Submissions log and industry associations'[1] responses to public consultation feedback

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
1	ACCAN	No comment on Codes as such. Generally welcoming of safety & transparency enhancing measures etc.	Consultation	General	Highlighting concern with short consultation timeframe. Generally recommending early and broad consultation.	Please note that more extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
2	ACCAN		Appeal and redress	All Codes	There is little detail about processes for users to appeal decisions or seek redress for loss of content or account access. Consumers will require clarity about how they can appeal decisions and seek redress It is not clear whether the Draft Codes' instructions for services to provide consumers with tools to complain about code compliance would cover the eSafety Commission acting as an external avenue for appeal. In the case of the Draft Codes, we feel that the eSafety Commission should be explicitly included as an avenue for consumers to appeal decisions made under the Codes and minimise consumer harm from incorrect decisions.	In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.
3	ACCAN		Application of National Classification Scheme to scale	All Codes	Concern that the National Classification Scheme is not fit to be applied to the internet due to grey areas. ACCAN is worried that the scale of content covered by the scheme and detection through automated scanning and crowd sourced flagging could lead to false positives where innocent consumers may lose access to crucial means of communication. Concern with resultant false positives and consequences (e.g. example of penis picture sent to doctor)	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1 Materials as defined in the OSA by reference to the National Classification Scheme. See above response re appeals.
4	Alannah & Madeline Foundation (AMF)	Measured approach; not critical but not positive endorsement of Codes i.e., can be improved.	Consultation	General	Need for extended consultation/expert input from Non for profits which work with children. Align approach with National Principles for Child Safe Organisations.	Non-profits that work with children have provided input into the consultation process both via the submissions process and the stakeholder roundtable conducted by the Steering Group. Please note that more extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.

[1] Comprised of the Australian Mobile Telecommunications Association (**AMTA**), BSA | The Software Alliance (**BSA**), Communications Alliance Ltd (**CA**), Consumer Electronics Suppliers Association (**CESA**), Digital Industry Group Inc. (**DIGI**) and Interactive Games and Entertainment Association (**IGEA**).

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
						The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback from eSafety provided throughout the drafting process) and by the OSA. As a result, the scope of the Codes primarily concerns Class 1 Materials informed by the OSA and the eSafety Commissioner's recommended approaches.
5	Alannah & Madeline Foundation (AMF)		Communication	General	Communicate how the Codes will better enable industry participants to work alongside public bodies to achieve agreed beneficial outcomes. Greater clarity about how the Codes align with the work of the Australian Centre to Counter Child Exploitation.	As set out in the eSafety Commissioner's Position Paper the scope of the Codes primarily concerns Class1 Materials which are equivalent to content that would be refused classification under the National Classification Scheme. The Codes are therefore generally aligned with that scheme and the eSafety Commissioner's expectations rather than with the laws such as laws that make child sexual abuse material illegal and the work that is done by bodies such as the ACCCE to enforce those laws.
6	Alannah & Madeline Foundation (AMF)		Measures relating to reporting PT and CSEM	Various	Codes measures should align with legislation requiring reporting of this material. Consider referring to these legislative obligations.	We have taken this feedback on board and clarified that the Code measures concerning reporting to law enforcement . are supplementary to Australian legislation that requires reporting of this material.
7	Alannah & Madeline Foundation (AMF)		Approach to risk assessment	RES, DIS and SMS in particular	Greater clarity about how participants assess risk overall. Each product or service should be assessed and reported upon at a tier level that is high enough to address the risks attached to that particular product or service. Where service can fall in more than one service category, should elect for code that offers the highest degree of protection.	The approach to risk is DIS has been clarified. We consider the approach in SMS and RES to be clear. The Code has also been amended to incentivise SMS, DIS, RES service providers to declare a Tier 1 status to the Commissioner on or prior to commencement of the Code (i.e. those participants need not carry out a risk assessment as they are automatically subject to the most stringent compliance measures) We consider the approach to risk assessment and reporting will ensure services are assessed and reported upon at an appropriate tier level, given the powers of the eSafety Commissioner to investigate and enforce Code breaches under the OSA. The question of how a service is categorised under the Codes must be determined by services in accordance with the definitions in the OSA. It should be noted that these definitions are very broad and potentially overlapping and can in some cases be amended by legislative instrument. eSafety feedback to industry during the drafting process was that these definitions should not be altered by these Codes. The flexible approach to risk was considered necessary because of these definitional challenges, the diverse companies in

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter’s comment	Industry associations’ comment consideration
						scope, the likelihood that the relevant services and products will evolve over time e.g. as a result of changes to their functionality and scale.
8	Alannah & Madeline Foundation (AMF)		Code review process	Head Terms	Extend consultation period to six weeks. Include targeted engagement with non for profit sector.	See above. Please note that more extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
9	Alannah & Madeline Foundation (AMF)		Reporting	All Codes	Consistent reporting requirements for at least all Tier 1 services. Articulate measures or indicators of change to sit beneath the nine topics listed for minimum consideration at each code review, so that code reviewers and eSafety can make an accurate assessment of how industry outcomes are changing over time. Develop with researchers a meaningful estimate of the impact of the Codes on public safety over time, to support continuous improvement.	The assessment of Codes compliance and effectiveness will be determined by the eSafety Commissioner under the OSA. We note that while the industry initially proposed a more flexible principles-based approach, eSafety feedback over the development process has led to the Codes containing mostly minimum compliance measures. We consider that the key measure for assessing the Codes should therefore be compliance with the measures in the Codes, rather than other metrics.
10	Alannah & Madeline Foundation (AMF)		Strengthen design measures to protect children	(Schedules 1, 2 and 7, Objective 1 Outcome 1; Schedules 3 and 5, Objective 1 Outcome 2; Schedule 8, Objective 2 Outcome	Demonstrate that the approach taken to protecting Australian children is as high, or higher, than that taken in other jurisdictions, within the limits of Australian legislation. For example, we suggest that the United Kingdom’s Children's Code (Age-Appropriate Design Code)	We consider that these issues are more relevant to Class 2 materials that are unsuitable for children of 18 or under and are not within the scope of these Codes. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap. We note that, in contrast to for example the proposed UK legislation (and other in-force international legislation), the Codes apply to a significantly larger range of online industry participants (i.e. they apply to whole categories of companies as opposed to select individual companies) and, do not limit detection of material to a specific period of time (as suggested in the UK legislation).
11	Alannah & Madeline Foundation (AMF)		Strengthen design measures to protect children	Schedules 1-8, Objective 2, Outcome 7)	Information provided to Australian end-users about child safety measures and risks, parental controls, reporting mechanisms, and the role of eSafety should be prominent, timely, concise, up-to-date, and appropriate to different ages and literacy levels. Ideally, such published terms would be developed via engagement with children, young people, parents, and carers.	We have amended the Codes to make clear that safety information must be appropriate for all users including children.
12	Alannah &		Proactive		Undertake that industry participants will work	We note that the Codes seek to impose proactive

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
	Madeline Foundation (AMF)		Detection of CSEM		with eSafety and the community towards an agreed outcome for appropriate detection and actioning of first-generation CSEM and contact between users that could facilitate the production of CSEM. We suggest a preferred approach would involve CSEM being identified and actioned via suitable, effective technology and appropriately qualified and skilled personnel, supported by adequate infrastructure.	detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). In response to feedback, the Code has been amended to extend proactive detection measures to very large Tier 1 relevant electronic services with more than 8 million monthly active Australian accounts and dating services. These measures require highest risk services to deploy the most accurate available approaches to detect CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified. We acknowledge the concern that industry invests in new technologies that can accurately detect first generation materials and supporting infrastructure (as for example is being developed in the EU). We consider that the Codes address this in an appropriate way, for example by requiring ongoing investments in safety by Tier 1 SMS, RES and DIS providers. Both the Outcomes based approach combined with the expectations in the BOSE also incentivise the industry to strive to improve their response to CSAM, including through collaboration with NGOs.
13	Alannah & Madeline Foundation (AMF)		Framing of Expectations	Schedules 1, 2, 3, Objective 1, Outcome 1)	Create separate items in the Codes to address reporting obligations for CSEM and for pro-terror material, in recognition of the different ways Australian law treats these materials.	We have taken this feedback on board and have made amendments to reporting obligations for services to report these materials
14	Alannah & Madeline Foundation (AMF)		Framing of Codes re children	Head Terms and industry Codes, Objective 1)	Amend the Codes to recognise the need to create and maintain a safe online environment for children, whether or not those children are Australian end-users of the specific digital platform.	The Codes contain measures specifically directed at the protection of children online. The Code is not intended to provide a comprehensive response to children's safety online but to Class 1A and Class 1B materials. Many issues associated with protecting children from harmful content are more relevant to Class 2 materials that are unsuitable for children of 18. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap. We have also updated the Codes to refer to the need to have regard to the best interest of interests of children.
15	Alannah & Madeline Foundation (AMF)		Framing of objectives re hosting of CSEM	Head Terms and industry Codes, Objective 1,	Amend the Codes to recognise that ending (not limiting) the hosting of CSEM should be the ultimate goal for industry participants.	We agree that ending CSEM is the ultimate policy goal. We do not believe that the Australian online industry, or indeed the tech industry alone, can achieve that outcome: that can only be achieved by a multi-

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
				Outcome 4		stakeholder approach, including from the relevant agencies and government departments involved in tackling CSEM in Australia and internationally.
16	Alannah & Madeline Foundation (AMF)		Framing of objectives re hosting of CSEM	Objective 2	Updating Objective 2 of the Codes to articulate an end goal of empowering individuals to avoid, report, and be supported to recover from any exposure to CSEM – not merely to 'manage' their own access and exposure.	Objective 2 was worded to reflect the wording of the eSafety Commissioner Position Paper.
17	Alannah & Madeline Foundation (AMF)		Framing of objectives re reporting of Class 1A and Class 1B materials.	(Head Terms and industry Codes, Objective 2, Outcomes 7, 8, 9)	Amend the Codes to recognise that industry participants should ensure that any concerned individual should be able to access their reporting mechanisms, information, and tools about Class 1A and 1B material, and referrals to eSafety – whether or not that individual is an Australian account holder or owner of the digital product.	Note that the OSA limits the jurisdiction of the eSafety to receive and action complaints to those brought by persons ordinarily resident in Australia or companies that carry on activities in Australia, See section 41. We consider that the complaints processes for the Codes should be consistent with the jurisdictional limits applicable to the power of the eSafety Commissioner to hear complaints of Code breaches under the OSA.
18	Alannah & Madeline Foundation (AMF)		Alignment with work of other public entities		Provide clear representation of how the Codes align with the work of relevant public entities (including but not limited to eSafety) and the legislative frameworks these entities operate within. For example, greater clarity around the relationship the Industry Codes under the terms of the Online Safety Act 2021, and their compliance with the Commonwealth Classification Act 1995, and the National Classifications Scheme.	We consider that the Codes have appropriately dealt with this issue, within the constraints of the National Classification Scheme and OSA. Please see the eSafety Position Paper and Annexure A of the Head Terms.
19	Annemarie Butler		Privacy of communications	General	An expectation of privacy. Whether this is in your own home or online. Just as I would not want someone listening in to my conversations in my home I would not want my emails or messages to family, friends or colleagues read by anyone other than the person for whom it was intended. I consider that a justifiable expectation. To violate that goes against hundreds of years of acceptable human interaction.	This concern is noted. The Codes have sought to take into account concerns about user privacy and surveillance. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
20	Annemarie Butler		Infringement on freedom of speech and liberty		No society can be civilised and educated without freedom of speech. Without freedom of speech we open ourselves up to authoritarian dictatorships. If we cannot criticise the government (which could be taken under these rules to be terrorism) then we do not live in a democracy or free country. We cannot have liberty unless we can express	This concern is noted. See above response.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					ourselves without fear of censure or repercussions. "If liberty means anything at all, it means the right to tell people what they do not want to hear." George Orwell	
21	Annemarie Butler		Warrants required		If there is a suspected crime a warrant must be gained with just cause before anyone can violate, liberty, privacy or freedom of speech. Anything else is tyranny.	This concern is noted.
22	Annemarie Butler		Call to abscond online safety restrictions and censorship		Therefore I submit – if we wish to retain liberty, privacy and freedom of speech, the very foundations of a civilised and educated society we must abandon any online safety restrictions or censorship	This concern is noted.
23	ARC/QUT		Pause further development until the Codes can be aligned to the Government's ongoing reform agenda	General	We suggest that the Office of the eSafety Commissioner delays any further development until the Codes can align with and give effect to legislation currently under review. In particular, the Privacy Act review may impose conflicting requirements on service providers. Similarly, the current Codes should not adopt the categories of the outdated and highly controversial existing content classification scheme. The outstanding classification review will hopefully enact the recommendations made by previous reviews to develop a cohesive classification framework for a converged media landscape. The Codes should also clarify what the overlap is between obligations relating to Class 1A and 1B material and material covered by the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019	Noted. We consider that these are issues that would need to be addressed by the eSafety Commissioner and by State and Federal governments.
24	ARC/QUT		Scope; coverage thresholds/competition impact concerns	General	The most substantial obligations under the draft Codes generally reflect current practices of well-resourced technology companies. These practices are not at all standard across smaller commercial and community providers. There has been extensive concern about the harmful impacts of limiting competition by increasing regulatory compliance costs without regard to the size of the provider. We note that the Office has provided some assurances that regulatory burdens will not be disproportionate, but we do not have sufficient information available to evaluate this risk at	Noted. The eSafety Commissioner could address these concerns in policies for the enforcement of Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					this time.	
25	ARC/QUT		Proactive detection	Outcome 1, SMS. DIS	The enacting legislation does not create obligations on service providers to proactively monitor communications over their networks. This was a deliberate choice and an integral component of the policy debates in the lead-up to the passage of the Online Safety Act 2021(Cth).Automated content classifiers consistently under-include harmful material that is targeted at members of marginalised groups, and they disproportionately include false positives for content originating from marginalised groups. High quality automated detection of harmful content is extremely difficult, and becomes exponentially more difficult as the scope of content targeted is increased. Machine learning classifiers are improving, but they are only appropriate for monitoring purposes in limited circumstances. The Codes should not be extended to require monitoring beyond matching of copies of unlawful material. The current draft Codes require automated detection of known instances of child abuse material. This technology uses hash-matching and other techniques that are generally reliable, and this category of material is usually clearly unlawful to possess or distribute. The risks of this type of automation for unlawful content are relatively much lower – although false positives are still common.	We acknowledge these concerns and note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). Following feedback these proactive detection measures have been extended to very large Tier 1 relevant electronic services and dating services. Very large Tier 1 relevant electronic services and social media services are also subject to new measures requiring proactive detection of certain pro-terror imagery and videos. These measures require these services to deploy the most accurate available approaches to detect CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users (including vulnerable and marginalised groups) are subjected to inappropriate enforcement action where materials are inaccurately identified. Guidance for these measures has been updated to make these risks clear. We consider that additional support for the development and broader use of proactive detection technology and the development of a supporting infrastructure to assist in its accurate deployment cannot be readily dealt with under these Codes and is best dealt with by other policy approaches including collaboration with NGOs.
26	ARC/QUT		Prohibition, deranking, and takedown for lawful material	General ; Head Terms, All provisions relating to Class 1B and Class 1A material that is not unlawful.	There is clear public support for the prohibition of child abuse material and some extremist content. There is much less public support for the prohibition of lawful material. The RC category in Australia's outdated classification scheme is well-known to be overbroad. It includes a great deal of content that is legal to produce, consume, possess, and distribute in Australia. A content scheme that uses the outdated RC category is not likely to have the same degree of support from the public as a more narrowly tailored one would. The larger the scope of content that is prohibited, the less it is likely to be routinely enforced. One of the major failings of the content classification regime under the Broadcasting Services Act 1992 (Cth) was that	This concern is noted. The development of the Codes is constrained both by the OSA that defines the content categories in the Codes and in the expectations outlined in the eSafety Commissioner's Position Paper. We have attempted to define the scope of materials covered by the Codes in Annexure A to the Head terms with as much clarity as possible within these constraints.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					it was practically unenforceable. Schedules 5 and 7 of the Act were not widely used, and the industry Codes never worked to effectively restrict access to RC material. The new regulatory regime should not repeat the same mistakes. Until the Government acts to modernise Australia's classification regime and creates a more coherent and certain approach to prohibited material, we suggest that the automated detection, complaints, removal, and downranking mechanisms in the Codes be limited to clearly unlawful material under Class 1A.	
27	ARC/QUT		access to data for independent research	Additional measures suggested	We suggest that the Codes build on the commitments to transparency and accountability developed in the Australian Code of Practice on Disinformation and Misinformation. 3 The Disinformation Code includes commitments from industry to 'support and encourage good faith independent efforts to research Disinformation and Misinformation', including through 'funding for research and/or sharing datasets, undertaking joint research, or otherwise partnering with academics and civil society organisations'. Critically, that Code includes a commitment that industry stakeholders will not 'prohibit or discourage good faith research … on their platforms'. These commitments should be mirrored in the current Codes under consideration.	Provision has been made for an optional compliance measure in measure 17 of Schedule 1 (SMS Code). We hope that the Outcomes based approach of the Codes will incentivise industry to offer greater support for researchers in relation to Class 1 materials.
28	Asia Internet Coalition	The Asia Internet Coalition (AIC) supports the codification of various efforts and emerging good practices across all eight of the sectors of industry to address online safety challenges.	Scope of Codes ; use of National Classification scheme to regulate online materials	General	Relying on this scheme creates significant challenges for industry due to their broad and outdated nature. The complexity and scope will require a significant investment of resources, leading to an unequal playing field, where smaller companies or new entrants to the market are not able to meet the demands.	We note this concern. We have sought to address the concern about the application of the Codes to smaller businesses/new entrants to the market in section 5.1(b)(iv) of the Head Terms.
29	Asia Internet Coalition		Scope of Code threat of penalties for noncompliance with Codes		the broad coverage of issues and the penalties attached for non-compliance may have a chilling impact on human rights as companies will have to take a blanket/generous approach to the	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback through the drafting process) the OSA. As a result, the scope of the Codes primarily concerns Class 1A and Class 1B materials. The Codes are therefore

