult websites.
Internet Search Engine Services	Yes providers must conduct age assurance for all logged-in users	Yes. By default, pornographic and violent material is blurred for logged out users. The code also requires providers to apply additional protections for all users which are automatically applied without the user needing to opt-in. These include requirements to prevent, for all users, pornography and violence from appearing in search results for search queries that do not intend to solicit the material and autocomplete predictions that are sexually explicit or violent. The Internet Search Engine Services code also requires services to promote trustworthy content over self-harm material, prevent autocomplete predictions seeking self-harm material,

Industry Section	Age Assurance Measures	Measures that require other Tools/ systems and processes to limit/restrict exposure
		and provide crisis information for all users.
App Distribution Services	Yes. An app store provider must restrict users under 18 from downloading apps rated unsuitable for that age range.	