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			incentivises companies to remove content that may not be in scope		implementation of the Codes.	aligned with the OSA and the National Classification Scheme which outlines how classification decisions should be approached. This is reflected in Annexure A of the Head Terms. We have sought to ensure participants implementing measures under the Code have regard to the importance of protecting and promoting human rights online. See section 5.1(b)(iii) of the Head Terms.
30	Asia Internet Coalition		Risk of inconsistent decisions around classification of materials		The extremely vague nature of 'Class 1' and 'Class 2' material means that content removal decisions will be judgment calls made by companies, resulting in a mish-mash of content decisions, with content left up on one platform and removed in another.	section 3(g) of the Head Terms acknowledges the inherent challenge of applying concepts in the National Classification Scheme to all categories of online content at scale. The eSafety Commissioner has not published any guidance about how content should be classified under the OSA Code. Should such guidance be published, this may assist in addressing this issue.
31	Asia Internet Coalition		Requirements to proactively detect Class 1 materials and Class2 materials) in Position Paper	Outcome 1	AIC notes that the Online Safety Act itself does not require industry to proactively detect and remove 'Class 1' (refused classification under the National Classification scheme) and 'Class 2' (material that is X+ 18 or R+18 under National Classification scheme) content, but rather remove this type of content after receiving a 'removal notice' from the Office of the E-safety Commissioner. It is surprising and dismaying, then, that the Office of the E-safety Commissioner in its 2021 Position Paper expects industry to proactively identify and remove 'Class 1' and 'Class 2' content. Requiring the proactive detection and removal of content is thus extra-legal, in addition to the challenges and limitations of the required detection and removal in practice. It also threatens the principles of online privacy, transparency and due process. We are particularly concerned about the potential for this problematic approach that requires judgment calls to be replicated across the region. These proactive detection and removal approaches and tool for vaguely defined content would be used for a very different purpose in certain markets – including for stifling political dissent under the guise of "crime" and "terror", leading to gross human rights Violations.	Noted. We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categories as Tier 1 (highest risk). Following feedback, proactive detection measures have been extended to very large Tier 1 relevant electronic services with more than 8 million monthly active Australian accounts and dating services. These measures require these services to deploy the most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified. Please see the response above about how human rights considerations are addressed in the section 5.1 of the Head Terms.
32	Asia Internet Coalition		Proactive detection of	DIS/SMS	There is a globally-accepted and widely-used system for the identification of 'known CSAM'	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			known CSAM measures		– a narrow subset of Class 1A material. We agree with the Code's attempt to stress the importance of utilizing the known CSAM 'hash' lists, which are lists of materials that have been vetted and approved by specialized third parties. This approach for known CSAM reduces the chances of false positives and promotes a more streamlined and transparent approach to content removal.	
33	Asia Internet Coalition		Proactive detection of categories of Class 1A and! B materials other than known CSAM		For all other areas of Class 1A and Class 1B content, the Codes expect companies to self-manage its identification and potential removal. As mentioned this will result in individual companies making ad-hoc decisions about content removal, invariably leading to the removal of content that is perfectly legitimate. There is a widespread practice of weaponizing abuse processes against legitimate content, further highlighting the risk of its removal.	Noted. See response above concerning how section 3(g) of the Head Terms deal with the issues associated with applying the National Classification Scheme at scale online.
34	Asia Internet Coalition		Limitations of proactive detection technology	Outcome 1	Proactive detection is a challenging area, largely due to the inability of the technology to assess context. Often relying on technology that is still in development. Where the technology is being utilised, it is often limited to large players, again excluding smaller companies and newer entrants. Expanding proactive detection to private communications and file storage will also have significant impacts on users' right to privacy.	Noted. The Codes do not contain minimum compliance measures requiring the deployment of proactive detection technology on file storage services. Following feedback, the Codes have been amended to include proactive detection by very large Tier 1 relevant electronic services with over 8 million monthly active Australian accounts and dating services. These measures require these services to deploy the most accurate available approaches to detecting CSEM online (See above response).
35	Asia Internet Coalition		DIS approach to Tiers	DIS risk assessment methodology	The current phrasing shows that Tier 1 website's sole purpose is to deliver 'high impact' materials. There is no clear definition of what constitutes 'high impact'. Considering the extremely challenging compliance requirements associated with Tier 1, it should be made crystal clear that Tier 1 is a very specialized, subset of content (for example, websites specizalizing in pornography). Tier 2's definition is extremely vague, which is particularly worrying as Tier 2 also faces extremely high compliance requirements.	We have taken this feedback on board and provided clarification about the approach to risk in Schedule 3 (DIS Code).
36	Asia Internet Coalition		Approach to risk assessment in Codes	DIS, RES, SMS	We welcome the flexible risk assessment model that is built into the Codes. This will ensure companies can develop and integrate risk assessments that are fit for purpose and	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					ultimately, the longevity of the Codes.	
37	Assembly Four	Negative. The Industry Codes must be halted until the completion of policy review and subsequent legislative changes regarding privacy, classification and surveillance to prevent unnecessary harm and cost to the Australian population and economy.			We have the chance to make the internet a safer place for all. The cost of getting this wrong is catastrophic and guaranteed if this process is to continue prior to privacy and classification reform.	We note this concern but consider that this issue can only be addressed by the government, rather than industry.
38	Australian Child Rights Task Force	The Codes do not reflect or align with existing international best practice. They fail to ensure that monitoring and regulation will support and protect children's rights in the digital world. There is minimal evidence of a consistent focus on identifying risk, addressing harms, enabling prevention of harm, and creating child-safe environments online. For the purposes of the Online Safety Act's process of development, the draft Codes do not meet or provide appropriate community standards. The Codes should not be registered	Proactive detection and reporting measures; scope	Outcome 1	Of particular concern to the Taskforce is the lack of clear, unambiguous acceptance of the need to proactively detect and report material and activities relating to child abuse (including child sexual abuse). Given that it is generally accepted (and legislated in many jurisdictions) that community members should report evidence of abuse, it clearly falls below the required community standard, that industry should not share this responsibility.	We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categories as Tier 1 (highest risk). Following feedback these measures were extended to very large relevant electronic services and dating services. (See Schedule 2.) These measures require these services to deploy the most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified. The measures in the Codes concerning reporting of CSEM and pro terror material to law enforcement were drafted to take into account the need for services to comply with the Privacy Act 1988 (Cth), which provides limited circumstances in which personal information can be provided to law enforcement. In response to feedback, these requirements supplement existing reporting obligations in State legislation.
39	Australian Child Rights Task Force		Approach to risk assessments by services		Risk assessments allow for significant exercise of discretion in reviewing and assessing content and in the required level of response to harm.	We consider the approach to risk assessment and reporting will ensure services are assessed and reported upon at an appropriate tier level, given the powers of the eSafety Commissioner to investigate and enforce Code breaches under the OSA. We consider that the approach to risk assessment is appropriate given the broad definitions of the

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
						products/services that are subject to the Codes under the OSA, the diversity of businesses in scope of the Codes and the likelihood that relevant services and products will evolve over time. For example, by expanding their user base or adding new functionalities to their service.
40	Australian Child Rights Task Force		Scope ; limited to Class 1A and Class 1B materials		There should be better evidence in the Codes of the need to understand and address experiences of online bullying and harassment and mental health impacts. The proposed social media Codes only focus on 'child sexual exploitation material and pro-terror content'. There is an obvious need to protect children from online sales of harmful products. The sale of e-cigarettes (Vapes) is an example given access via social media platforms and the serious harm. A more comprehensive approach and understanding of risk, safety and harm would recognise the impacts of online advertising and sales and the socialising of dangerous behaviours and exposure to unsafe environments. We would support recognition of the increased risks of exposure to harms to health (such as junk food, alcohol, gambling and tobacco) through advertising and socialisation by commercial interests supported by industry	We note that these are important issues, but they are out of scope of these Codes which address Class 1A and Class 1B materials under the OSA Online Content Scheme.
41	Australian Child Rights Task Force		Use of GPS location data of children	Privacy of children	At the least, the Codes should reflect a prohibition on the collection of GPS location datas to address risk of misuse or safety breaches.	We consider that this issue is best addressed by the Privacy Act 1988 (Cth) (under review).
42	Australian Child Rights Task Force		Consultation	General	Codes development calls for a transparent and comprehensive examination of international best practice and the opportunity for informed and engaged public debate and discussion. We support the more detailed analysis provided by Reset Tech in its submission. The examination and debate should be led by an independent facilitator (such as the eSafety Commissioner) and properly resourced to allow for full and effective community engagement. There should be appropriate research into the most effective regulation for the industry	
43	Australian				Endorsing IIS Partners submission	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
	Information Security Association (AISA)					
44	Australian Information Security Association (AISA)		eSafety and the wider policy context	General	IIS observed that commentary in relation to complementary areas of public policy – such as discussed in the eSafety Position Paper (Other relevant Australian Codes), the Australian Competition & Consumer Commission's (ACCC's) ongoing Digital Platform Services Inquiry, initiatives of the Australian Cyber Security Centre (ACSC), the Australian Information and eSafety Commissioners' involvement in the Digital Platform Regulators Forum, etc. – was largely missing. We agree with IIS' perspective that this omission is a lost opportunity. IIS considered that the Explanatory Paper for the proposed Codes is a meaningful opportunity for the Code Developers to clarify how key online safety concepts are enmeshed with other Australian public policy imperatives. Additionally, material covered in the Explanatory Paper may – at an appropriate juncture – form the basis for Guidelines (on the operation of the Codes) and other educational materials for industry and the community more broadly. Recommendation: Discuss the areas of Australian public policy that are complementary to online safety within the explanatory memoranda for the proposed Codes.	We consider that this clarification would best be provided by government rather than industry, given that these policy areas are constantly evolving.
45	Australian Information Security Association (AISA)			Head Terms 6.1	In support of the limitation listed in 6.1 with respect to the key online safety objectives and outcomes 1-3. AISA also notes that "reasonable and proactive steps" with respect to information security to support the Codes, will mean different things to each organisation. As noted in the section above with respect to "Complementary areas of public policy," above, AISA emphasises the need to harmonise the Codes with current and evolving regulation with respect to privacy and information security and notes that weak information security in particular can lead to devastating online safety issues, like use of exploited servers to provide harmful online	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					content or to defeat measures to prevent, detect and address it	
46	BCR, Joshua Gavin Alex Jenner-Rossi, Brenan Kitcher, Josh Hopkins, Rowan Lysaught, Liam Brown, Kieran Nichols, Joshua Millwood, Michael Alderman, Thomas Abley, Joseph Caelli,Hamish Paterson, Aaron Clarke, Daniel Dompierre-Outridge, Andrew Miller		Systemic weakness	Head Terms 6.1(a)	Define systemic weakness but given the difficulty of doing so, preferred option, leave out 'systemic' in 6.1.	The industry is comfortable that this terminology can be readily interpreted by participants.
47	BCR et al.		Importance preserving practice of pseudonyms and anonymous users	Head Terms 6.1(f)	"(though an industry participant may be required to adopt compliance measures that are intended to prevent end-users from exploiting anonymity or other identity shielding techniques to share harmful material)". I suggest that this parenthetical information be deleted. The online safety risks from measures that ban pseudonymous interaction are far greater than the benefits of requiring providers to identify users: Data breaches are the greatest online safety threat facing users today - and the data from these breaches are often sold by criminals, to other criminals, to be used for criminal purposes. Pseudonymous services allow users to compartmentalise their identity, so that if all information a provider holds on them is breached, the impact is limited to that service (and some users might even interact with the same service under multiple pseudonyms, to keep different realms - e.g. professional and personal - separate to each other), and so are a major tool users have to protect their online safety. Unintentional data leaks aside, there is also a significant risk to users that data required to be collected by industry participants will be used by the organisation collecting it for	We think the language here is sufficiently clear that anonymity is not banned; only the exploitation of anonymity for sharing harmful materials.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					purposes other than the purposes of the code. A requirement to collect 'real' PII would increase that risk. Furthermore, banning pseudonymous activity could also cause users to self-censor non-harmful content; for example, people might be less likely to share personal details and build strong connections with others online if everything they say might be leaked against their real identity. They might not be as willing to get involved online in political activism, or in presenting innovative ideas that might or might not work. These types of connection are increasingly important in Australia as we recover from COVID-19, and an industry code that might require identity verification would be a net negative for society Therefore: redraft (f) to "collect, verify, store, retain, or publish the real identity (or any other personally identifiable information) of any end-user"	
48	BCR et al.		Data minimisation	Against background of 6.1(f)	Recommendation of data minimisation, especially for personally identifiable information	Data minimisation principles are part of the AAPs under the Privacy Act. We consider that any changes to that principle would properly be dealt with by changes to privacy laws.
49	BCR et al.		Scope of services covered	SMS, 2.1 Note: where similar concerns apply in other Codes, they have not been repeated.	This is likely a significant burden to smaller services, disproportionate with any risks. I suggest in addition to 3(d), the section of the code only applies to services that expect to have 10,000 or more monthly active users - even if other criteria are not met	We acknowledge this concern and have sought to address this issue in 5.1(b) (iv) of the Head Terms. It is open to the Office of the eSafety Commissioner to further address this issue in their policy on Code enforcement. Note that Schedule 1 operates to automatically class some services as Tier 3 but does not prevent other services being categorised as Tier 3.
50	BCR et al.		Termination of an account	SMS, MCM 3(c)	There are several reasons why permanent termination might be unreasonable: As in the above case study, the material might have been misidentified due to missing context. Alternatively, there might be doubt about which individual submitted the material. This can happen in several ways: criminals commonly use the resources of other people - for example, they might connect to unprotected wi, or compromise a computer. In addition, it is a common tactic by bullies to frame victims of bullying in ways that have negative consequences for the victims - this	Noted. These contextual considerations would be taken into account by providers in taking enforcement action pursuant to these measures.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					behaviour can start as graffiti on a school desk attributed to the victim, but it is not a far stretch from that for bully to access a device of a victim and post something the bully knows will result in that victim being banned from a crucial social media network for life. In addition, even if someone genuinely posted the material, there should be some recognition that they might eventually serve a sentence and be remorseful and rehabilitated, and hence it would be disproportionate to never allow them to return. On the aspect of ensuring the response is restricted to features that could cause harm, I suggest replacing terminate an end-user's account with suspend an end-user's ability to submit content to be viewed by other users without manual review by staff.	
51	BCR et al.		Appeals mechanism missing	SMS, MCM 3(c)	In addition, to avoid the code being used as a mechanism to enable cyberbullying, it should add a new requirement: (d) provide a genuine appeal process that: (i) allows end-users to appeal on any grounds the end-user chooses, and attach supporting documentation the end-user deems relevant; (ii) includes review by at least one staff member with genuine discretion and authority to reinstate the user's access or to deny the appeal; (iii) provides for reinstation of access unless it is satisfied, after considering all evidence, that the individual end-user personally submitted the material to the account, that the material was genuinely CSEM or pro-terror material, and that the end-user has not already been cleared, acquitted, discharged, or completed any sentence (including any period in which they are forbidden to use the service under any conditions of probation). (iv) prohibits the use of information provided in the appeal for any purpose other than determining the appeal (except where the information provided for the appeal is itself abusive or illegal, or as required by law).	In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.
52	BCR et al.		Re-creation of accounts by 'bad actors'	SMS, MCM 3(d)	The guidance suggests a reasonable measure is to block new accounts: created from that device or IP address either indefinitely or for a period of time This is not a reasonably practical measure, because IP addresses	Noted. In response to feedback, the guidance has been updated to reference blocking the identifier used for registration.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					often change regularly (due to dynamic IP address allocation practices), and also are often shared between end-users (for example, due to technologies such as Carrier Grade Network Address Translation - CGNAT - which is increasingly being deployed due to exhaustion of the IPv4 address pool). Many platforms - including the web platform - deploy countermeasures to reduce the risk of fingerprinting of users other than through socially supported measures such as cookies, and provide ways to clear cookies, and so obtaining a consistent user identifier is (rightfully) difficult. Attempting to implement this would simply result in other users being caught as collateral damage. The only practical ways to support 6.3(d) are invasive measures such as requiring verification of personally identifiable information from users, which, for the reasons discussed earlier in this submission, are a net negative for users. I suggest removing 6.3(d) entirely	
53	BCR et al.		SbD material can only be uploaded by a registered user	SMS, MCM 6 (a)	Argument that this, strictly applied, bans anonymous accounts. In turn, many widely used protocols and mail servers which do not require registration are classified as social media service. Therefore, MCM 6(a) breaks interoperability, removes choices, entrenches dominance of overseas players etc. and ought to be removed. Please refer to submission for details (p. 6 submission)	We note this concern but do not think that this prohibits anonymity per se. See section 6.1(f) of the Head Terms which makes it clear that the Codes do not have this effect.
54	BCR et al.		Detection and removal of known CSAM	SMS, MCM 8(a)	This requirement is problematic for smaller providers (which might still be classified as tier 1 due to the nature of their services, and might have low operating budgets) - especially those hosting federated services, because databases of known hashes are not generally published. Until there is an entirely openly available database of hashes available freely, this should not be a requirement. This would be less onerous if it only covered exact matches of files that the same provider had already removed. As it is, it will create barriers to entry and mean that only large companies can operate services that would be classified as tier 1.	Noted. Please see responses about small businesses above.
55	BCR et al.		Overburdening	SMS, MCM 9,	The requirement that potentially tiny tier 1	Noted. The eSafety Commissioner could address these

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			small Tier 1 SMS with investment requirements	14, 15, 19, 32	providers need to invest in novel research will essentially mean that only large companies can operate services that would be classified as tier 1. I suggest removing this requirement.	concerns in policies for the enforcement of these Codes.
56	BCR et al.		Registration of users	RES, MCM 7	I think the requirement that a user `register' is unclear as to whether or not the service or system can assign an identifier to the user (rather than using a pre-existing identifier). Assigning an identifier to a user is a reasonable technical measure. However, it is not clear what the benefit of the requirement to register actually is - so I suggest deleting it	These measures reflect industry best practice and assist participants to ensure that only account holders have accountability for uploading content and compliance with terms and conditions.
57	BCR et al.		Participation in industry forum	RES, MCM 15	This requirement could particularly be very onerous (or even impossible if no such forum is available) - especially for small providers, and if there are fees to take part in the forum, or it requires travel.	We note this concern and consider that ways for smaller RES businesses to participate can be addressed when forums are being established. In response to feedback, we made clear that online participate must be an option, thereby reducing the financial burden on smaller providers (travel).
58	BCR et al.		Info provision of role eSafety and how to make a complaint	RES, MCM 18	Where providers offer federated or hosted open source services that use clients developed by a third party, there might not be a reasonable way to implement this.	Noted. This concern was not clear to us but we also do not see a means to address it without exempting these services – something that the framework parameters do not allow us to do. It is within eSafety's discretion to enforce the Codes accordingly.
59	BCR et al.		Detection and removal of known CSAM	DIS, MCM 6	Some services to which the schedule applies do not even have user-supplied content. As such, they would have non-technological mechanisms to achieve the same thing. Manual review of 100% of all content is the gold standard, so the standard should only apply to user-submitted content. In addition, some types of services encrypt data end-to-end, so that the provider does not have the technical means to scan the plain-text data.	Noted. MCM 6 only applies to the highest risk Tier 1 DIS such as pornography sites. We consider that the measure should apply to all content on Tier 1 DIS and not just UGC. See section 6.1 of the Head Terms which makes clear that the Codes cannot undermine encryption.
60	BCR et al.		Agreements with third-party app providers	Apps, MCM 1(a)	This would essentially prohibit or greatly limit app distribution providers which collect third party Free / Open Source apps and distribute them on their own initiative - for example, the F-Droid app store. F-Droid works by collecting apps which are provided under an open source license (i.e. software for which the source code is available and which is distributed on terms that it can be redistributed and modied by others, subject to conditions), and providing them to users. The apps in it are typically much less abusive of	Noted. eSafety provided feedback to industry that it could not exempt services in scope from the Codes. It is open to the government to provide legislative exemptions for open source apps. As a general principle, however, we do not think special treatment is appropriate.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					users rights (for example, because they are Open Source, they typically do not track users and collect PII to send back to the app producer, unlike many apps in commercial app stores). As such, F-Droid is a currently legal service that is a positive thing for online safety. App providers do not ask F-Droid to list their apps; instead, they are licensed and put publicly on the Internet by app authors, and are then gathered by volunteer contributors to the project. As such, F-Droid do not have a relationship with app providers, they rely on licenses unilaterally offered to anyone by the authors. For F-Droid to continue operating, they would need to get all the app authors to agree to something - and it is likely that if they are approached by an organisation they have no relationship to and be asked to sign something in relation to software they have agreed to make available for free, that many might decline. In some cases, one piece of software might have been started by one author, who could even now be deceased, and been continued by other authors - as written now even the deceased author might be treated as a third party app provider. Perhaps this could be mitigated if Open Source apps were exempted from the code / treated as 1st party	
61	BCR et al.		Content ratings	Apps, MCM 3	Many apps are very generic - for example, a browser app or an ebook reader app. Neither the maker of the app nor the app store reasonably can control what content a user will load in the app. It should be made clear that such apps do not need to be rated based on the worst possible thing that could be loaded (and especially should not be removed on those grounds.	Noted. We think that this issue is addressed in the guidance for MCM 3.
62	BCR et al.		Family Friendly Filter (FFF)	ISP, MCM 9	It is inappropriate to use a legally binding code to promote a particular service, especially if it is a service which providers must pay one of the developers of the code or its partners to be listed under. This should be removed.	Noted.
63	BCR et al.		Tools within the OS to reduce risk of harm to children, incl.	Equipment, MCM 6	Free / Open Source OS providers should be exempt from these requirements, because anyone installing the OS on a device would be able to modify the software if needed.	Noted, however we do not think that Open Source providers should have lesser obligations than proprietary systems providers to address these risks.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			Default settings		Otherwise, this could be unreasonably burdensome on small community efforts.	
64	BCR et al.		Annual forums, reporting	Equipment, MCM 1 and 13	These are likely to be particularly burdensome to small providers of Linux distributions - it could actually total a higher time commitment compared to developing a basic distribution (as an adaptation from an existing system) in some cases. Exempting Free / Open Source Operating Systems / distributions from the requirements would avoid this.	Noted. We note this concern and consider that ways for smaller businesses to participate can be addressed when forums are being established. In response to feedback, we made clear that online participation must be an option, thereby reducing the financial burden on smaller providers (travel).
65	Chris Skelton	The Online Safety Codes are unacceptably broad, over-reaching, harmful, and open to abuse by dishonest government. They should not be implemented.	Reduced anonymity and lack of data minimisation, thereby increasing risk	General	Regarding the proposed online safety Codes, it should be noted that behind the cover of protecting children from sex and terrorists; practical policy outcomes can include measures that: - Increase online storage requirements for personal identifying information. - Reduce anonymity of online actors While the Codes may propose legislative measures to protect against these, data security is unique in that bans, punishments, and compensations do not undo the damage done by a breach. The fundamental truth is that "The most secure data is uncollected data." As a result, the Online Safety Codes may unintentionally increase risks of: - Identity theft, fraud, cyberscams	We have taken this concern on board and clarified in the Head Terms that the Codes do not require implementation of age assurance measures. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
66	Chris Skelton		Increased costs and liabilities for services, even those that support victims etc.	General	- Increase running costs and liabilities for services that include any type of file/image hosting. - Increase running costs and liabilities for support services that discuss child abuse, violence, etc. As a result, the Online Safety Codes may unintentionally increase risks of: - Reduced accessibility to support services for survivors of trauma - Hobble small and startup - Reduced freedom of expression for all Australians.	We acknowledge this concern. We have sought to address the potential impact on small businesses/start ups in section 5.1(b)(iii) of the Head Terms. We note that it is also open to the eSafety to address these matters in policies for the enforcement of the Codes.
67	Chris Skelton		Over-removal of content	General	- Overcapture content, allowing corrupt actors to censor content. As a result, the Online Safety Codes may unintentionally increase risks of: - Domestic violence.	This concern is noted. The Codes have sought to take into account concerns about user privacy and surveillance.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					- Retaliation against whistleblowers. - Reduced freedom of expression for all Australians. web-based businesses and services. - State oppression and censorship.	
68	Collective Shout	Negative: While we welcome industry participation in the development of these draft (voluntary) Codes, unfortunately we do not believe they are strong or comprehensive enough to ameliorate current and predicted harms. The Codes fail in their intended aim of protecting children. They do not address first generation CSAM, do not address live-streamed child sexual abuse, do not contain provisions requiring shorter take-down times and complaint handling processes, take no account of parent run accounts and paid sponsorships for children and ignore the dangers of end-to-end encryption. The draft Codes therefore fail in their stated aims				Please note that the Codes are not voluntary. If registered, they would form part of an enforceable co-regulatory scheme under the OSA. Non-compliance with the Codes by industry participants may result in significant penalties.
69	Collective Shout		Approach to pornography	Schedule HT	It is not possible to separate pornographic material from class 1A or 1B material. Sexual violence is a subcategory of "extreme crime and violence material," according to page 26 of the Explanatory Memorandum: Pornography increasingly depicts violent, cruel, non-consensual, extreme acts. It is cited as a driver of child sexual abuse material and sex trafficking, and used as as tool to groom children. A significant amount of material in Classes 1C, 2A and 2B belongs in Classes 1A and 1B. Pornography genres normalising rape, torture, sadism, incest, and extreme	Noted. Our understanding is that pornography is not in scope of these Class 1 Industry Codes. This understanding is informed by the eSafety Commissioner's Position Paper is that pornography should generally be treated as Class 2 material for the purpose of development of Phase 2 of Industry Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					violence against women and girls are routinely offered on the largest porn-hosting platforms in the world. A	
70	Collective Shout		Complaints handling	All Codes	There is insufficient urgency and accountability in the proposed mechanisms and timeframes to resolve complaints. Codes must include mandatory time limits on responding to complaints. Providers should make detailed data available on all complaints. Providers should include access to a mechanism for end-users to make a complaint to a third party if they are dissatisfied with the provider's response to a complaint.	Noted. The Codes contain mechanisms for end-users to be directed to the eSafety Commissioner if they wish to make a complaint/are dissatisfied with the handling of a complaint.
71	Collective Shout		Reporting/ CSEM activity	All Codes	We recommend that providers be required to report in detail on complaints and reports regarding CSEM activity including: ● incidents/pieces of content/number of accounts detected +/- removed proactively and method of detection (AI vs human moderators). ● incidents/pieces of content/number of accounts reported by user community, and outcome (takedown/mandatory reporting requirements fulfilled vs dismissal, including reason for dismissal). ● number of incidents/users referred to regulators/authorities for CSEM activities. ● number and demographics (age, sex, country) of minors implicated by paedophile/CSEM activity. time taken to respond to the report. ● nature of the content, and ● what action was taken by the provider	Noted. In response to feedback, the Codes have been amended to provide additional annual reporting requirements for SMS, RES and DIS Tier 1 services and Search engines concerning CSEM and pro-terror materials.
72	Collective Shout		Termination of accounts where CSEM detected	Outcome 1, SMS,	Social media platforms should not tolerate violations of laws prohibiting CSAM material. They should remove the requirement that an end-user "repeatedly violated terms and conditions, community standards, and/or acceptable use policies." Codes should remove clauses specifying that end-user accounts are terminated only if they intend to cause harm. Social media platforms must not tolerate violations of laws prohibiting CSAM material. They should remove the requirement that an end-user "repeatedly violated terms and conditions, community standards, and/or acceptable use policies."	Noted. We consider that this approach is appropriate, given industry's experience that materials can be inadvertently shared, including by young people who may not be intending to cause harm.
73	Collective Shout		Use of term	general/drafting	The term 'reasonable' is left undefined and	Noted. We note that the term reasonable is a common

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			reasonable		should be replaced with the term 'necessary' to accomplish a focus on the best interests of every child	standard used both in many regulations including in the Basic Online Safety Expectations under the OSA) and in common law.
74	Collective Shout		Reporting of CSEM	Outcome 1	CSEM should be reported regardless of suspected victim's location or nationality	We note that the development of these Codes pose complex jurisdictional issues, including concerning the scope of obligations to report CSEM materials. We have sought to align the approach with the objectives of the OSA to improve online safety for Australians and promote online safety for Australians (see section 3 of the OSA). We acknowledge that children everywhere should be safe from child sexual abuse. However, other jurisdictions such as the US have different reporting obligations which may be in conflict with these Codes if obligations to report were broader in scope (for example, in the US reporting of CSEM to law enforcement can jeopardise the successful prosecution of CSEM offenders). This issue is in our view outside the scope of these Codes to resolve.
75	Collective Shout		Detection of first generation CSEM	Outcome 1	Identification of first-generation CSAM. Tools are available to them, and there are rapid developments of technology which provide "breakthrough technology that identifies and classifies previously unknown CSAM images and video at scale. Online companies must employ all tools available to them to tackle first-generation CSAM. ● Industry must invest in tools and resources to enable providers to detect and deal with first-generation, existing, and live-streamed CSAM.	We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). In response to feedback, these measures have been extended to very large relevant electronic services and dating services (See Schedule 2.) These measures require these services to deploy the most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified. We acknowledge the concern that industry invests in new technologies that can accurately detect first generation materials and supporting infrastructure. We consider that the Codes address this in an appropriate way, for example by requiring ongoing investments in safety by Tier 1 SMS, RES and DIS providers. Both the Outcomes based approach combined with the expectations in the BOSE also incentivise the industry to strive to improve their response to CSAM, including through collaboration with NGOs.
76	Collective Shout		Proposed takedown times	Outcome 1	Industry should provide further explanation supporting the proposed 24 hour takedown	Please see the guidance provided in relation to the timeframe for taking down these materials which

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			are unjustifiably and unacceptably lengthy.		time for CSAM images. It is possible that there are good reasons for this in terms of internal and external investigations and so on; in this case, the Codes should specify.	explains why more time may be needed before CSEM materials are removed.
77	Collective Shout		Codes fail to address sexual discussions and other degrading treatment of minors	Outcome 1	● Industry Codes must explicitly prohibit non consensual sharing of minors' content. ● Industry Codes must explicitly prohibit sexual discussions and other degrading and exploitative treatment of minors. ● Industry Codes must explicitly prohibit paedophilic networking, including the use of red flag terms known for use in connecting sexual predators and aiding trade in child sexual abuse material	We acknowledge these important concerns but they are not within the scope of these Codes. We consider that the Codes provide appropriate community safeguards concerning CSEM within the constraints of the Online Content scheme in the OSA (which provides for the development of these Codes) and in the light of the eSafety Commissioner's Position Paper which sets out the Office's expectations as to the measures that should be included.
78	Collective Shout		The Codes lack detailed information for parents and carers about how to manage children's access and exposure to class 1A and 1B material	Outcome 7	To be understandable and applicable to ordinary users, this information must include examples and case studies of common ways that children might be groomed, exploited or harmed, including: ● DMs from followers ● Followers joining in to live videos ● Requests for images, videos, and livestreams ● Self-generated CSAM ● Threats to force compliance and secrecy ● Data theft ● Content theft ● Cross-platform exploitation ● Deep fakes ● "Tributes" and "shout-outs" ● CSA narratives ● Paedophilic discussions ● Abusers rely on the deep embarrassment and shame that children feel, as a protective mechanism against seeking help from adults.	The Codes contain measures for all products/services in scope to provide appropriate safety information to end-users. The exact content of that information as the risks to end-users will vary, depending on the type of services and other factors such as its functionality and scale. We note that this type of educational material is also published by eSafety.
79	Collective Shout		Monetising children's content must be prohibited. Currently, child predators are being incentivised and rewarded for engaging with children.	No measure	We believe industry Codes must reflect genuine commitment to children's safety and explicitly prohibit this activity. Industry must also indicate how they will detect, remove and appropriately report accounts engaging (or appearing to engage) in the sale of child exploitation material to relevant authorities and/or regulators	We note these concerns but consider this is out of scope of these Codes which are primarily concerned with Class 1A and 1B materials. See response above. The provisions concerning reporting of CSEM were drafted to take into account the need for services to comply with the Privacy Act 1988 (Cth) which provides limited circumstances in which personal information can be provided to law enforcement. In response to feedback the relevant measures have been amended to make clear that the reporting requirements supplement existing reporting obligations in State and Territory legislation
80	Collective Shout		Paid partnerships and 'kidfluencing'	No measures/ SMS code	Since there is currently no regulation around this activity, we believe social media platforms - the primary hosts of brand-kidfluencer activity - are well placed to take responsibility and prohibit this inherently risky practice which	See above.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					puts children at serious risk of exploitation	
81	Collective Shout		Age verification and children on social media	Outcome 1 SMS,	On the point of age verification, the draft Codes offer guidance for preventing children from using Tier 1 services. We recommend removing the suggestion that it would be sufficient to require a user to declare their date of birth during the account registration process, as this is an ineffective method. It is also insufficient to have only a "tick box" to ensure the user of an internet carriage service is an adult (as in Schedule 7). More accurate technology is available and should be used.	We understand that this issue will be addressed by the eSafety Commissioner's Age Verification Roadmap when it is finalised. The Codes have been drafted so as not to pre-empt the government's position as to the appropriate methods of age verification that industry should deploy.
82	Collective Shout		end-to-end encryption	Outcome 1	We note that there are tools available and being developed which have the capacity to detect grooming and abusive behaviours on E2EE services whilst still preserving user privacy. Such technologies are being developed in the UK by the government's cybersecurity experts, as well as by companies such as Cyacomb, DragonflAI, Apple, and SafeToNet. International Justice Mission is spearheading advocacy in this area. Industry must use existing tools to detect behavioural signals and CSAM materials in end-to-end encrypted services. Industry must invest in tools and resources to enable providers to detect and deal with first-generation, existing, and live-streamed CSAM in end-to-end services.	Our understanding is that while efforts are being made to develop such tools they are not yet at a stage where CSEM activity can be accurately detected across all E2EE encrypted services while maintaining adequate user privacy. See above response on further development of proactive detection technologies.
83	Counter Extremism Project	Supportive: This submission provides specific recommendations on how to strengthen the draft Social Media Services Online Safety Code (Class 1A and Class 1B Material) to ensure effective regulation against terrorist content online.	Removal of pro-terror material	Objective 1/Outcome 1/compliance measure 3 SMS Code (schedule)	CEP recommends that terrorist content be removed within one hour of upload. The European Union's Regulation on the Dissemination of Terrorist Content Online (TCO) set a reasonable precedent by calling for removal within one hour of notification obliging tech companies to act quickly to remove terrorist content is necessary to stop the spread of this heinous and violent material. The EU's TCO regulation entered into force earlier this year, and because of that pioneering regulation, European public authorities can now require online platforms or cloud services to remove specific posts, music, livestreams, photos, and videos inciting violence and glorifying terrorist attacks. Promoting terrorist groups and instructions for how to commit an attack is also forbidden	The EU regulation requires platforms to respond to notices to remove TCO from a competent national authority of a member State. Australia has passed the Abhorrent Violent Materials Act 2019 (Cth) and given the eSafety Commissioner additional powers under the OSA to issue notices to deal with removal of AVM content. The Codes are developed to give effect to the Online Content scheme in the OSA. The Codes in general, deal with action that must be taken by service providers in response to Class 1A (inc pro-terror material) and Class 1B material under the National Classification Scheme. That Scheme is designed to address material that is broadly contrary to community standards, rather than TVEC or pro-terror

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					online under the TCO. Significantly, tech companies will have one hour to take down terrorist content after it has been flagged by an EU country.1	material specifically. See Annexure A for explanation. However, note that the ISP Schedule contains a minimum compliance measure that requires all ISPs to sign, upon request by the Commissioner, the Protocol governing ISP blocking under Part 8 of the Online Safety Act 2021 (currently only the largest ISPs). This protocol deals with the blocking of such AVM. The Codes therefore supplement the existing legislative regimes in Australia for dealing with pro-terror material and AVM.
84	Counter Extremism Project		Industry cooperation in detection and removal of pro-terror material.	Objective 1/Outcome 5/compliance measure 16 SMS Code (Schedule)	CEP recommends that social media companies in Tiers 1, 2, and 3 should collaborate to share best practices, information, and technology—including hashes and known terrorist content—to ensure that terrorist content does not spread and is not reuploaded across multiple sites and platforms. This cooperation should not be limited to Tier 1 companies and is a reasonable, proactive measure for all social media platforms concerned about the spread of terrorist content. The GIFCT is supposed to facilitate cooperation between large companies—which have more resources and manpower to moderate extremist content on their platforms—and small tech firms. There is no reason to simply mandate that only Tier 1 social media companies collaborate across industry when such frameworks exist to promote and facilitate the exchange of technology and knowledge among companies of all different sizes. Moreover, it is essential that government agencies, including the eSafety Commissioner, hold tech-led groups like GIFCT to account when it fails13 to prevent terrorists and extremists from exploiting online sites and platforms—the organization's stated mission	We gave careful consideration to whether the Codes should include measures to proactively detect pro-terror materials and /or share hashed of known pro-terror content. Following feedback, we introduced measures requiring very large social media services and relevant electronic services to proactively detect certain kinds of pro-terror imagery and videos. We think that is an appropriate response to concerns about this material online. There are significant risks in requiring all services in scope to deploy proactive detection technology to identify and remove this material, because it requires context-based judgments and investment in significant human moderation and supporting processes that may be out of reach of many businesses. We have provided guidance with these measures that makes these issues clear. We note that with a hash database for example, there are risks for example that hashes of material could be misused to target legitimate forms of political dissent. We note that NGOs such as the GIFCT play an important role in this space and the Codes encourage industry support for NGO work in this area.
85	Counter Extremism Project		A mechanism for users to appeal to Australia's eSafety Commissioner if	Objective 2 Outcome 8, measure 23 and Outcome 9 measure 26 SMS Code	CEP recommends that, in addition to measures #23 and #26, an additional measure be included to allow Australian end-users to appeal to the eSafety Commissioner should the social media company fail to adequately respond to takedown requests of terrorist and	Section 38 of the Online Safety Act already provides a mechanism for end-users to make reports to eSafety about Class 1 materials under the Online Content Scheme including pro-terror materials and for eSafety to issue notices to industry participants to take down or remove links to Class 1 materials.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			social media companies do not adequately respond to content takedown inquiries.	(Schedule1)	pro-terror content.	
86	Counter Extremism Project		Content of transparency reports.	Outcome 10, Outcome 11, Compliance measure 32 and 33 SMS code (schedule)	Social media companies must disclose how much of their budget is dedicated to content moderation efforts in transparency reports. CEP recommends that the eSafety Commissioner require social media companies to disclose how much of their budget, including personnel and research and development, is dedicated to content moderation in its Code reports. Companies should include a breakdown of how much is spent on developing and maintaining a well-trained and well-supported content moderation and review program. The breakdown should include, among other things, information on how many personnel is responsible for and dedicated to content moderation, funds for research and development, financial resources for subject matter and best practices training, and money spent on mental health programs for content moderators. Notably, reporting should also clearly specify how much of these resources are used to combat class 1A and class 1B, compared to other types of materials like copyrighted content and spam, which tech companies have a business and legal incentive to remove.	Noted. We do not think that expenditure by companies on content moderation is an adequate measure for determining whether companies are meeting the Outcomes and Objectives of the Codes. In general, when developing measures, we had regard to the list of measures outlined by the eSafety Commissioner in the Positions Paper on Code development and feedback from eSafety during the Code development process. We agree that adequate content moderation resourcing/training is important. We consider that this has been provided for in the Codes.
87	Counter Extremism Project		Content of transparency reports.	Outcome 10, Outcome 11, compliance measure s 32/33 SMS code (Schedule)	Social media companies must report on the effectiveness of its interventions and efforts to combat terrorist content. CEP recommends that the eSafety Commissioner require social media companies to report on the effectiveness of its interventions and efforts to combat terrorist content in its Code reports. For example, when a company announces a ban of ISIS content from its platforms, how much of that content remains on the platform and how quickly is that content removed? When members of the GIFCT declare that companies will use the group's hashing	Following feedback, we have made amendments to reporting obligations for Tier 1 SMS, RES and DIS services and Search services to report on CSEM and pro-terror these materials. The eSafety Commissioner has a broad discretion under section 42 of the OSA to require companies to provide additional information about actions taken by companies to deal with pro-terror content in relation to investigation of complaints under the online content scheme and concerning Codes breaches. The Commissioner has additional broad powers under sections 48, 49 and 59 of the OSA to require statements/reporting of information under the BOSE instrument which also articulates expectations regarding how this material will be addressed.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					database to remove known terrorist content from its social media sites, how much of that content is still able to be uploaded and subsequently reuploaded on to those platforms? This recommendation should also be mandatory for reports from Tier 1 and 2 companies. Tier 3 companies should be required to submit reports, as requested by the eSafety Commissioner.	
88	Daniel Smith		Anonymity/age verification	General	- The introduction of age verification for Social Media Services. particularly concerned about the impact towards users who wish to remain anonymous for safety reasons (for example, a political activist). The use of Artificial Intelligence to estimate age is also worrying, due to issues of inaccuracy and bias.	We have taken this concern on board and clarified in the Head Terms that the Codes do not require the implementation of age assurance measures. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
89	Daniel Smith		Compliance burden/inability to comply for smaller providers and consequences	General	- Reporting of objectionable material. Moderating and reviewing reports of objectionable material at scale is a very challenging problem. Compliance with this legislation may be too burdensome for small platforms and/or may cause platforms to remove functionality and/or user groups to avoid the problem entirely. Furthermore, malicious users could take advantage of this legislation to report content in bad faith.	We have sought to address the potential impact on small businesses/start ups in section 5.1(b)(iii) of the Head Terms. We note that it is also open to eSafety to address these matters in policies for the enforcement of the Codes. In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.
90	Daniel Smith		Sharing of information with eSafety and other Gov agencies	General	- Sharing of information and intelligence with eSafety. While the scope of information shared is intended to be only related to class 1A and 1B material, adhering to this legislation is problematic for encrypted applications where the nature of content cannot be determined. I am also concerned that government agencies may request data unlawfully, particularly in light of the ombudsman report on the behaviour of police and integrity agencies.	We note these concerns. We have sought to address these issues in section 6.1 of the Head Terms, which for example, limits the impact of the Codes on end-to-end encrypted services.
91	Daniel Smith		Minimum	General	- The protections outlined in the Codes do not	This concern is noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter’s comment	Industry associations’ comment consideration
			measures are not differentiating by age		vary for different ages of children. While young children should undoubtedly be sheltered from some online content, older teenagers are better equipped to deal with problematic content	Changes have been made to measures in the Codes concerning settings for children so that these are now targeted at users under 16, in recognition of the needs and abilities of users age 16-18.
92	Digital Rights Watch	Neutral: The key areas of concern we raise in this submission are: 1. the Codes interaction with the government’s ongoing reform agenda, including pending reform to the Privacy Act and review of the National Classification Scheme, 2. the risks and challenges of proactive detection of material, and that its use should be carefully and strictly limited and with robust safeguards to prevent over- or mis- use, 3. the lack of clarity regarding coverage thresholds, and possible adverse impacts upon competition which ultimately consolidates power into the hands of large commercial entities, and 4. the need to include provisions to increase accountability of both industry as well as the eSafety Commissioner by way of providing access to reporting and data for public interest and research purposes				This concern is noted. See responses below.
93	Digital Rights Watch		Pause further development until the Codes can be aligned with the government’s	General	The Codes are being developed ahead of significant regulatory reform that is highly likely to impact the way the Codes are implemented. While we understand the desire to move quickly, doing so runs the risk of creating an overly complex, contradictory, and constantly	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) the OSA. As a result, the scope of the Codes primarily concerns Class 1A and Class 1b materials. The Codes are therefore aligned with the OSA and the

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			ongoing reform agenda		changing regulatory landscape. The Codes should be consistent with broader government policy and related regulation. For instance, the outcome of the review of the Privacy Act is likely to have a direct impact upon the Codes. Personal privacy is crucial to online safety for many people, especially vulnerable populations, and so any industry code providing guidance for online safety must integrate best practices for privacy protection.	National Classification Scheme which outlines how classification decisions should be approached at this time. This is reflected in Annexure A of the Head Terms. While these concerns about the impact of future regulatory changes are valid, we do not think that the industry is able to ensure the Codes align with policy areas that are under development; that is a broader issue for the government. Section 7.6 provides for the review of the Codes at which time they can be updated to take into account changes to the Privacy Act 1988 (Cth) and National Classification Scheme, which as noted are under review.
94	Digital Rights Watch		Application of concepts in National Classification scheme	Heads of terms, definitions	Similarly, the Codes, and indeed the entire approach of the Online Safety Act, is based upon the controversial and outdated National Classification Scheme, which is also currently under review. Developing an approach to regulation that is based upon an outdated and soon-to-change foundation is a surefire way to exacerbate Australia's already fragmented and complex internet and communications regulatory regime	See above response.
95	Digital Rights Watch		Proactive detection	Outcome 1, SMS and DIS	We agree that proactive detection of material in private communications and file storage is an unreasonable invasion of privacy and creates additional security and safety risk for individuals, businesses and governments. Proactive detection will always carry with it some level of privacy and security risk. While Digital Rights Watch does not argue against the use of hash scanning in public platforms for known CSAM, we remain concerned that there are not adequate safeguards in place to prevent use of proactive detection technology from expanding into other areas. Given the inherent risks to privacy and digital security, any requirement placed upon companies to use proactive detection technologies must be carefully balanced with robust safeguards and restrictions to prevent misuse and abuse of technology.	Noted. We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categories as Tier 1 (highest risk). Following feedback these measures have been extended to very large Tier 1 relevant electronic services with more than 8 million monthly active accounts and dating services. These measures to require these services to deploy the most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified.
96	Digital Rights Watch		Proactive detection and	General; scope of Codes	There is nothing within the enacting legislation, the Online Safety Act, that creates	Noted. The inclusion of measures concerning proactive detection was in response to the eSafety

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			regulatory overreach		obligations on service providers to proactively monitor communications over their networks. This was a key part of the policy debates in the lead-up to the passage of the Act. It is not acceptable for the Codes to be used as a way to extend obligations beyond the legislative intent reflected in the Act—this would represent a serious overreach of eSafety power	Commissioner's Position Paper and feedback provided by eSafety through the Codes' development process. See above response about the approach taken to these issues.
97	Digital Rights Watch		Prohibition on monitoring/ Inconsistency with international approaches		We wish to highlight that there is a risk of creating challenging misalignment between Australia and international jurisdictions should Australia move toward requiring general monitoring, while the EU prohibits it	Noted.
98	Digital Rights Watch		Challenges of automated processes to detect unknown or previously unseen content	Outcome 1	Machine learning classifiers which seek to automatically flag possibly harmful content (as opposed to matching content to known, or previously identified harmful content) may be improving, but they remain seriously flawed when it comes to classifying complex material at scale. One issue is accuracy and the risk of both over- and under- capture of content. We note our support for groups such as Scarlet Alliance and Assembly Four which have emphasised the harm caused to sex workers and others who post legal sexual material when their content is taken down due to incorrect or overly broad content classification. Another issue is that due to the lack of training data, classifier models are more likely to make mistakes related to marginalised groups, and in doing so further entrench existing inequality. Further, there remain ongoing challenges regarding the explainability of machine or deep learning classifiers. While this is an area of ongoing technical research and development, at this stage it may not be possible to explain or justify why some content is flagged by an automated machine learning content classification system. DRW recommends that the Codes should not be extended to require monitoring beyond matching of known CSAM in the highest risk public and semi public services. In addition to this, strict limitations and safeguards should be in place to prevent this technology from being rolled out more broadly	Noted. See above.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
99	Digital Rights Watch		Scope of Codes/competition impacts	General	Coverage thresholds need further clarity and risks to competition should be carefully considered. We remain concerned about the possible harmful impacts of limiting competition by increasing regulatory burden upon small, independent, community-led or non-commercial entities. Despite the three-tiered risk assessment system, there remains a strong incentive for entities to 'round up' their compliance where there may be any confusion regarding which category or tier they might belong to, incurring what is likely to be an unreasonably regulatory compliance burden. The Codes currently suit incumbent powerful companies, especially large social media companies, as more risk and compliance cost for community-led and hosted online spaces means that more traffic will be driven to Big Tech.	Noted. We have attempted to address this concern in section 5.1(b)(iv) of the Head Terms and by classifying as Tier 3 many categories of businesses, many of which will be smaller in nature and lower in risk due to their scale. Many measures for Tier 3 services are optional. It is open to eSafety to provide further clarification on this issue in developing its enforcement policy for the Codes.
100	Digital Rights Watch		public interest research	Proposed new measure	We recommend including provisions within the Codes to require members of the online industry to provide access to reporting data. This assists in research and public interest auditing, ultimately assisting in the transparency and accountability of the regulated entities, the eSafety Commissioner, and regulatory scheme in general. High level aggregated reporting is not enough.	Many multinational companies in scope of these Codes already undertake extensive transparency reporting on a voluntary basis, as well as providing access to datas to researchers. However, we do not consider that such access should be provided automatically on demand so that services are able to ensure that data is handled ethically and in accordance with best independent research practices. We consider the industry approach to reporting is appropriate given that the eSafety Commissioner has broad powers to require reporting and information under the OSA, including in relation to investigations into industry compliance with Codes.
101	Dr Greg Roland	Endorse		Definition of Material requiring notification Schedule 1 Social Media Services, section 6.1.b ● Schedule 2 Relevant Electronic Services, section 8.2.ii ● Schedule 3 Designated	Recommended changes: ● Omit qualifiers in relation to threat immediacy and nationality/residential status in relation to reportable CSEM. ● Notification of CSEM material to appropriate entities to be mandatory across all Codes and services. (We draw attention to the fact that, under the current draft Codes, Tier 3 relevant electronic services; and Tier 2 and 3 designated internet services appear to be exempted from the requirement to notify cases of CSEM material to the appropriate entities [per Schedule 2, section 8.2 and Schedule 3 section 8.1]). Basis for recommendation: Any possession of CSAM outside law	The drafting of the provisions relating to the notification of CSEM are limited to those services and products that have the capacity to report that material where it is identified on a service. In response to feedback these measures have been amended to make clear that they supplement existing State legislation that requires reporting of this material. Outside of those State laws, reporting of this material is subject to the Privacy Act 1988 (Cth) that permits disclosure of personal information to law enforcement in limited circumstances. The measures in these Codes have been drafted to take into account these limitations.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
				Internet Services, section 8.1.b ● Schedule 4 Internet Search Engine Services, section 7.15.d.ii	enforcement contexts - irrespective of origin or context- is illegal in all Australian jurisdictions, regardless of whether it constitutes an immediate threat. In the case of CSAM (material documenting child sexual abuse), such material, while always serious and damaging, may not necessarily represent an immediate threat to a child. Live-streaming abuse or discussion of impending abuse certainly satisfies this condition, however much CSAM is historic, comprising evidence of abuse that has already taken place, including where there is no indication of immediacy or presence of future offending. This does not mean the content is not criminal or should not be reported. We also note that circulation of historic CSAM constitutes a form of re-victimisation for survivors and poses additional threat (which may be immediate or otherwise) due to its use as 'normalising' examples for grooming other children into abuse.	
102	Dr Greg Roland		Framework for identifying applicable Code and Category/Tier for a service	Preamble, Head Terms, reporting(?)	Recommended changes: ● Clarify guidance on Identifying the applicable code provided in preamble. ● Require industry participants to keep records of decisions as to which Code will apply to each online activity that they undertake, and the criteria or basis on which they have made these assessments. Basis for recommendation: The current advice is unclear and leaves considerable scope for industry members to selectively choose a code that might incur less burden of compliance, rather than aspiring to appropriately meet obligations of the highest risk services they might provide. In particular, we consider that the case example offered in the guidance note to this section of the Head Terms preamble (p4) does not make sufficiently clear the distinction between what is meant by "predominant purpose" versus "primary purpose" or how the assessment of which code should apply to the service should be decided. Requiring industry participants to keep a record of how they have determined which Code will apply to their various activities (and to be able provide	The issue concerning the lack of clarity around the application of the Codes to different industry sections arises from the broad manner those sections are defined under the OSA. It is not open to industry to change the relevant definitions in the OSA. We therefore consider that the application of Codes to different companies needs to be determined on a case-by-case basis, taking account any guidance issued by the eSafety Commissioner. We note that it is open to eSafety to take enforcement action under the OSA if they consider companies have not correctly assessed the way they are subject to the Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					this evidence to the eSafety Commissioner if so required) will protect entities who are acting in good faith and mitigate the potential for unscrupulous operators to take advantage of the ability to 'scale down' perception of risk and onus for compliance.	
103	Dr Greg Roland		Risk profile and risk assessment	All Codes, RES	Recommended changes: ● Institute minimum obligation for all industry participants across all Codes to undertake some level of risk assessment - even if their risk profile is considered to be minimal - and to maintain records of such assessments. ● Remove proposed exemptions to the obligation to undertake risk assessment currently offered to certain types of services under Schedule 2 (section 5d) of the draft Codes. ● Tier Indicators to include (reasonable estimation of) the age of end users of a service – i.e. having a high proportion of users who are children should be considered a Tier 1 indicator. Basis for recommendation: The reality is that there are risks of child sexual exploitation activity and CSEM/CSAM occurring in all 'Tiers', as well as those services currently proposed to sit outside the tier system, i.e. providers of - (i) a closed communication relevant electronic service; or (ii) an encrypted relevant electronic service; or (iii) an enterprise relevant electronic service; or (iv) a gaming service with limited communications functionality. We do not accept there is a reasonable rationale for these services to not conduct some level of risk assessment in relation to child safety, and to assess the risk posed to end users that CSAM (as a subset of class 1A material) will be accessed, distributed, or stored on the service. This is particularly important because all of the above types of services do carry risk as channels for sharing or soliciting child exploitation content, or for 'grooming' children. To illustrate this, we note that "limited communications functionality" as defined in the Codes (Schedule 2, section 3) leaves considerable room for exchange of exploitative content. The example of a gaming service with limited communications	Please note that the approach to risk assessment has been carefully considered. Certain services have been exempted from risk assessment such as closed communication services as there are both legal and practical limitations to their ability to take action against online content carried on their services, including their ability to assess the risk of CSEM and pro-terror material on their services. Please note that the approach of these Codes is intended to regulate services in a manner proportional to the risk of Class 1A and 1B materials, on services. We do not think that it is practical to assess services on the basis that they may pose a theoretical or very minimal risk of Class1 Materials. This approach is consonant with the eSafety Commissioner's Position Paper.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					functionality that allows for text that is subject to automated filtering technology may (depending on the efficacy of that technology) still be subverted by predatory individuals with a sexual interest in children; or, even if successful in blocking communications would (if this type of service is automatically considered to be Tier 3 as proposed at Schedule 2, section 7a) not be bound by minimum compliance measures for notifying or acting on CSEM that could help law enforcement to identify offenders or prevent future harms to children. These are precisely the types of considerations that we think should be properly articulated in risk assessments, and why we consider exemptions from risk assessments are not warranted. Requiring all industry participants to keep a record of risk assessments (and to be able provide this evidence to the eSafety Commissioner if so required) will protect entities who are acting in good faith and mitigate the potential for unscrupulous operators to take advantage of the ability to 'scale down' perception of risk and onus for compliance	
104	Dr Greg Roland		Record keeping and reporting	Reporting requirements Schedule 2 Relevant Electronic Services, section 8.2 ● Schedule 3, section 8.1	Recommended changes: ● Institute a requirement for all services across all schedules to keep records (and report to eSafety or other relevant agencies) in relation to: numbers of reports of suspected CSEM, numbers of complaints or reports regarding predatory or sexually exploitative behaviours by end users of the service against children, and the numbers of verified instances of CSEM or other CSE activity on their services. Basis for recommendation: Schedules 1(Social Media Services) and 4 (Internet Search Engine Services) require industry participants in all tiers to report instances of CSAM found on their service. However, Tier 2 and 3 service providers in Schedules 2 (Relevant Electronic Services) and 3(Designated Internet Services) - as well as those defined in Schedule 2 section 3 that lie outside the tier system - do not have the same obligation. This is problematic as these excluded services in these tiers can still be	In response to feedback received we have included a reporting measure for Tier 1 relevant electronic services (as well as Tier 1 social media services, Tier 1 designated internet services and all search engine service providers) to also report the volume of CSEM or pro-terror material removed by the provider.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					operated as platforms for the trafficking of CSAM/CSEM. Whole of industry reporting of CSEM content and volumes across the full span of the Australian online services industry is required to, not only investigate perpetrators, but to understand the scope of the problem, to correlate instances of discovery, characterise usage behaviours, and better understand where measures to combat online child sexual exploitation and abuse are having impact and effect.	
105	Dr Greg Roland		Documentation of procedures for reported CSEM	Enforcement measures Schedule 1 Social Media Services, section 6.3 ● Schedule 2 Relevant Electronic Services, section 8.5 ● Schedule 3 Designated Internet Services, section 8.2	Recommended changes: ● All service providers bound by Schedules 1, 2, and 3 (Codes for Social Media Services; Relevant electronic Services; and Designated Internet Services) should be required to have documented procedures in place in the event that CSEM is reported/detected. Basis for recommendation: The draft Codes identify some of the barriers to prescribing a definitive set of protocol for actions in the event of CSEM being reported or detected - for example, deletion of content or termination of suspect user accounts may need to be deferred during an active law enforcement investigation, rather than proceeding to timeframes that might be expected to apply in other instances. We suggest that to mitigate against uncertainty on how to act in the event of Class 1A material being identified, all services across all Codes should be required to develop and maintain records of internal procedures for this eventuality, to cover matters such as the protocol for verifying reports, internal training in procedures, threshold and steps for contacting law enforcement, and the subsequent removal of material and suspension of implicated end-users (including under the direction of law enforcement) so as to minimise secondary trauma and interference with forensic investigation. The proposed Codes do not currently require this of all industry participants. The Consultation drafts of Schedules 1(Social Media Services), 2 (Relevant Electronic	These Codes contain requirements concerning policies and procedures for handling this material. These have not been drafted in a prescriptive manner, because given the breadth of services in scope of these Codes, these will need to be tailored to the needs of different types of services. We also note that a risk-based approach is set out in the Position Paper, recognising that not all services across the wide spectrum of participants do pose the same risk but need to have an appropriate compliance burden. The Head Terms requires companies to maintain records of Code compliance (See section 7.2.) This clause has been amended in response to feedback to make clear these records should be maintained for 2 years.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					Services), and 3(Designated Internet Services) require only those service providers who self-identify as being within risk Tiers 1 and 2 to have procedures in place for the handling of Class 1A material. This is despite the risk of significant CSAM trafficking occurring in all Tiers (i.e. including Tier 3) - as well as within those services defined at Schedule 2 section 3 that are currently proposed by Industry as being exempt from risk assessments. If providers outside of Tiers 1 and 2 are not required to be prepared for such an eventuality, missteps in the handling of CSAM reports/detection may result in interference with forensic investigation as well as secondary traumas to personnel exposed to such material.	
106	Electronic Arts, Inc, Ubisoft Entertainment S.A. and Take Two interactive Software, Inc.	supportive: commend the efforts of the working group, and particularly the Interactive Games & Entertainment Association (IGEA), in recognizing that video games present lower online safety risks than other online services. Specifically, we support the specific definition in the code of "gaming service with limited communications functionality." The draft code appropriately limits the obligations applicable to services within scope of that definition, and specifically designates gaming services with limited communications functionality as Tier 3 relevant electronic services. In its structure and terms, the draft code acknowledges not only the distinction			Because of the safety features in place and the limited nature of in-game communication, illegal content such as violent extremist content or child sexual abuse material is very rare in in-game communication. The terms and structure of the draft online Codes reflect both the limited risk to online safety posed by video games and the powerful tools already put in place by the industry to protect the online safety of players. The final version should preserve the definition "gaming service with limited communications functionality." It also should impose limited obligations on services within scope of that definition and maintain the designation of gaming services with limited communications functionality as Tier 3 relevant electronic services.	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		between video games and other online services, but also the critical work of the video game industry over the last several decades in building protections for players of online games				
107	Eros Association	Supportive of Class 1 C exclusion	Exclusion of Class1 C (festish pornography) from Codes	H T	We welcome the designation of "class 1C material" as a subcategory of class 1 material that is comprised of particular online pornography, including fetish material. This acknowledges the relative severity and potential for harm associated with different types of material. This definition of this material is, however, reliant on the National Classification Code and Classification Guidelines, which are woefully out of date. We are concerned, however, by the statement that "industry participants may use different terminology to describe… class 1C material for different audiences." In our view, consistent terminology should be used across the Codes to avoid scope creep and confusion. We recommend that this clause be deleted.	As a result of the feedback receive, we have sought to clarify the definitions of Class 1A and 1B materials in light of concerns about the extent these may capture mainstream pornography categories. Class 1C is not in scope of these Codes and is not impacted by the guidance. See amendments in Head Terms.
108	Family Zone	Rejection of Codes in favour of standards. Largely status quo.	Exclusion of online safety tech from def. of OSA	Def. of online safety industry of OSA	OSA def. of online safety industry excludes online safety tech (e.g., Family Zone, NetNetty Norton etc.) and, consequently, are excluded from the collaborative efforts around the regulatory regime despite being the only ones being truly aligned with community expectations.	We note that as identified in this submission the OSA does not regulate online safety tech. This is not an issue that can be addressed by industry Codes.
109	Family Zone		Class 1B material	All Codes	Any social media or gaming platform that is targeted at or frequently used by pre-teens and in any event where a platform (i.e. SMS, gaming, websites apps, web portals, file sharing) is aware that pre-teens are using the platform, moderation technology be required to be implemented to block Class 1B materials for those users. Blocking of Class 1B material is possible, reasonable and expected by community.. Concerned that Class 2 Codes are similarly weak.	It is not technically or practically possible to comprehensively block Class1 B material from being accessed in Australia. The assessment of whether material should be classified as Class 1B material requires context-based judgments on a case-by case-basis. We note that the Codes do contain measures concerning the prohibition of Class 1B materials and enforcement of these policies on these services. Please see, for example, measures in Schedule 1(SMS Code).
110	Family Zone		Risk assessments	SMS, DIS, RES App,	Largely reflect current practices and offer the designated online safety industries too much	We consider that the risk assessment approach is appropriate given the challenges of implementing the

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
				Equipment(?)	subjectivity and wriggle room to determine their risk profile and thus required measures to be taken. This construct will fatally undermine the ability of the Codes to address other classifications of material (as these Codes evolve).	broad definitions of the industry sections under that are subject to the Codes under the OSA, the diverse companies in scope and the likelihood that relevant services and products will evolve over time, for example by expanding their user base or adding new functionalities to their services. eSafety Commissioner's Position Paper asked industry to combine an Outcomes (principles-based approach) to Code development with specific measures. We think that the drafting approach balances the need for specific measures with the need for participants to adapt to changes in the online environment, in a way that is responsive to the need to meet the Outcomes of the Codes.
111	Family Zone		Age assurance	SMS, RES	Codes rely on deficient age assurance (DOB). Instead use: Device operating systems already have secure mechanisms to identify & authenticate users. Should be required to accept and retain maturity tokens set by a parent in the operating system or through a 3rd party parental control app. Parental control apps or operating system settings can then leverage these maturity tokens as parameters to pass to online platforms. Online platforms can then accept these maturity tokens and provide a maturity appropriate experience, including blocking the upload and distribution of Class 1B material as required.	We consider that these issues are more relevant to Class 2 materials that are unsuitable for children of 18 or under and are not within the scope of these Codes. This is consistent with the eSafety Commissioners' Position Paper. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap.
112	Family Zone		BYO learning devices	All Codes?	Codes do not consider the fact that BYO learning devices (2-3 million) are usually (per school requirements) free of online safety technology.	We consider that this issue is best dealt with by schools which are not within the scope of the OSA or Codes.
113	Family Zone		Operating systems / privacy/security settings on devices	DIS / Equipment	Codes ignore the fundamental role of the operating system providers and their obstructive behaviour. Apple, Google, and Microsoft offer business app developers access to more functional and more robust safety features to support the supervision and protection of adult employees than they offer app developers seeking to support mums and dads to protect their kids. Various examples where these companies have limited parental control options to be accessible for parental control apps (while still being available to business app developers)	This opinion is noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					Codes substantially reflect current practices and offer little practical progress. Specifically the proposed Codes accept the current methods made available to parents and children to configure privacy and security settings. These are manifestly failing. Require that all platforms support the following measures to enable content moderation: Parent Settings: Parent settings which can be configured to restrict users to maturity appropriate content and features (eg Comments, Video streaming, Location tracking); and Parental Control APIs: API's which can be used by on-device safety software to direct users to maturity appropriate content (like provided by Google with YouTube Restrictions & Google Safe Search) and features; It is critical that requirements be for both of these measures. Parent settings are too easily bypassed by children. On-device technology is critical and Google's YouTube Restrictions is a fantastic example of what is possible (all schools and parental controls can easily enforce maturity levels in YouTube because Google provides an API).	
114	Family Zone		Example scenarios		Provides 9 examples of scenarios not covered by Codes, see sub.	Noted.
115	Family Zone		Future access to materials	All Codes	Government should issue guidance to apps/sites on suitability of various forms of content (classification scheme) and features (eg chatting with anonymous accounts, location tracking] for different maturity levels. Codes/Standards should be set which require platforms implement techniques which allow users and/or their parents to configure (based on maturity) access to these materials or functionalities through: Platform user profiles;and On-device restrictions configured in parental control apps or as tokens set in the operating system. On device restrictions can be passed to the online platforms to ensure moderated access	Noted. We consider that these issues are more relevant to Class 2 materials that are unsuitable for children of 18 or under and are not within the scope of these Codes. See the eSafety Commissioner's Position Paper. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap. In response to feedback received, the Codes contain measures specifically addressing age restriction and other requirements for dating apps.
116	Family Zone		Class 2:	General	All adult websites to register with eSafety or	We consider that these issues are more relevant to

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			Mandatory adult site registration		body. All telcos, wifi hotspots, schools etc. to block unregistered websites.	Class 2 materials that are unsuitable for children of 18 or under and are not within the scope of these Codes. See the eSafety Commissioner's paper on Code development. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap.
117	Family Zone		Mandatory free content scanning software		Given they profit from the internet to a huge extent, Google, Apple, and Microsoft ought to be compelled to provide free access to tools which scan images & videos for material which is illegal and harmful.	The scope of the Codes primarily concerns Class 1A and Class 1B materials as set out in the eSafety Commissioner's Position Paper, not all illegal or harmful material. It is not technically possible for services to accurately scan for all harmful and illegal materials online. Classification of online materials in most cases require context-based judgements on a case-by-case basis. The Codes set out compliance measures on proactive detection of known child sexual abuse materials by high risk services in Schedule 1, Schedule 2 and Schedule 3 of the Codes. In response to feedback proactive detection measures for known CSAM have been extended to some very large relevant electronic services and dating services. Measures have also been introduced requiring proactive detection of pro-terror materials by very large social media services and relevant electronic services.
118	Family Zone				Require Google, Apple, and Microsoft plus all internet browser providers support, equally through first and third party apps or extensions features which allow schools & parents to: Sites: Restrict users to age-appropriate websites (eg. block adult sites) Content: Restrict users from inappropriate web-content (eg block comments in YouTube) Apps: Restrict users to age appropriate apps (eg block dating apps) Device Features: Restrict users to age appropriate device feature (eg block location sharing, use of VPNs or Hotspotting) App Features: Ensure their children are directed to age-appropriate feature within apps (eg Google Safe Search and Youtube Restrictions)	Noted. We consider that these issues are more relevant to Class 2 materials that are unsuitable for children of 18 or under and are not within the scope of these Codes. See the eSafety Commissioner's Position Paper. Note the eSafety Commissioner is engaging with some of these issues in developing the Age Verification Roadmap.
119	Family Zone		Mandatory network-based filtering	ISP plus more?	Require any publicly available or child accessible network to implement technology which Blocks illegal and adult sites on child accessible networks eg WiFi Hotspots & Schools; and	See eSafety Position Paper that sets out the Commissioner's position on that material that is unsuitable for under 18 's and the intention that it be dealt with under Class 2 Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					Blocks illegal material and non-compliant / unregistered adult sites on telco networks.	
120	Francis Leister	Rejection	Code not justified; end (sex exploitation reduction) does not justify the means.	General	Rejects premise of child exploitation as a valid reason to restrict basic human rights, introduce censorship or limit right to privacy.	See above response.
121	Francis Leister		Classification of material /classification as basis of what is acceptable	General	Imagine a cohort of Muslims setting the standard of dress for film classification. Or some 'Hillsong' religious person in power that decides we should go back to the religious sensorship of the 1930's when we were all good God fairing people, no kissing or pictures of any couples in bed etc. I even question the need for sensorship of child pornography, if it was generated in computer simulations without any actual children being involved! And no actual crime has taken place without the use of the children, so the crime should not be in the picture of the crime...for it is a slippery slope, if the same standards were applied to crime of murder, all those watching murder misteries on television and elsewhere would be guilty of engaging in murder. Not that I wish to be seen advocating child pornography or anything, I'm just trying to make a point, that privacy policies hatched from some misdirected good intention can go off the rails and are never going to be fit for purpose in a modern free society, in which a new election outcome could see daconian controls in the wrong hands!	See above response.
122	GEN VIC/Vixen Collective		Sex workers' ability to advertise and communicate negatively impacted by the Codes	All Codes, esp. SMS, RES, DIS, (Hosting)	Furthermore, GEN VIC's member, Vixen Collective, is very concerned about the Codes' impacts on sex workers' ability to advertise and communicate online about sexual violence and safety issues. Sex workers need to be able to advertise online as a matter of safety – advertising helps sex workers screen clients, which is imperative for their safety. For further details, GEN VIC refers to Scarlet Alliance's submissions to the Online Safety Act, the Select Committee on Online Safety, Basic Online Safety Expectations and Age Verification for Online Pornography.	We acknowledge this concern and have sought to clarify the definitions of Class 1A and 1B materials in light of concerns about the extent these categories may capture certain commercial pornography categories. Class 1C is not in scope of these Codes and is not impacted by the guidance.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
123	Gender Equity Victoria (GEN VIC)		Education	General	We believe that online regulatory measures will be most effective when coupled with education about media literacy and consent for people of all ages, including young people.	Noted.
124	Gender Equity Victoria (GEN VIC)		Scope and Consultation	General	We commend the Online Safety Codes for some of the mechanisms outlined to ensure Australians, particularly young people, are protected from viewing violent and abhorrent material. We also appreciate that concerns from civil society organisations have been taken into consideration in the drafting of the Codes, particularly around community objections to industry surveillance of private correspondence.	Noted.
125	Gender Equity Victoria (GEN VIC)		Codes not easy to understand for public	All Codes	GEN VIC's principle concern with the Online Safety Codes is they are not easy for a lay person to understand. Online safety expectations and Codes need to be intelligible for as many people as possible, not only those with a law or legal background. Therefore, our first recommendation is that the final Codes be written to be clearly understandable by lay people.	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1A and Class 1B materials. Note in particular this resulted in the industry using technical concepts in the OSA such as definitions of different categories of services regulated by the Codes and adopting a Code structure based on the eSafety Commissioner's Position Paper. We note that it is exceedingly difficult to draft Codes that provide sufficient legal and technical detail for companies to comply while at the same time being easily understood by lay people. However, ultimately, companies need to comply with the Codes and derive sufficient direction and legal certainty from the Codes. We also note that the eSafety Commissioner requires a certain legal language to find the Codes enforceable.
126	Gender Equity Victoria (GEN VIC)		Class 1B material	All Codes	Online Safety Codes should not restrict access to safety information that may be flagged as Class 1B material.: The second recommendation we make is around how the broad scope of what is considered Class 1B material may inadvertently restrict access to safety information. Material posted online may be related to these (Class 1B) topics, and can be posted to inform, educate or raise awareness. GEN VIC's concern with the broad scope of this classification is that it could incentivise restrictions on:• harm reduction websites related to gendered violence (1)	We acknowledge these concerns. Please note that section 5.1(b)(iii) of the Head Terms require industry participants to consider the importance of protecting and promoting human rights online in implementing these Codes. In Annexure A of the Codes, we have clarified the scope of Class 1B materials as far as possible within the Constraints of the OSA and the eSafety Commissioner's Position Paper. In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					• BDSM pornography (1, 2) • political manifesto (2) • reproductive health, including abortion access (3, 4) Requiring industry to take proactive measures in removing content classified under this scheme could see industry over-zealously removing material that may be classified as Class 1B without any warning or right to redress.	there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.
127	Gender Equity Victoria (GEN VIC)		Threat of removal of material with lacking context is restricting ability to communicate about gendered violence and safety issues	All Codes	GEN VIC is concerned the Online Safety Codes may make women and gender diverse people less safe by restricting their ability to communicate online about gendered violence and safety issues. While the Codes ostensibly only cover materials that "describes, depicts, expresses or otherwise deals with matters of crime, cruelty or violence without justification", it is not clear from the Codes or the Act what "justification" means. It is quite possible that industry would pro-actively take down content that describes incidents of gendered violence from a victim-survivor's perspective, regardless of the context in which that material was posted. This may mean it is difficult for women and gender diverse people to discuss matters related to their safety online without fear of censorship and surveillance from industry.	Noted this concern. eSafety provided feedback to industry that the approach of classification of materials subject to the Codes needed to replicate the approach of the National Classification scheme. The issue raised here could be addressed by guidance provided by the eSafety Commissioner on the application of the National Classification Scheme to the categories of online materials subject to the OSA.
128	Global Network Initiative	Neutral : If carefully balanced and subject to appropriate safeguards, including regarding transparency in implementation, independent scrutiny and oversight, and opportunities for adjustment going forward, GNI is hopeful that Australia's approach can help demonstrate effective and rights-protecting content regulation. However, absent these safeguards, there is a real risk that Australia's	Scope of Codes: need for a proportional approach to regulation.	General :impact on certain business types.	The type of and proportional impact that the Codes will have on non-profits, start-ups and smaller entities should also be taken into consideration. Requirements to regulate speech may have unintended impacts on the pluralism of content and providers of consumer services that may be available. Of particular concern is that the introduction of any OP Code provisions may require ICTs to collect more information than they otherwise would for that entity's functions or activities.	We note this concern. We have sought to address the concern about the application of the Codes to smaller organisations and new entrants to the market in section 5.1(b) (iv) of the Head Terms. See also 5.1(b) (iii) of the Head Terms concerning the need for participants to have regard to human rights. The drafters of the Codes have also been mindful of the need not to pre-empt any changes that may be made to the Privacy Act 1988 (Cth) which is under review.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		approach will have negative impacts on human rights online, both in Australia and beyond.				
129	Global Network Initiative		Scope of Codes: need for a proportional approach to regulation	Application of Codes to services distant from end-users	As a general rule, the more distant a particular service is from the end user, the less visibility and granular control it has over user-generated content. Even for services that are "close" to end users, it is important to consider a variety of factors, including the type of service and its functions, the extent to which user generated content is public or private, and the extent to which content or data are persistent or ephemeral.	The approach we have taken to Code development took into account the role of products and services in scope in the digital ecosystem as explained in each schedule. section 5.1(b) of the Head Terms sets out a range of considerations that should be taken into account by services implementing the Codes.
130	Global Network Initiative		Scope of Codes and impact on ecosystem at large		Finally, it is important to understand the ways in which industry Codes may affect the Internet ecosystem at large — including research, public archiving, historical, artistic, and journalistic activities.	See above response. Note also the National Classification Scheme allows context to be considered in classifying material as explained in Annexure A of the Head terms.
131	Global Network Initiative		Relationship between Codes and Commissioners standards that revise industry positions	General	Where there is a discrepancy between the eSafety Commissioner's position paper and the industry Codes—such as on technological tools for proactive detection—it is unclear which view will prevail in the final and binding version of the industry Codes. We recommend a system of review and oversight to ensure that the eSafety Commissioner's revisions of industry Codes are consistent with principles of human rights and democratic governance.	The assessment of Codes effectiveness will be determined by the eSafety Commissioner under the OSA. The issues raised here, concerning revisions, of the Codes can be considered as part of the Code review process in section 7.6 of the Head Terms.
132	Global Network Initiative		Relationship between Codes and other legislative schemes under review by government		We therefore recommend that a review process ensure regulatory coherence and clarity between the industry Codes, privacy legislation, and revised classification system.	These issues can be considered when the Codes are reviewed in accordance with section 7.6 of the Head Terms.
133	Global Network Initiative		Measures that require proactive detection of online content: limitations of tools	eSafety Position Paper	We have concerns about the eSafety position paper's emphasis on the significant role of proactive detection technologies. In our Policy Brief, GNI cautioned against overreliance on automated tools to proactively detect and remove content. Such tools can be flawed and often lack the ability to assess important context, and may lead to unnecessary removal	Noted. We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). Following feedback, these measures have been extended to very large Tier 1 relevant electronic services with more than 8 million monthly active Australian accounts and dating services. These measures require these services to deploy the

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					of legal content. This can result in both the under-removal of illegal content, and the unwarranted removal of legal content. In addition, there is a significant risk that the error rates and impacts of such tools will fall disproportionately on marginalized communities and voices, who are also less able or willing to use grievance or appeals mechanisms to correct these mistakes.	most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified.
134	Global Network Initiative		Incentives in Codes to encourage development of automated proactive detection tools for non CSAM categories.		Athough the industry Codes only require certain high-risk services to use hashes and other tools to detect child sex abuse material (CSAM), the Codes nevertheless encourage both the development and use of automated tools and processes to detect, report, and remove class 1 material more generally. A range of mechanisms and techniques exist for identifying, verifying, hashing, and sharing CSAM in appropriate ways. However, the same cannot be said for other categories of problematic content. This is in part due to the fact that satirical, humorous, journalistic, and counter-messaging content is much less likely to be confused for CSAM, as has been documented to be the case for violent content or other categories that may eventually be deemed "class 1" material. Given the risks inherent in these tools in these non-CSAM categories, we recommend that the Codes acknowledge these distinctions and provide guidance on how to assess and mitigate the risks to freedom of expression associated with proactive detection technologies, including through human review, redress mechanisms, and appropriate transparency.	Noted this concern. See also section 5.1(b)(iii) of the Head Terms concerning the need for participants to have regard to the importance of protecting and promoting human rights online in implementing the Codes. We agree that there are risks involved in implementing proactive detection tools for materials that require context-based judgements and investment in human moderation. Throughout the Codes guidance on proactive detection tools has been updated to assist in the accurate deployment of proactive detection systems and processes where required. We consider that industry participation and support for NGOs can play an important role in providing guidance to industry on these issues. For example, we note the work of the GIFCT, which has industry membership and has a strong focus on human rights while encouraging members to share information that can assist in combating TVEC online. We encourage industry collaboration on these types of initiatives in the Codes where appropriate.
135	Global Network Initiative		24 hour takedown rules	SMS	As described in the Codes, various services are required to remove content within 24 hours or "as soon as reasonably practicable" when there is "evidence of a serious and immediate threat to the life or physical safety of an Australian adult or child." Although GNI applauds the effort to limit such strict and short timelines to a narrower category of content, the deadline may nevertheless be very tight for services that process enormous volumes of content and could be extremely burdensome for smaller services who lack the resources to monitor and adjudicate content that quickly.	The 'as soon as reasonably practicable" time frame for removal of materials gives services leeway where it is not practical for the service to make a considered decision about content within the 24-hour time frame as explained in the accompanying guidance for those measures.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					Notwithstanding the "reasonably practicable" caveat, there is a significant risk that services will be penalized despite good-faith efforts to evaluate and remove harmful content due to the arbitrary strictness of the timeline. This could lead to an inappropriate reliance on automated detection technologies, notwithstanding their limitations.	
136	Global Network Initiative		Scope of Codes; services accessible by Australian end-users	H T, definitions, section 6.1.	The Codes are designed to cover all internet services that are accessible to Australian end-users, which means that the Codes could apply to any service, website, or provider in the world, 5 regardless of their relationship with or physical presence in Australia. This raises a range of jurisdictional questions, including the extent to which the Codes will end up impacting the services and content available to users in other jurisdictions, potential conflicts of law that could be created, forum shopping by companies and users, and whether and how companies or services not based in Australia may face consequences, including blocking in Australia. While section 6.1h of the Head Terms state that the Codes do not require breach of foreign laws about managing personal information of foreign end-users, it is unclear whether the potential conflicts between the Codes and applicable foreign or international laws have been sufficiently examined, and how contradictions will be adjudicated. We recommend further clarification on how the risks of conflicts between Australian and foreign law should be examined, understood, and avoided or resolved.	We acknowledge the challenges of the jurisdictional issues raised here in the development of these Codes and the potential for conflicts of laws issues. We have sought to align the approach to this issue in the Codes with the objectives of the OSA to improve online safety for Australians and promote online safety for Australians (see section 3 of the OSA). The resolution of conflicts of law issues raised by these Codes is a matter for the domestic courts of the jurisdiction where enforcement action is commenced. This issue is in our view outside the scope of these Codes to resolve.
137	Google	Supportive Welcomes the opportunity to be held accountable for our efforts to address online safety challenges and to increase transparency across all of the industry. We remain committed to working alongside the rest of industry towards registration of the Codes			Google supports the codification of various efforts and emerging good practices across all eight of the sectors of industry to address online safety challenges, with an oversight regime that will boost the accountability and transparency of efforts. The Codes introduce significant new safety obligations for many companies that would raise the level of protections and safeguards across the entire online industry. We believe the Codes as currently drafted strike the right balance between online safety, user privacy and freedom of expression, particularly around	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		later this year			services used for private communication and storage, and believe the proposed measures are reasonable and proportionate to the harm posed by different types of Class 1A and Class 1B material	
138	Google		Proactive detection technology; limitations	Outcome 1	There are commonly used methods across industry for detecting child sexual abuse and pro-terror material. These categories of material are easier to identify because they are often clearly illegal and because of assistance from independent third party NGOs which verify and assist companies in removing this material. YouTube uses the GIFCT Hash Database (which contains over 320,000 unique hashes), for example, to prevent any videos identified by the database as meeting the definition of violent extremism from being uploaded to YouTube. Google / YouTube also uses the Content Safety API to identify new and unseen examples of CSAM. However, these tools have their limitations. For example, the GIFCT Hash Database is made up of hashes added by member companies on the basis of violations of their policies and only for entities designated by the United Nations or perpetrator-produced content following a real-world violent extremist event. Hashes contained within this database are not labelled by legality or illegality, either under Australian or any other law. The GIFCT Hash Database, along with other CSAM related hash databases, only contains hashed images or videos that have been seen before; they do not detect new or novel content. There is also no industry standard or tool used by industry today to proactively detect extreme crime and violence or other types of Class 1B material. These types of material are much harder for an algorithm to detect (and therefore the margin for error when seeking to automatically detect this content would be significantly higher) and require greater human intervention to review (which takes more time). For example, in the context of content that depicts crime and violence, differentiating between documentary footage, content produced by actors, a video of a real life fight, martial arts training resources and satirical / humorous horse play requires significant	Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					human intervention and cannot be left to technological scanning to moderate.	
139	Google		Proactive detection tools: scope of services which should be required to deploy these tools outside of SMS and Search services.	eSafety Position Paper	While Google employs proactive detection on YouTube and in limited context search (for example, with known CSAM links), Google does not support broadening proactive detection measures in the Codes to services that are considered to be more private to an individual, such as messaging or file / photo storage services.	Noted.
140	Greg Tannahill	I agree with and support the comments made publicly by Electronic Frontiers Australia and others as to the Codes being unnecessary and unworkable, and as to specific criticism of the content of the Codes	Codes inappropriate means to regulate	General	To the extent that the Australian government regulates the internet, it should not be through the mechanism of industry Codes, as this places key decisions affecting the rights and privacy of Australians in the hands of private corporations, many of them based overseas, with no clear path of transparency, accountability, or review.	We note this concern but consider that this is an issue to be addressed by the government, rather than industry.
141	Greg Tannahill		Appeal and redress, Judicial review, and FOI	General	The industry Codes should not be adopted or proceeded with without a clear, legislated means of third-party review of decisions under these Codes, which should sit outside the eSafety Commissioner with an ombudsman-like office. The industry Codes should not be adopted or proceeded with without a clear, legislated right of judicial review, and freedom of information provisions to allow Australians to access data about decisions and how they were made.	We note this issue, but we consider that it can only be addressed by the government.
142	Greg Tannahill		Regulation by the Commissioner and personal qualifications of the current Commissioner	General	The management of this aspect of internet regulation should either not sit with the eSafety Commissioner, or the position of eSafety Commissioner should be restaffed. I note that the current eSafety Commissioner Julie Inman-Grant was originally appointed to a role that had dramatically lesser responsibilities and operated as an advocate rather than a regulator, and that during her time in the position Ms Inman-Grant has made numerous lapses of judgement that call into question her understanding of the space she	We note this concern but consider that this is an issue to be addressed by the government, rather than industry.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					is regulating, and her professional ability to regulate it. Given the significance of the area being regulated, a review should be undertaken into the appropriate office to hold the relevant powers. Many of my complaints above specifically mention the skill and professional qualifications of the eSafety Commissioner, and therefore note the inherent conflict in the eSafety Commissioner being the position running the consultation	
143	Greg Tannahill		Consultation	General	Noting the refusal of the eSafety Office to engage respectively and proactively with affected parties and industries on this process, including sex workers, adult industries, the LGBTIQA+ community, women's health providers, the current consultation process should be terminated and restarted under a new auspice, such as a parliamentary committee. I note also the failure of industry themselves to respectively and proactively engage with the parties mentioned above in the development of these Codes and note that it is unlikely that industry will do that consultation in future about the way in which the Codes are implemented and maintained. Also see above re Commissioner.	We note this issue but we consider that it can only be addressed by the government. We consider that we have engaged with a broad range of stakeholders, within the constraints of the short time frame for consultation, including via roundtables and research of the community views. Details of these additional consultation processes are published on onlinesafty.org.au.
144	Greg Tannahill		Discrimination of smaller players on basis of technology, leading to less choice for consumers		The nature of the proposed industry Codes is flawed because the resources needed for a company to provide the level of moderation and assurance contained in them are ONLY available to "big tech", and their adoption will forever shut smaller companies and innovators out of important digital spaces, leading to a reduction in competition and consumer choice and ironically entrenching the very players and issues the Codes are aimed at regulating.	We note these concerns. We have sought to address the potential impact on small businesses/start ups in section 5.1(b)(iii) of the Head Terms. We note that it is also open to the eSafety to address these matters in policies for the enforcement of the Codes.
145	Greg Tannahill		Over-removalof content		The inevitable nature of the content moderation that the Codes are aimed at achieving is likely to lead to over-moderation, and the suppression and censorship of a wide range of legal and necessary speech and content, including sexual health and maternity information, queer content, resources for	We note these concerns.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					trans, genderqueer and intersex Australians, legal erotica, resources for sex workers and adult industries, resources and promotion for burlesque dancers and drag shows, political speech touching on any of the topics above, and certain religious speech. History has shown: government regulation has instead caused more harm and benefit (ref. FOSTA/SESTA in the US, shutdown of Switter) Internet regulation of social media sites such as that contained in the Codes has flow-on effects to related industries who may over-censor or deny services to certain industries in order to minimise their regulatory risk. Examples of this include banks and finance providers refusing services to adult industries; internet hosts refusing to host otherwise legal sites with adult, queer, or women's health content; search engines blocking or omitting links to legal sites based on keyword moderation. The cumulative effect of these can be to ostracise and discriminate against Australians in vulnerable communities or industries who are engaged in legal activity.	
146	Greg Tannahill		Objection to Classification system as the basis of the Codes		- Firstly, the Australian classification system is overdue for review and is acknowledged by all parties to be outdated and in need of significant refreshing. - Secondly, the Australian classification system was never intended to classify content created by individuals and shared on a non-commercial basis on social networks. (Indeed, social networks didn't meaningfully exist when it last received a significant overhaul.) - Thirdly, decisions by the Classification Board are made (in theory) by a group of qualified and specialised individuals after careful consideration, in consultation with the relevant content creator, and are subject to FOI request and both internal and external avenues of review. The current regulation scheme instead asks corporations, private individuals, and/or the eSafety Commissioner to "deem" a classification for content, often without any consultation or regulatory checks and balances. Noting the well-documented historical difficulty of classifying material according to "community standards", this	We note these concerns but consider that these are issues for the eSafety Commissioner and the State and Federal governments.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					process is almost certain to result in bad decisions, usually leaning towards a bias towards censorship in order to minimise risk to the decision-maker. - Finally, I note that the eSafety Commissioner Julie Inman-Grant has stated on public record that she has no relevant qualifications or experience in content classification, does not intend to seek training or professional development in that area, and would not know where such training or development might be obtained from. If I understand correctly, she intends to fill that expertise gap by hiring appropriately qualified staff, but given it is the eSafety Commissioner herself who would hold and exercise the relevant power, it raises questions as to how she can personally hold an informed position on what classification a given piece of content should hold.	
147	Greg Tannahill		Codes are unnecessary/disproportionate to harm/not based on evidence		There is no compelling evidence that the changes brought about by the Codes are necessary, or that they meaningfully address any identifiable harm to any Australian, or that they achieve any goal that is proportionate to the imposition on the rights and privacy of Australians that they represent. Any Codes adopted must arise from an evidence-based approach, and be derived from clear peer-reviewed evidence showing that the proposed actions are likely to have a measurable effect on an identifiable harm eSafety Commissioner and police at the federal and state levels already have existing powers to address many of the harms purported to be addressed by these Codes, including intimate image crime and child sexual abuse material, and these powers are either already being used to achieve the desired aims, or the relevant bodies have declined to exercise those powers. the most notable and high-profile cases of online harassment and abuse in Australia over the last year, including the harassment of female journalists and the saga of stalking/doxxing site Kiwifarms, would not be captured or helped by these proposed industry Codes, and that the eSafety Commissioner has declined to use her existing powers to intercede in these matters.	We note these concerns but consider that the need for the Codes is a matter for the eSafety and government rather than industry. Please note that the Codes have sought to take into account concerns about user privacy and surveillance and human rights. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
148	Greg Tannahill		Rather education to empower Australians		Effect of granting additional powers and privileges to the existing established and powerful players in the online space. I would urge the government to rethink its regulatory direction and ask instead how to empower Australians through education, culture change, transparency, privacy and protection of rights	We note this concern and consider that this is an issue for the government, rather than industry.
149	Greg Tannahill				I have deep concerns over the direction any 'privacy policy' takes law enforcement, censorship, and basic human rights. I know how it works, you can appeal to over 50% of the population by the inference of the need to protect children from sexual exploytation….and then hitch your wagon of of policies to that and get support that eats into everyones right to privacy. Just remember though any policies that allows non consensual details to be collected from people, is open to abuse, no mater the good intentions with which it was introduced. Imagine a cohort of Muslims setting the standard of dress for film classification. Or some 'Hillsong' religious person in power that decides we should go back to the religious sensorship of the 1930's when we were all good God fairing people, no kissing or pictures of any couples in bed etc. I even question the need for sensorship of child pornography, if it was generated in computer simulations without any actual children being involved! And no actual crime has taken place without the use of the children, so the crime should not be in the picture of the crime….for it is a slippery slope, if the same standards were applied to crime of murder, all those watching murder misteries on television and elsewhere would be guilty of engaging in murder. Not that I wish to be seen advocating child pornography or anything, I'm just trying to make a point, that privacy policies hatched from some misdirected good intention can go off the rails and are never going to be fit for purpose in a modern free society, in which a new election outcome could see daconian controls in the wrong hands!	The Codes have sought to take into account concerns about user privacy and surveillance and human rights. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
150	ICMEC Australia	The scope and substance of the draft	Drafting approach and	General	Complexity and length of Codes may hamper compliance.	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		Codes proposed by the Steering Committee, as one means of contributing to this goal, are commendable but can be improved in terms of protecting children from sexual abuse online	structure		Each industry Code is required to be read in tandem with the Head Terms, which includes reference to sections of the Online Safety Act 2021(Cth), several legal definitions, and complex procedures for service providers. This can make it difficult for people without adequate training to interpret and apply the Codes in practice and consistently implement the compliance measures. Drafting approach may prove too static as crimes are constantly changing. Advances in technology such as virtual reality and changes to the marketplace can alter the way CSEM material is shared or created such that it could exist outside the parameters of the Codes. This drafting approach may also impede business risk assessments and the use of those assessments in identifying, investigating, and responding to CSEM risks	feedback provided by eSafety through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1 materials. We note that these constraints resulted in the industry using technical concepts in the OSA such as definitions of different categories of services and products regulated by the Codes and adopting a Code structure based on the eSafety Commissioner's Position Paper. The two year review process of the Head Terms provides opportunities for adjustments to the Code to address new online safety challenges associated with online materials subject to the OSA.
151	ICMEC Australia		Focus of Codes on Content categories as defined under the Classification scheme	General	Significant focus on classification of materials risks a departure from the main intent of the Codes (to reduce harm). Redraft to re-balance their focus toward actions to reduce harm against children.	See above response.
152	ICMEC Australia		De-platforming users	Measures requiring enforcement of policies concerning Class 1A materials	Requiring immediate removal of offending platform users could, in some circumstances, prevent a more comprehensive response to harm. In some circumstances (recognising, of course, the need to carefully balance against the threat of continuing harm), requiring platform users to be placed on watch without removing them.	The approach adopted by industry in the Codes aligns with the eSafety Commissioner's Position Paper and the OSA which is targeted at the removal of Class 1A materials.
153	ICMEC Australia		Lack of transparency for reasons users de-platformed		If clear reasons for decisions taken under the Codes or Act, together with information on avenues for review / appeal are not provided, it could foster negativity toward the Codes, in turn impacting their legitimacy and limiting support from end-users and service providers. The Codes should require reasons for some or all decisions by participants to be documented and provided to end-users upon request.	In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.
154	ICMEC Australia		Codes are silent on Case		Service providers should be adequately resourced, including an ability to complete	We consider the Codes contain appropriate measures concerning the resourcing of trust and safety functions

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			management resourcing i.e., people resources as opposed to technological resources		timely human reviews of material where appropriate. Regarding Item 5 above, there may be cases where innocent activity is caught by machine rules, and customers will need a non-machine review process. All draft Codes should be added requiring a (non-prescriptive) investment in adequate resourcing to ensure compliance, human review of decisions, and rights of appeal	by relevant service providers. See above response re the inclusion of further appeals mechanisms.
155	ICMEC Australia		Codes may place disproportionate compliance burden on some industry participant	General/DIS code	Small businesses and community groups are unlikely to have the same time, resources, and technical knowledge to comply with the draft Codes as larger corporations or businesses facing higher CSEM risk.	The Codes seek to address this concern in the Head Terms and in the approach of risk to DIS which classifies certain types of businesses as Tier 3(which are subject only to optional compliance measures). It is also open to the eSafety Commissioner to deal with this issue in policies for the enforcement of the Codes.
156	ICMEC Australia		Not enough emphasis on new and improved forms of technology to identify materials	Proactive detection measures DIS, SMS	As drafted the draft Codes could be seen as not encouraging new technology that can proactively detect and prevent new forms of CSEM as they are created. This seems an odd response for the technological industry to pursue, as the eSafety requirements provide a regulatory stimulus to the development of more effective CSEM screening and blocking technologies. Once developed, the cost of these solutions will drop for all the organisations using them (in Australia and offshore), with the potential to remove many children from harm	We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). In response to feedback, the RES code has been amended to require proactive detection of known CSAM by very large Tier 1 RES (with over 8 million monthly active Australian accounts) and dating services. These measures require these services to deploy the most accurate available approaches to detecting CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified. We acknowledge the concern that additional proactive detection technology be developed to detect new forms of CSEM online. We consider that the Codes address this in an appropriate way, for example by requiring ongoing investments in safety by Tier 1 SMS, RES and DIS providers. Both the Outcomes based approach combined with the expectations in the BOSE also incentivise the industry to strive to improve their response to CSAM, including through collaboration with NGOs.
157	ICMEC Australia		Review of Codes process	Head Terms	No obligation to review Codes to assess their continued effectiveness and / or measure their success in delivering on their intent risk	We consider that these issues are dealt with appropriately in section 7.1 of the Head Terms.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					applying ineffective Codes	
158	ICMEC Australia		Industry Collaboration	Outcome 5	The private sector should be encouraged to share and collaborate with one another on data and insights to ensure their design and development processes align and are effective as a matter of market practice.	A general requirement encouraging sharing and alignment of technology under development as a 'matter of market practice risks' creating compliance issues for companies under competition law. We note that the Codes do encourage industry cooperation through appropriate, open forums.
159	ICMEC Australia		Need to take into account victim and survivor considerations re CSEM	General	The Five Country Ministerial Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse highlight the importance of victim and survivor considerations to companies' response to CSEM. This includes how companies initiate reporting mechanisms, taking into consideration the lived experience and trauma caused by persons reporting material published or otherwise available on their platforms or services. It also notes the need for specialised approaches for children given their vulnerability as users of platforms or services	We acknowledge this concern. The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1 materials. We have, however, included a range of measures throughout the Codes that are specifically designed to protect children.
160	ICMEC Australia		Need to boost end user engagement to combat CSEM	CSEM reporting measures	The Codes place most of the responsibility for combatting CSE on service providers. However, end-user engagement is integral to assist service providers with reporting CSEM content and preventing its spread.	See above response.
161	ICMEC Australia		Provide additional guidance to address complexity	General	Simplify Codes and / or produce practical guidance material complete with examples in a separate accompanying publication for each industry section.	See above response on the reasons for the drafting approach.
162	ICMEC Australia		Principles based drafting approach	General	Adopt a principles-based drafting approach where possible to future-proof Codes. This also aligns with the approach taken in the Five Country Ministerial Voluntary Principles to Counter Child Sexual Exploitation and Abuse	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1A and Class 1B materials. Note in particular this resulted in the industry using technical concepts in the OSA such as definitions of different categories of services regulated by the Codes and adopting a Code structure based on the eSafety Commissioner's Position Paper.
163	IIS Partners	We have not provided commentary on Code contents; rather, we consider foundational	Process for Codes development	General	It is unclear from the documentation published at onlinesafety.org (i.e., the Explanatory Paper and the draft Codes) the extent to which robust community consultation has been	The approach to consultation was informed by the OSA and the eSafety Commissioner's Position Paper. The Code developers have sought community views both through this submission process, direct invitations to

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		matters that are impactful to the contents (and success of a Codes-based regime). We focus on: • Recent learnings about Codes (having been formally involved in regulator Code review processes), including commentary on using Code Developers and the importance of further Code consolidation, and • Understanding the Codes in context, noting related public policy imperatives and the importance of being able to read and understand the Codes.			undertaken by the Code Developers in their initial creation of the draft Codes, which IIS notes would be in addition to the eSafety Commissioner's expectations set out in section 4 of the eSafety Position Paper (Position 8), which simply requires this level consultation prior to registration of the Codes. Suggest drafters clarify the extent to which Code Developers have proactively engaged with the community in Code development to-date, and ensure ongoing involvement of the community in future Code iterations.	make submissions to more than 150 organisations and through a roundtable with stakeholders conducted by the Steering Group. Additionally, the Steering Group sought the views of the community by commissioning research by Resolve Strategic, published on onlinesafety.org.au.
164	IIS Partners		Number of Codes/difficult for the public to understand.		Explore opportunities to further consolidate or otherwise limit the number of Codes.	The approach to Code development including separate Codes was informed by the OSA. Section 137 of the OSA makes clear that Codes should cover the section of the industry and activities described in section 134 and section 135. Owing to the diversity of services and products in scope, we concluded that additional consolidation was not achievable.
165	IIS Partners		Explanatory paper/ Accompanying explanatory memoranda	General	IIS considers that the Explanatory Paper for the proposed Codes is a meaningful opportunity for the Code Developers to clarify how key online safety concepts are enmeshed with other Australian public policy imperatives. Additionally, material covered in the Explanatory Paper may – at an appropriate juncture – form the basis for Guidelines (on the operation of the Codes) and other educational materials for industry and the community more broadly.	Noted.
166	IIS Partners		Definitions	Head Terms e.g., end-user	Based on definitions in the Online Safety Act, IIS queries who an end-user is intended to be in the context of the Codes – an adult, a child, a parent, an Australian adult, an Australian child, Australians, a target of cyber-abuse or cyber-bullying material, all of these, none of these, or something else? Suggest revisit definitions in Head Terms to ensure	The OSA refers to end-users in various places but this term is undefined. The approach taken to defining end-users in the Codes was informed by the objects of the OSA set out in section 3, following discussions with eSafety during the Code development process.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					consistency with those in the Online Safety Act.	
167	International Justice Mission of Australia	Commend the industry associations for detailing measures in the draft Codes by which digital service providers can proactively detect and remove the most harmful online content and take greater responsibility to ensure a safer online environment.	Proactive detection measures limited to known CSAM / not applicable to encrypted services	Outcome 1	Providers of online platforms and services be required to use technological tools to detect not only known CSAM, but also first-generation CSAM and livestreamed CSAM. Providers of encrypted electronic services be required to use technological tools and behavioural indicators to detect CSAM before it enters the encrypted space.	Noted. We note that the Codes seek to impose proactive detection measures for known child sexual abuse material. These measures require services to deploy the most accurate available approaches to detecting CSEM online. The Codes imposed these measures on Tier 1 SMS services and Tier 1 DIS. Following feedback these measures were extended to very large relevant electronic services and dating services (See Schedule 2). We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified.
168	International Justice Mission of Australia		Framing of Codes	General	The digital industry tangibly support through their policies, tools, and rules the privacy and security of victims and survivors to create a safer online environment for all.	Noted.
169	Internet Association of Australia	In general, IAA agrees with the measures proposed for ISPs under the Code. We appreciate the recognition that as ISPs generally don't have control over or dealing with what content is distributed to the end-user, and thus responsibilities should be reflective of the specific role and function ISPs play in the Internet eco-system. However, there are certain compliance measures which do not reflect this principle. Furthermore, we believe the Code should provide greater clarity in certain areas to ensure effectiveness and ease the burden of compliance for ISPs.	ISPS notification of Class 1A materials to hosting service providers	Schedule 7, compliance measure 6	IAA opposes the proposed minimum compliance measure 6 which sets out a requirement for all ISPs to notify hosting service providers if the ISP becomes aware of alleged class 1A material being hosted. If such a measure is to come into place, it should be specifically and only in circumstances where the hosting service provider hosting the alleged class 1A material is a direct customer or direct partner of the ISP. This reduces burdens on the ISP having to take "reasonable steps" to identify and obtain the email address of a potentially random hosting provider the ISP does not have any relationship with. The Internet industry is not a law enforcement network and industry participants should not be made to take on the role of general policing of the Internet.	We note that the incidences of this occurring are likely to be very minimal (to say the least). The requirement is to take 'reasonable steps' to identify the hosting provider, this could be a quick online search on the ACID tool. We do not believe this requirement to be overly burdensome or onerous.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
170	Internet Association of Australia		Reporting by ISPs	Schedule 7 Minimum compliance measure 14	There should be limited circumstances wherein ISPs are requested to submit a Code report to eSafety. For example, the circumstances could be limited to where there have been complaints specifically against the ISP, where eSafety is aware of class 1A or 1B material that was distributed online involving the ISP's direct customer carriage services	Noted. The reporting requirements seek to balance the need to respond to the eSafety Commissioner's Position Paper and feedback provided during the Code development process concerning reporting with concerns about the extent ISP's ought to and can report on online content given their role in the digital ecosystem. Hence reporting in measure 14 to eSafety is by request only.
171	Internet Association of Australia		Record keeping of compliance	H T clause 7.2 (b)	At clause 7.2(b) under Head Terms, we believe the requirement for all industry participants to keep records of compliance measures for "reasonable period" is too vague and clarity should be provided., A period of two years could ease regulatory burdens on the telecommunications sector by setting out a time period consistent with other data retention laws applicable to the sector.	We have taken this feedback on board and amended the head terms to limit retention of records under section 7.2 (b) of the Head Terms to two years.
172	IoT Alliance Australia (IoTAA)	Welcomes the new only safety industry Codes initiative, and recognises its need and importance	Scope of material	All Codes	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.	Noted. The approach is consistent with this view.
173	IoT Alliance Australia (IoTAA)		IoT devices potentially in scope	Equipment	Concern that the focus on "traditional" online community has to some extent ignored fast growing newer Internet of Things industry community whose primary focus is not general internet access and would in general be of a lower risk profile but may, nevertheless, be subject to the industry Codes suggested, without proper awareness and consultation.	We acknowledge that concern and have sought to address this in the approach to risk in Schedule 8.
174	IoT Alliance Australia (IoTAA)		Risk of non-compliance by IoT sector due to lack of understanding of Tiering / ill-defined access/boundaries	Equipment	There is a real risk that the IoT community may fail in its adherence to the code, because: - the Tier1/2/3 boundaries are not yet understood, - IoT technologies are evolving and their risk status may well change during a device lifecycle – how this be managed is not understood - Of ignorance of code and whether it applies to them. Applaud Codes that "design measures that are reasonable and proportionate to the service and harm type in question" but are concerned that the device boundaries suggested in Schedule 8, are not necessarily understood by the IoT device community. (This may include devices, for example, which	Noted. It is difficult to future-proof the Codes against future technological definitions in light of the broad scope of this section of the industry in the OSA. We have endeavored to respond to this concern in our approach to risk assessment and guidance.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					have hitherto been provided for closed operational technology (OT) but now whose functionality now includes broader internet access to accommodate on open and collaborative eco-system. Such as AR/VR devices for maintenance)	
175	Jade Jackson	General opposition to the Codes	Warrantless mass surveillance of private data and comms	General	I do not consent to the warrantless surveillance of my personal and private data and communications. The proposed online safety Codes treat all Australians as criminals. The age old excuse of 'child exploitation' won't hide your real intent - total surveillance and control of all information.	This concern is noted. The Codes have sought to take into account concerns about user privacy and surveillance.
176	Jade Jackson		Opposition to limitation of free speech that the Codes seek to implement	General	The Australian Government Corporation does not approve of free speech and free thought as recently expressed by the Australian eSafety Commissioner, Julie Inman Grant, when she said "we're going to have to think about a recalibration of a whole range of human rights" like "freedom of speech". The rating system will be used to monitor and censor opinions deemed unacceptable like alternative views on government health measures or climate change. When Jacinda Ardern referred to freedom of speech as a "weapon of war" while addressing the UN General Assembly she was expressing a view shared by governments and NGOs worldwide. The attack on free speech and privacy is global. The Australian people would like the Australian Government Corporation to back off and stop this march towards the Chinese style mass surveillance and social credit system you're so desperately trying to implement.	This concern is noted. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
177	Joint submission of the ARC Centre of Excellence for Automated Decision-Making and Society and QUT Digital Media Research Centre	Neutral. Further development of the Codes be paused until they can be aligned with any legislative changes resulting from current policy reviews, including particularly on privacy and classification. ● The coverage thresholds for application of the Codes				Noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		to different providers is clarified as a priority. ● The complaints, detection, removal, and downranking mechanisms in the Codes be limited to clearly unlawful material under Class 1A only and should not be extended to lawful material in the outdated RC category. ● The Codes guarantee support for independent research in the public interest, building on the commitments to transparency and accountability developed in the Australian Code of Practice on Disinformation and Misinformation.				
178	Joshua Gavin		Codes too onerous for small tech companies	General	if the Codes are implemented as are they will continue the brain drain as the tech industry flees Australia for more accommodating nations.	This concern is noted.
179	Joshua Gavin		Anonymity, account creation	SMS, RES	I also feel that the Codes as they are constituting a serious cyber security risk by mandating that all companies with interactive online presence record visitor's identity credentials like drivers license or passport. If companies like Optus or government departments like the NSW Roads and Maritime Services can experience data breaches that result in threat actors gaining access to treasure troves of thousands of millions of identity documents that enable identity theft, what hope do start-ups with a limited cyber security capability have to protect such information? Again, considering the fallout of such data breaches, it is pointless to require personal ID to authenticate someone's social media account. Many identities can be found online for free, and criminals can easily buy bundles of identities, enough to facilitate identity theft off darknet forums with little trouble if they	We have taken this concern on board and clarified in the Head Terms that the Codes do not require users to provide personal identification or the implementation of age assurance measures. Please also see section 6.1 of the Head Terms which also limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					want to post illegal content, or perform scams. Cyberbullying is something that also carries a high risk of identity theft. The attacker knows intimate details about the victim and has incentive to impersonate the victim to frame them as part of a larger attack.	
180	Karina Honeyman		Hate speech (power of companies to classify material)		What is important is not what they report but what "they" classify as hate speech. zuckerberg thinks the word golliwog is hate speech, zuckerberg says saying hitler also thought god was on his side is hate speech. who is some idiot american to say what we can say and cant say. hate speech is being used as a front for censorship and censorship of ridiculous parameters. funnily enough i can say i look forward to the day america gets obliterated without that being classified as hate speech but i cant write the word golliwog. i even had one comment of qld health isnt a tardis classified as hate speech.	Please note the scope of these Codes concerns Class 1A and I B materials as outlined in Annexure A of the Head Terms. The Codes do not regulate hate speech.
181	Mark Davenport	Reject	Concerns with privacy, data breaches, security risk.	None	General comments, non-specific change required.	See above.
182	Mark Hunter	Rejection/pointless	Reduced anonymity and lack of data minimisation, thereby increasing risk	General	Due to the current Optus fiasco. Holding ID by any agency seems to be a terrible idea. On top of that anonymity on the internet is important for people to discuss without fears of reprisal. I have seen a family member make comments about a politician who then called her workplace and attempted to have her fired as retaliation. This will be extended if people's ID is online. Further to this anyone who wants to commit crimes will use another persons ID, making the purpose of this bill pointless.	This concern is noted. We have taken this concern on board and clarified in the Head Terms that the Codes do not require users to provide personal identification or the implementation of age assurance measures. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
183	Mark Nottingham	proposed Industry Codes are harmful to the Internet itself, would have serious impacts on freedom of expression and freedom of assembly on the Australian Internet, and furthermore may have anti-competitive effects.	Scope of websites and effect of independent publications	DIS	The Designated Internet Services Online Safety Code proposes that some sites be exempt from risk assessment (and effectively, exempt from the code). Because the exemption is scoped using a closed list, many sites and content sources would be subject to this regulation, even though the risk that they represent to online safety is minimal. For example, a purely personal Web site (e.g., a blog) does not clearly qualify for exemption.	Note that no services are exempted from the Codes; we have only provided that some services will automatically qualify to be designated Tier 3 in certain instances to reduce the impact of the Codes on lowest risk services.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		If adopted, we are concerned that the Codes will the effect of handing control of the Australian Internet over to the biggest of technology enterprises, endangering both the economic health of this country and the basic societal tenets of what it means to be a healthy democracy in today's world.			Neither does a community group, a site for a shared interest or hobby, an online tool, or even a joke site. All are common on the Internet. Furthermore, because the definitions of each kind of site qualifying for exemption are open to interpretation, application of any such exemption is not likely to be consistent, and the resulting doubt is likely to create a strong chilling effect on independent online publication. For example, does a site about health issues qualify as 'health', or does one need to be registered with a recognised health-related authority to qualify? Is my personal site considered 'professional' because I talk about mostly professional things on it, or does it need to be associated with an ABN? Will 'academic research' only be considered such when its online publication occurs via an.edu.au domain name? These overly broad effects are not limited to Designated Internet Services. Designated Internet Services The Designated Internet Services Online Safety Code nominates types of Web sites for exemption based on a closed list. This is problematic for the reasons discussed above. Adding new types of sites to the list is not appropriate, because there is not a closed list of things you can do on the Internet. It also disqualifies any site that allows 'end-users to upload content'. This is unworkable, since 'content' is such a broad concept. Sites that allow chat or messaging are similarly disqualified, despite the arguments regarding those functions above. As a result, 4(d) needs to be completely reworked. Placing an industry-focused compliance burden on most every Web site in Australia is clearly undesirable, disproportionate, and will lead to Australian online discourse and content being concentrated into a few, powerful hands. In almost every case, it's also unlikely to lead to meaningful improvements in online safety. We suggest that instead of focusing on types of sites or features they use, a good starting point would be whether they are commercial in nature and assessing their level of social	

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					impact and visibility as a baseline for inclusion in these Codes. For example, id.au domains should not require compliance to industry Codes, nor should similar sites in other top-level domains	
184	Mark Nottingham		Scope of services too broad	SMS	Social Media Services: The Social Medial Services Online Safety Code applies to any service whose primary purpose is 'online social interaction 'that 'allows end-users to post material on the service.' With such a broad definition, this Code is likely to include any online gathering place in Australia – even ad hoc, non-commercial ones. The proposed Code does exempt Tier 3 services, but such services cannot 'create a list of end-users with whom an individual shares a connection with…', 'view and navigate a list of See Competition and Consumer Act 2010 (Cth), s 45AD. 12 Social Media Code (n 6), s 2.1(c)(i)(C). 6 other end-user's individual connections', or 'construct a public or semi-public profile within the bounded system created by the service. These restrictions are problematic. These effects can be mitigated by removing 3(d)(iii). If the Commissioner feels that is too broad, an additional requirement that the service be non-commercial could be added. Also, if industry and the Commissioner were to give meaningful support to non-commercial and small services regarding their compliance requirements – for example, guides, tools, advice, help desks, Open-Source software to support certain functions (provided it wasn't used as a backdoor to collect more data), that might also assist this sector in maintaining their online presence. However, any requirement on smaller services should not be imposed until such support is available for a service's chosen tools, and of high quality. In either case, public services not provided by any one entity (for example, Usenet) that are based upon widely recognised technical standards should be explicitly exempted, to remove any doubt about how they should be handled by other parties. While such services are not free from problematic content (by any means), applying Industry Codes to them is	We note these concerns and consider that it is open to the eSafety Commissioner to deal with these in policies for the enforcement of the Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					inappropriate and unlikely to lead to better safety outcomes. Their regulation should be considered separately.	
185	Mark Nottingham		Scope of services too broad	RES	Relevant Electronic Services Like Social Media Services, the Relevant Electronic Services Online Safety Code predicates qualification for Tier 3(and thus exemption) on not allowing 'end-users to view a list of other users' individual connections', 'search for other end-users […] using known identifiers', 'search for other end-users […] based on interests or keywords', and 'recommend[ing] other contacts […] based on interests or shared connections.' Again, this is too broad; messaging is a fundamental activity on the Internet, and identity (and thus profiles) are intrinsic to it. Tying a large compliance burden to these functions effectively hobbles many potential Internet services and drives more traffic to 'big tech' platforms. These concerns could be addressed by removing, in 6(c), the box at the intersection of 'Tier 3 Indicators' and 'Discoverability of users.' As with social media services, an alternative approach might be to provide adequate support. And, as with Social Media Services, public services not provided by any one entity (for example, IRC, Matrix and Mastodon) that are based upon widely recognised technical standards should be explicitly exempted	Noted. We think that the approach to risks is appropriate given the diverse services in scope, many of which do not have these functionalities. We consider that it is open to the eSafety Commissioner to deal with concerns about the impact of the Codes on small businesses in policies for the enforcement of the Codes.
186	Mark Nottingham		Open source captured, criteria for equipment classification	Equipment	Equipment The Equipment Online Safety Code currently tiers its application by degree of user interactivity. While this is one important metric, it also captures significant hobbyist and Open-Source community members. Requiring compliance from these participants is not proportional. It is also not effective; because most projects have at least some overseas contributors, the regulatory burden inherent in the proposed Code creates a disincentive for Australian participation and innovation, rather than leading to safer outcomes. One way to mitigate this over-regulation	eSafety Commissioner provided feedback during the development of the Codes that industry should not alter the scope of the Codes by altering the definitions of the OSA, including by exempting services from the Codes. In general, we do not think Open Source applications should be treated differently under the Code. We note that it is open to the eSafety Commissioner to address this issue in policies for the enforcement of the Codes.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					would be to have the Code only apply to equipment and Operating Systems that are commercially available in Australia, explicitly exempting nonprofit, community-based and hobbyist efforts.	
187	Millie Novak		Surveillance of private storage, search history and comms	General	We move into dangerous territory when online safety can be used as online surveillance and data collection of individuals. I could have chosen to spy on my children's online search history, but instead decided to promote trust and a sense of responsibility. Censorship has been a disservice in recent times and what may be deemed disinformation today may well be true tomorrow. Preventing harmful content should be the onus of the companies; to view every citizen as a potential criminal is like non-stop spying on my children, leaving no room for dignity or trust to evolve.	This concern is noted. The Codes have sought to take into account concerns about user privacy and surveillance. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
188	Mouna Ibrahim	Reject		General	Get a live Get out of our lives or suffer the consequences.	This concern is noted.
189	Nicholas Davis	I plead with the commission and the industry to send these Codes back for rewriting and reiterate my opposition to the act, the commission and the attempts to censor the rights of Australians, treating them as criminals, failing to respect innocent until proven guilty and potentially destroying the integrity of the internet as we know it.	Degree of power given to eSafety Commissioner as an individual	General	The online safety Codes through the online safety act provide an unseen level of discretion and by effect power to the commissioner I fundamentally disagree with this power being given to an individual, I believe that this leaves open corruption or the use of these powers along political lines	This concern is noted but we consider that this is not an issue that can be addressed by these Codes.
190	Nicholas Davis		Freedom of speech, privacy	General	I am concerned the act and by extension these Codes do not force the consideration of potential content and the rights of the Australian public a set of examples are obviously the rights to freedom of speech, association, expression and privacy.	The Codes have sought to take into account concerns about user privacy and surveillance. Please note that we have included a requirement in section 5.1(b)(vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
						limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
191	Nicholas Davis		Risk of weakening of encryption/proactive detection	General	I am concerned the online safety act and by extension the online safety Codes may either implicitly or explicitly force or corrupt companies into weakening encryption, encryption is a technology that protects every individual that uses technology, any act that seeks to weaken encryption must be opposed at every level. The commission has said it doesn't wish to weaken encryption, but this statement does not match what it wants providers and companies to do under the Codes, for example proactive monitoring at the device level could require files to be unencrypted to be scanned. I fundamentally oppose this as a citizen, and I hope the commission listens to experts on this important matter.	Please see above. The Codes do not require service providers to weaken encryption. Please see section 6.1 the Head Terms.
192	Nicholas Davis		Privacy	General	I am concerned that the Codes effectively will weaken if not remove privacy on the internet, privacy is a fundamental human right it allows the minority to speak without fear of prosecution on many important issues, a democracy in the modern world should not be seeking to remove privacy from the internet, it should be seeking to improve privacy protections. The commissions weaponization of children to remove privacy from the internet is disingenuous at best.	The Codes have sought to take into account concerns about user privacy and surveillance. Please note that we have included a requirement in section 5.1(b) (vi) of the Head Terms that companies implementing the Code consider the importance of protecting and promoting human rights online. Please also see section 6.1 of the Head Terms which limit the operation of the Codes so as to minimise their impact on user privacy, anonymity and security.
193	Nicholas Davis		Objection to Classification system as the basis of the Codes		I fundamentally oppose the proposed classification system that these Codes will run under, the act enforces one of the biggest complaints of the Australian public, that being the classification board is a group of individuals that have the power of censoring media and expression in this country based on what they find offensive or fitting in certain categories. The classification board is a group of rich white people, how do they have the right to purport to know what content is harmful or needing to be censored to protect the public? I do not believe the classification system is fit for purpose in a modern Australia. By extent the Codes proposed being defined in part by this archaic classification system is one of the greatest abuses of power I have	The scope of the content covered by these Codes was set by the eSafety Commissioner pursuant to the OSA (see Position Paper) and is in our view a matter for the eSafety Commissioner and government, rather than industry.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					ever seen, I am genuinely fearful that this country is on a slippery slope to fascism and other horrible things I don't even want to think about. The code and the act is the definition of "the path to hell is paved with good intentions".	
194	OPTF Ltd	We are deeply concerned by the potential impact of the Online Safety Industry Codes on our operations, as we do not have the funds nor the resources to moderate content on our messaging app	Impact of Codes on start ups	RES/scope	While large, global platforms have significant resources to comply with the Codes, this will leave Australia tech projects like ours in a perilous situation, further undermining the opportunities for Australian developers to produce privacy technologies. We do not believe the Codes are fit-for-purpose, and wish to propose broader, more inclusive consultation and feedback to design a strategy which is effective for all parties concerned.	Noted. We have attempted to address this concern in section 5.1(b)(iv) of the Head Terms and by classifying as Tier 3 many categories of businesses, many of which will be smaller in nature and lower in risk due to their smaller scale. Many measures for Tier 3 services are optional. It is open to eSafety to provide further clarification on this issue in developing its enforcement policy for the Codes.
195	Pattr	We have a few concerns about areas that we see as potential missteps under the proposed/draft Codes.	Scope of Codes	H T general; impact on start ups	Stemming the tide of CSEM material and prosecuting the creators of it is an extremely noble undertaking, and one that should be applauded. It's because of how clear cut classifying CSEM material is under the law that it can be pursued so broadly. Requirements to classify or pro-actively detect pro terror content or other content that requires context judgments is a substantial regulatory burden that could drastically increase costs of bringing new services to market. These kinds of regulatory frameworks can be critical drags on innovation and could lead to many innovative new companies and technologies simply not being created in Australia, where other markets offer better protections of companies, or have less stringent regulatory requirements. Putting a 'policeman in every pocket' does not seem to be the silver bullet many in industry think it is. The concern here is the nebulous term of 'extreme crime, cruelty or violence'. This becomes an issue fraught with contextual information. This is not something that classification systems at scale are effective at handling, computers are blunt instruments that are very good at comparing a piece of content to a collection of content to say, identify a gun or a knife or even a bikini	We acknowledge this concern and have sought to address this issue in 5.1(b)(iv) of the Head Terms. It is open to the Office of the eSafety Commissioner to further address this issue in their policy on Code enforcement. Please note that the Codes seek to impose proactive detection measures for Known Child Sexual Abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). Following feedback these measures have been extended to very large Tier 1 relevant electronic services and dating services. Very large Tier 1 social media services and relevant electronic service are also subject measures to detect certain pro-terror imagery and videos online. These measures require these services to deploy the most accurate available approaches to detecting CSEM and pro-terror materials online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified.
196	Pattr		Approach to encryption	General: heads of terms, RES	The second concern Pattr has is the seeming lack of discussion around encryption and	This concern is noted.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					encrypted contents. The existence of encryption should not be seen as mitigating efforts to track and prosecute those engaging in illegal activity, but the power of encryption does stymie the ability to do a lot of this server side analysis. Even forgoing full file encryption, or individual encrypted files stored on a common file serving system (e.g Dropbox) - steganographic tools that can bypass classification systems have existed for years. Most of these Codes imagine that users would somehow willingly upload to third party services in Australia that would dynamically detect the content and report this to police, we believe it's extremely unreasonable to think that users trafficking in this kind of content would not use basic encryption technology to hide their tracks from AI systems snooping and classifying this content remotely. These are noble goals, but the means outlined in the draft Codes are both substantial in terms of a regulatory and cost burden and in light of how cheap and easy modern encryption is to use, somewhat naive when it comes to outlining legal burdens when users store content on your servers or systems that you cannot view or classify	
197	Protect Children / Suojellaan Lapsia	wish to express our sincerest support for the proposed industry Codes to regulate harmful online content. Considering the exponential growth of CSAM distributed globally and children increasingly being abused through the very platforms offered by these online service providers (OSPs), regulating their conduct is fundamental for ensuring the realisation of children's fundamental rights. Imposing mandatory, positive duties on OSPs		Objective 1, Outcome 1	The obligations proposed under Objective 1, Outcome 1 to take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material are particularly important to reduce the harms of online sexual violence against children, and therefore the strength of these obligations must be maintained – including in the process of interpretation and implementation of the Codes.	Noted. We note that the Codes seek to impose proactive detection measures for known child sexual abuse materials on SMS and DIS services that are categorised as Tier 1 (highest risk). In response to feedback these have been strengthened to include proactive detection measures for very large Tier 1 relevant electronic services with more than 8 million monthly active Australian accounts and dating services. These measures require these services to deploy the most accurate available technology to detect CSEM online. We consider this approach appropriate, given concerns in submissions about end-user privacy on other service categories and the resultant risks end-users are subjected to inappropriate enforcement action where materials are inaccurately identified.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		is a necessary step, as current global measures, which mainly rely on voluntary efforts, are evidently not sufficient, nor is solely relying on reactive methodologies for taking down CSAM. We must adopt a proactive approach on a large scale to truly tackle the problem and to protect children from all forms of sexual violence, grooming, and harassment				
198	Protect Children / Suojellaan Lapsia		International cooperation is needed to combat CSAM	General	The issue of CSAM use requires international cooperation to achieve significant results	Noted.
199	Relationships Australia	Neutral: do not consider the extent to which the draft Codes adopt the positions, meet the expectations, or follow the guidelines set out in the eSafety Commissioner's Position Paper, Development of industry Codes under the Online Safety Act. Nor do we express views on whether proposed measures are reasonable and proportionate, given that we are not in a position to assess risk posed by services and devices.	Framing of Codes with respect to vulnerable groups	General	The draft Codes expressly acknowledge that perpetrators of family domestic and sexual violence (including intimate partner violence, abuse of children and young persons, and abuse of older persons) create, share and store Class 1A and 1B materials (see below for further discussion of the use, risks, harms and other impacts of technology-facilitated abuse). Acknowledge that where Class 1A and 1B materials are created, shared and stored within such a context, there are particular power imbalances, risk factors and vulnerabilities that may not arise in other contexts and that inherently elevate the impact and likelihood of severe and enduring harm to victim/survivors.	See above response.
200	Relationships Australia		Consultation with children	General	Industry directly engage with children and young people, including by establishing a specialist advisory group comprised of children and young people, to further inform development of the Codes, as well as to inform implementation and periodic review	A broad range of non- profits, including those that work with children and vulnerable groups, have provided input into the consultation process both via the submissions process and the roundtable of stakeholders conducted by the Steering Group.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
						More extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
201	Relationships Australia		Consultation with people with disability	General	Industry directly engage with people living with disability, and their advocates, carers and service providers, to develop tailored arrangements to deter, detect and take appropriate regulatory action against, scammers targeting people with disability in the digital ecosystem.	See above.
202	Relationships Australia		Class 1A and I B material	Supports threshold for Codes content	This is inherently material that will cause the most severe impacts on those depicted in, exposed to, or otherwise attributed to the material (for example, seeking to implicate a former partner (or a new partner of a former partner) in the production and distribution of CSEM or pro-terror materials, as well as in the commission of other offences. This can be used, for example, to attempt to gain leverage in contested parenting or property matters	Noted.
203	Reset Australia	Negative: The Online Safety Codes fail to provide appropriate safeguards for children. They will not improve online safety for children in Australia; in some instances they would undermine existing safety practices and in others fail to offer global standards of protection. The problems with these Codes are systemic and significant. We recommend that these Codes not be put forward for registration.	Standards for reporting CSEM lower than some existing state legislation	Measure 1 SMS measure 8 RES etc.	Current legal requirements around suspecting child sexual abuse are higher in Queensland, Tasmania, the Northern Territory, Victoria and New South Wales 1. In these States and Territories, child protection laws and criminal Codes have created an obligation to disclose; all adults (including those employed by tech companies) must report all suspicions or CSEM. This Code proposes that child sexual exploitation material needs to reach a higher threshold before it is reported. Rather than simply identifying abuse, a social media service would need to believe that abuse material also constituted 'a serious and immediate threat' to a child. This opens up space for interpretation and proposes making reporting requirements harder to reach. This has the effect of weakening protections for children. This is also weaker when compared to global CSEM reporting standards. For example, the UK's draft Online Safety Act requires all child sexual exploitation and abuse content to be reported when it is detected, with detection defined as simply "when a provider becomes aware of the content", without space for	In response to feedback, we have clarified that the Codes supplement Australian legislation that required reporting of this material. The Codes have been drafted to take into account the need for services to comply with the Privacy Act 1988 (Cth) which provides limited circumstances in which personal information can be provided to law enforcement. Note that the UK legislation is still to pass parliament and, in its current form, only applies to a specific companie by determination for a limited duration, as opposed to the OSA which is actual legislation (i.e. has parliament) and applies to a very broad range of organisations, without limited duration. Similarly, the Codes apply across a wide range of organisations and without limited duration.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					interpretation about threat levels	
204	Reset Australia		Children less protected under Codes than in some other jurisdictions	E.g. Safety by design measures for children such as default privacy settings	For example, if we compare the proposals in Australian Codes to protect children by defaulting their accounts to private, we see how Australian children will be less protected under these Codes. Australian 16 & 17 year olds would not have the same protections as other young people. 16 & 17 year olds should be protected from unwanted contact with adult strangers	In response to feedback the Code provisions concerning privacy settings on children's accounts have been amended to apply to children under 16.
205	Reset Australia		Protection around collection of data about children's geographical location	Safety by design measures for children such as default privacy settings	Requirements around children's precise geographic location appear much weaker than emerging global norms. Note gravity of the harms enabled by now-convicted abuser Alexander Jones' ongoing access to the Victorian DHSS' vulnerable children's database	We consider that this issue is best dealt with through changes to the Privacy Act 1988 (Cth) (currently under review).
206	Reset Australia		Measures are directed at protecting children who are account holders/actually use a service only. "	Safety by design measures for children such as default privacy settings	likely to be accessed" test is now more often used to decide if a service is in scope of any additional requirements for children	Noted.
207	Reset Australia		Scope of Code limited to Class 1A and Class1 B	General	These Codes would be better retitled 'Class 1A & 1B material Codes' to avoid any confusion around the level of comprehensive safety they offer. We appreciate that they are responding to requirements to develop guidelines around handling 1A & 1B materials, but believe this is a missed opportunity for a more comprehensive approach to safety. For example could contain measures around recommender systems and other lawful but harmful content such as material that encourages eating disorders. For children and young people, there is a widely used typology of online risks called the 4Cs.	The Codes are titled Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material). We think that the scope of the Codes is therefore clear.
208	Reset Australia		Child's right perspective needed	Framing	Children's broader rights in relation to the digital environment, including rights to privacy and participation, are notably absent from these Codes	In response to feedback, section 5.1(b)(iii) has been updated to refer to the need to have regard to the **best** interests of children.
209	Reset Australia		Evaluating	reporting/metric	Because they are built around demonstrating	The approach of the Codes was informed by the

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
			success of the Codes	s	minimal compliance steps, this framework is divorced from achieving any positive safety outcomes for children which could be more useful 'measures of success'.	eSafety Commissioner's Position Paper. The paper set out a flexible Outcomes and Objectives based approach in combination with minimal compliance measures based on services risk. The assessment of the success of the Codes will be determined by the eSafety Commissioner under the OSA. We note that while the industry initially proposed a more flexible principles-based approach, eSafety feedback over the development process has led to the Codes containing mostly minimum compliance measures. We consider that the key metric for assessing the effectiveness of the Codes should therefore be compliance with the Code measures.
210	Reset Australia		More Consultation needed	general	Too short ; the community had 32 days – 22 working days – to respond to 9 different Codes in total (including the Head Terms). Young people must be consulted on their views. young people may find that neither the content of these Codes nor the drafting process meets their expectation.	Non-profits that work with children have provided input into the consultation process both via the submissions process and roundtable conducted by the Steering Group. CA and DIGI also commissioned research from Resolve Strategy that provides insights into the views of 16- to 18-year-olds on the regulation of Class1 materials online. More extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
211	Scarlet Alliance	Objection to use of the Classification scheme: The conflation of BDSM activities with 'sexual violence' is a likely impact of the current draft Codes, as it has been throughout the history of the Classification Review Board's engagement with this content. This stands to significantly impact a range of stakeholders, including sex workers who produce BDSM, fetish or kink content for private or public sale. As the Classification Code remains under review, we do not believe that it is	Class 1 a and Class 1B to the extent they cover extreme crime and violence and crime and violence and impact in particular on sex workers	Definitions in heads of terms/ Position Paper	While we agree that depictions of non-consensual sexualised violence can raise legitimate content moderation issues that the Codes are charged with addressing, we do not believe that depictions of BDSM, kink and fetish content created by and for adults should be subject to restriction via the Codes. We also raise concern regarding any use of automated detection of this type of content, given the inability of current tools to consider available context in determining whether material depicts BDSM activity or non-consensual sexual violence.	As a result of the feedback receive, we have sought to clarify the definitions of Class 1A and 1B materials in light of concerns about the extent these categories may capture mainstream commercial pornography categories. Class 1C material is not in scope of these Codes and is not impacted by the guidance. See amendment in Head Terms.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter’s comment	Industry associations’ comment consideration
		appropriate for new legislation and resultant regulatory documents and actions to be aligned with it.				
212	Scarlet Alliance	Support for approach to proactive detection	Scope of proactive detection	DIS, RES and SMS Outcome 1	We believe that the Codes handle detection of CSAM in a way that is proportionate to its prevalence and impact, and do not support addition of any first-generation CSAM detection as required or optional measures in the Codes. The existing National Classification Scheme deals with depictions of individuals who ‘appear to be under 18’ in problematic ways that mis-identify adults with physical features that are outside of mainstream beauty standards (for example, smaller breasts) as falling outside of the acceptable classifiable ‘adult’ body type, with the implication that they are depictions of people under 18. Given the replication of the Scheme in the OSA, we have concern for the same type of content ‘flagging’ through any automated detection processes, and the scope for over capture and inaccurate capture.	Noted.
213	Scarlet Alliance	Changes suggested	Risk of de-platforming in enforcement	Outcome 1, especially SMS and DIS Codes and Search engine Code.	Throughout our many submissions to the development and implementation of the Online Safety Act and its various regulatory mechanisms, we have provided extensive information about the impact of deplatforming, content removal, de-listing, and other mechanisms used in the systemic digital marginalisation of sex workers. These submissions outline in depth the consequences of internet regulation that fails to consider the safety of sex workers, or that positions sex workers and the content we produce as anathemas to the safety of other end-users.	Noted. See response below regarding appeals.
214	Scarlet Alliance		Need for appeals mechanisms if users de-platformed	See Outcome 1 SE, SMS and DIS measures dealing with enforcement.	The draft Codes 1 and 4 (and likely many of the other Codes) make no provision for an impacted end-user to appeal an action taken by a Tier 1 or Tier 2 service. This means that end-users whose content has been wrongfully classified and removed, whether through automatic detection or user reporting, are unable to address this. The process should have the following	In response to feedback, the Head Terms have been amended to include a requirement to consider the issue of appeals when the Codes are reviewed, at which time there will be information available about participants' experience with the deployment of proactive detection technology and its impact on users of their services.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					features: ● Timeliness: the harm caused by account removals particularly is felt immediately, and may result in loss of income, loss of access to safety information. A protracted process will be ineffective in controlling such damage. ● Human monitoring: sex workers commonly report being stuck in endless loops with bots and/or circular reporting processes on social media platforms when we report a wrongfully-removed account or go through an account retrieval process. Note many social media platforms already proactively monitor sex worker accounts and content and/or ban known sex worker users from making new accounts. ● Context-informed: sex workers, like other social media users, should be able to live rich digital lives. Just because content was posted by someone who has been flagged as a sex worker doesn't mean that it's 'soliciting sex' or otherwise outside of the terms of use or community standards of a platform.	
215	Scarlet Alliance		General approach; risk of misalignment with other laws under review including privacy laws and the Classification scheme	See Position Paper.	We regard the development of the industry Codes for Class 1 material to be, as has been the case with all aspects of the Online Safety Act's passage and implementation and out of step with other reform processes in progress (including reviews of the Privacy Act and the National Classification Scheme). Government and regulators have repeatedly ignored calls from stakeholders to align online safety regulation with other aspects of content and internet regulation.	Noted.
216	Scarlet Alliance		General: approach to consultation	Need for more targeted engagement with sex industry	We regard the window of time provided for public consultation on the Codes to be insufficient, particularly for stakeholders like Scarlet Alliance with low capacity to respond.	Please note that more extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
217	Tech Against Terrorism	Neutral: specific recommendations: response is primarily focused on the Codes concerning social media services, relevant electronic providers,	Defining pro-terror material	HT definitions	The Codes should mandate that companies provide a definition of what it considers to be terrorism/a terrorist organisation and how it adjudicates on what constitutes "terrorist content". The Codes should provide as much of a framework to inform this definition as possible to uphold the rule of law. eSafety should provide a detailed framework for	The approach of the Codes was informed by the eSafety Commissioners Position Paper and feedback provided by eSafety during the Codes' development process. The categories of material in scope align with this input and the National Classification scheme. The guidance in Annexure A of the Head Terms provides guidance to industry within those constraints. Noted: the suggestion that guidance be given on the application of

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		designated internet services, hosting platforms and search engines, as we work with these types of companies more closely.			companies to define what they mean by terrorism / a terrorist organisation and help them with adjudicating on what constitutes terrorist content on their online services. This could include directing companies to refer to Australian law and international and national designation lists. In doing so, eSafety can ensure that the rule of law is upheld when companies choose what content is moderated and remove do help companies operationalise this standard.	the scheme online.
218	Tech Against Terrorism			Search engine Codes, Outcome 1, minimum compliance measures for terrorist operated websites..	Codes for search engines should include specific minimum compliance standards addressing the threat from terrorist operated websites (TOWs). Search engines should look to delist and, if possible, deprioritise these websites. These measures must be underpinned by the rule of law, namely the use of designation lists to determine if a website is in scope. Tech Against Terrorism also recommends that the Codes list the Terrorist Content Analytics Platform inclusion policy as best practice for tech companies in identifying websites in scope. When companies issue countermeasures against a verified TOW, it is vital they work with and deconflict with intelligence agencies, to ensure they do not harm any existing law enforcement operation. eSafety should therefore provide these companies with the appropriate support with liaising with national and international intelligence agencies.	The preamble to the Search engine Code explains the role of Search engines in the ecosystem and why measures in that Code cannot require search engines to proactively assess the legality pages they index. The Codes require search engines to delist links to class 1A materials, which can include terror-related material, pursuant to a legal removal request. The Code also require search engines to use best efforts to prevent autocomplete / predictive prompts for questions / phrases that would facilitate an Australian end-user's search for material for the purpose of inciting terrorism or extreme crime or violence;
219	Tech Against Terrorism			Outcome 1: SMS, RES and DIS Codes, minimum compliance measures, alternative options for content moderation.	The Codes for social media services, relevant electronic services and designated internet services should outline alternative options for content moderation beyond content removal, such as disengagement, educational or communication-based tactics, and community empowerment. To ensure companies do not rely on content removal, we recommend that the Codes explicitly outline other ways to make to harmful content harder to access. These can include hiding content, disengagement, educational or communication-based tactics, and community empowerment. This allows platforms to reduce accessibility and de-incentivise harmful content whilst limiting impact on users'	Noted this suggestion. The Codes are part of the Online Content Scheme under the OSA, which provides for the removal of this content online. The Codes are informed by the approach of the eSafety Commissioner in the Position Paper and feedback received by eSafety in the Code development process. They are therefore focused on measures aiming to prohibit and remove Class 1A and Class 1B materials.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					freedom of expression. We have a dedicated section on alternative content moderation solutions within our Knowledge Sharing Platform which we can share with eSafety upon request.	
220	Tech Against Terrorism		Scope of transparency reporting requirements for Class 1A and 1B materials.	Outcome 10,11	We commend the industry associations for including minimum compliance Codes for transparency around how services deal with Class 1A and 1B content, however in most cases the standard only applies to services deemed Tier 1. We recommend that this minimum standard is applied to all companies in scope, as this ensures that companies are accountable for how content is dealt with on their platforms. For guidance on transparency reporting, please refer to our transparency reporting guidelines.	Noted. In response to feedback the Codes have been amended to include additional transparency obligations on certain services concerning pro-terror and child sexual abuse materials. Please note that the eSafety Commissioner has a broad discretion under section 42 of the OSA to require companies to provide additional information about actions taken by companies to deal with pro-terror content in relation to investigation of complaints under the online content scheme and concerning Codes breaches. The Commissioner has additional broad powers under section 48, 49 and 59 of the OSA to require statements/reporting of information, and the Basic Online Safety Expectations instrument which also articulates expectations regarding how this material will be addressed. In this context we think the reporting approach is appropriate,
221	Tech Against Terrorism		Scope of services subject to Codes, need for proportionality in application to smaller businesses.	General	Tech Against Terrorism commends the industry bodies for disaggregating the Codes by platforms and services' different purposes and functions. As such, we believe that the Codes provide appropriately varied minimum compliance standards to account for these differences. We also recognise that the Codes for social media services and relevant electronic services consider the size of a platform's user base in the assessment of risk, however this does not provide a complete picture of the size of a given platform. There is no acknowledgment that companies' human and technical resources and capacity within its workforce would impact both its risk to users and its ability to fully comply with minimum compliance standards. For instance, a common minimum compliance standard in companies across all 8 sectors is that they must have inhouse or third-party trust and safety functions. Failure to do so could incur a financial penalty. This is problematic as the Codes do not consider whether support will be given to smaller companies with less resources to achieve this standard., eSafety and industry bodies should look to provide funding for less well-resourced companies to	Noted. We have considered this issue and consider that the market will likely respond to this need by providing outsourced trust and safety solutions for smaller companies.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					incorporate a trust and safety function into their business. This could be through dedicated government funding to allow these companies to hire dedicated staff or outsource third party risk management organisations.	
222	Tech Council of Australia	We welcome the industry Codes process as important in creating a new shared baseline across the tech sector. This action by the online industry needs to be part of a comprehensive suite of measures across multiple sectors to limit and respond to harmful content.				Noted.
223	Tech Council of Australia		Risk-based approached; general		We particularly welcome the proportionate, targeted and risk-based approach that has underpinned the development of the industry Codes, whereby the level of obligation is tailored to the type of service, the risk posed by the service and the type of content.	Noted.
224	Tech Council of Australia		Definition of a designated internet service	DIS, HT	We believe there is still a great deal of uncertainty around the types of services that fall within the scope of Designed Internet Services (DIS). The DIS code appears to capture a range of online services that would be considered very low-risk for publishing, accessing or spreading class 1A and class 1B material. For example, the definition of DIS appears to include services where there is limited (or no) evidence that they enable the provision of harmful material, including: Tech Council of Australia www.techcouncil.com.au - Websites and apps that have no (or limited) interface to allow end-users to upload content. This could include general business websites or apps offered by small businesses (such as cafes, restaurants and retail businesses) and general purpose websites operated by private individuals for lawful purposes. - Software-as-a-Service products and services that support business functions, such as accounting, HR, OH&S and project management. - Fintech services offered to businesses in areas like payment processing. - Business-to-consumer	The question of how a service is categorised under the Codes must be determined by services in accordance with the definitions in the OSA. eSafety feedback to industry during the drafting process was that these definitions should not be altered by these Codes including by providing exemptions for any service category. We note that this issue could be dealt with to some extent by legislative instruments providing exemptions under the OSA.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					software products and websites that provide services in areas like skills and training, health and wellbeing or property management. Excluding these low-risk services, or clarifying pat they fall within Tier 3 of the DIS code, would support the Government's goal of growing Australia's tech sector by reducing unnecessary regulatory costs that may be particularly challenging for start-ups and scaleups. Recommendation 1.1: We recommend providing additional or more detailed guidance within the industry Codes (or through separate guidance documents) to deem certain low risk services and activities as falling within Tier 3 of the DIS code. Recommendation 1.2: The Minister for Communications should consider providing further clarity on what constitutes a 'Designated Internet Service' by developing a legislative instrument under section 14(2) of the Online Safety Act to explicitly exempt low-risk services. This may include: - General-purpose business websites operated for the sole or primary purpose of lawful trade or commerce where there is no, or limited, interactive user interface. - Websites operated for lawful personal or domestic use by private individuals where there is no, or limited, interactive user interface - Business-to-business software operated solely for lawful professional purposes - Business-to-consumer software services operated solely for lawful professional purposes in low-risk areas (such as skills and training platforms).	
225	Tech Council of Australia		Feasibility of compliance measures	General, esp. measures for Outcome 1	Large social media providers have significant resources at their disposal and often have more sophisticated technological tools to prevent and detect harmful content, but this is not the case for smaller tech companies and start-ups. For example, smaller tech companies have significantly less scope to implement proactive AI monitoring technology or employ large teams of human moderators. These sorts of high-cost measures would also be inappropriate for low-risk services such as B2B software, where the software provider is technically and contractually unable to manage content on the customer environment. Recommendation 2.1: When finalising the	We acknowledge this concern and have sought to address this issue in 5.1(b)(iv) of the Head Terms. It is open to the Office of the eSafety Commissioner to further address this issue in their policy on Code enforcement.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					Codes, continue to ensure the compliance measures are designed in a way that is feasible and appropriate for industry to implement, taking account of the broad range of businesses that may be captured, interactions with privacy and surveillance laws, and issues around human rights, freedoms and community expectations	
226	Tech Council of Australia		Proactive detection; DIS	DIS	There is one further matter that requires clarification in the draft DIS code. The sixth compliance measure is expressly intended to relate to the 'Use of technological tools by Tier 1 designated internet services to detect and remove known Child Sexual Abuse Material (CSAM)' (as defined). However, the measures listed in part (c) of that item apply beyond known CSAM to broader concepts of 'CSEM and linked activity, pro-terror material or extreme crime and violence material'. This creates some uncertainty for industry over the scope of that measure. Recommendation 2.2: Clarify the intent of compliance measure 6(c) in the DIS code and whether it is deliberately intended to be broader than "known CSAM".	We have taken this feedback on board and clarified the scope of the measure in DIS is limited to known child sexual abuse material
227	Tech Council of Australia		Supporting effective implementation		Feedback received by the TCA indicates that there is a low level of awareness across the broader tech industry of the Codes and the requirements that they would impose, particularly under the DIS code. This demonstrates the need for a concerted and coordinated effort by the eSafety Commissioner, supported by industry, to lift awareness. It also highlights the need for an appropriate period to allow industry to understand the Codes and become compliant. Given many industry providers captured by the Codes have not previously been exposed to online safety regulation, there is also a need for additional tools that can improve their understanding of online safety concepts and the industry code obligations (including the risk assessment process) Recommendation 3.1: Implement an awareness campaign led by the eSafety Commissioner, with appropriate support from relevant industry associations, to ensure the broad range of tech companies likely to be	Noted. The need for additional outreach about the Codes to raise awareness about their scope and impact across the community is also consonant with the results of the Resolve Strategic research commissioned by the Steering Group on community views of Class 1 Content. We would support an awareness campaign by the eSafety Commissioner as proposed by this submission.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					captured by the Codes are aware of their possible obligations. Recommendation 3.2: Provide industry with a reasonable transition period of up to 12 months before the Codes take full effect (this is particularly important for the DIS code, which is significantly broader in scope and where there is low industry awareness). Recommendation 3.3: Develop additional tools (such as an online tool or additional tailored guidance) that could support industry compliance with the Codes, including the risk assessment process.	
228	Tech Council of Australia		Compliance and enforcement	General	We believe there is a need for clearer guidance around the escalating compliance and enforcement approach that will be applied to the industry Codes. For example, it is unclear what consequences may apply in circumstances where an industry participant has self-assessed that their service is low or moderate risk, but where the regulator has a different perspective. Similarly, it is unclear what level of expectation is required by the regulator for industry to demonstrate compliance with the risk-assessment process and other elements of the draft industry code. Recommendation 4: The eSafety Commissioner develop clear guidance (designed in consultation with industry) on the escalating compliance and enforcement approach that would apply to the industry Codes and include this in an updated compliance and enforcement policy.	Noted. We consider that these issues are best addressed by the eSafety Commissioner, for example, via published policies on enforcement of the Codes.
229	UNICEF Australia	Measured: Codes should lift their ambition	Consultation	General	Extend and expand the public consultation on the Draft Industry Codes to ensure they better meet community expectations, with particular efforts made to genuinely consult with children, young people, organisations that work with them, and Children's Commissioners and Guardians.	Non-profits that work with children have provided input into the consultation process both via the submissions process and the roundtable of stakeholders conducted by the Steering Group More extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA.
230	UNICEF Australia		Scope of Codes	General	Broaden scope of the Draft Industry Codes to provide greater protection for children and young people in line with a more holistic understanding of the harms they face online. Some examples of specific areas where this is needed include the requirements for reporting CSEM under the Social Media Services Code,	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) and the OSA. As a result, the scope of the Codes primarily concern Class 1A and 1B Materials and are focused on removal of this material for all online users, acknowledging that this material does pose

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
					the age for defaulting children's accounts to private, and additional duties for services which permit children to hold an account as opposed to services children actually use. Broadly though, the Codes would be improved by taking a more holistic view of the harms and risks that children face online. This could be done in line with the widely used 4Cs typology – covering not just the risk from exposure to Content (as they currently do to an extent), but also from Contact with stranger adults, from their own harmful Conduct, and from Commercial risk	specific risks to children. The Codes are therefore aligned with the Position Paper, the OSA and the National Classification Scheme rather than other approaches to the protection of children.
231	UNICEF Australia		Approach of Codes	General	Take a rights-based approach in the Draft Industry Codes which considers children's best interests and evolving capacities, to ensure the protection and promotion of all their rights.	In response to feedback, we have amended the Head Terms which requires participants to have regard to the **best** interest of children.
232	Uniting Church of Australia Synod of Victoria	Neutral, with some concerns and recommendations	Approach to classification of materials	Head Terms section 3(g)	As drafted, the section allows an industry participant to incorrectly classify material and not have to take any corrective action because of the incorrect classification. The industry participant should be required to accept a categorisation of material by the eSafety Commissioner and be required to adjust its treatment of material accordingly. Categorisation of material by industry participants should not be given equal weighting and validity as those by the eSafety Commissioner or relevant law enforcement agencies	section 3(g) acknowledges the inherent challenge of applying concepts in the National Classification Scheme to all categories of online materials at scale. We note that the eSafety Commissioner has not published any guidance about how content should be classified under the OSA. Should such guidance be published this may assist in addressing this issue.
233	Uniting Church of Australia Synod of Victoria		Complaint mechanism requirements	section 4, Objective 2, Outcome 8 HT	There should be a requirement that complaint mechanisms are easy to access and use.	The complaints mechanisms required by the Codes are set out on a case-by-case basis in the schedules for each service/product subject to the Codes. These measures require mechanisms to be accessible.
234	Uniting Church of Australia Synod of Victoria		Human rights considerations	HT section 5.1	section 5.1(b)(iii) the wording should reflect the UN Convention on the Rights of the Child and the word 'best' added, to read: *(iii) 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 that in response to feedback, the Head Terms 5.1(b)(iii) have been updated to refer to the need to have regard to the **best** interests of children.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
235	Uniting Church of Australia Synod of Victoria		Complaint handling	section 7.4 H T	section 7.4, an industry participant should be required to have a staff member acknowledge receipt of any complaint within 24 hours, so the complainant can have confidence that the complaint is being taken seriously. It should not be sufficient that there is an automated response alone to the receipt of a complaint.	The Codes contain various measures that require information to be provided to end-users about complaint handling that are appropriate to the type of complaints they are required to manage under the Codes.
236	Uniting Church of Australia Synod of Victoria		Risk assessment	SMS schedule 1 section 4b)	Under section 4(b), one of the factors the social media service provider should be required to take into account is their own knowledge or public evidence that class 1A and 1B material are already being accessed, distributed or stored on their platform.	We considered and rejected this as this was not a risk factor identified in the eSafety Commissioner position paper and could act as a disincentive to services to improve their existing reporting and detection mechanisms which would be contrary to the objectives of the Codes.
237	Uniting Church of Australia Synod of Victoria		Reporting CSEM and pro-terror material	Compliance measure 1 SMS	Under section 6, compliance measure 1, the social media service should be required to report the detection of CSEM and/or pro-terror materials to an appropriate entity within 24 hours unless it is certain the material has already been reported or, in the case or pro-terror material, is historical and no longer relevant as a threat. The social media service should not be in a position not to report the presence of CSEM on its platform because it has assessed that the material is not an immediate threat to the life or physical health or safety of an Australian adult or child. The Synod does not believe social media services have the skills and powers to make such an assessment	These provisions were drafted to take into account the need for services to comply with the Privacy Act 1988 (Cth) which provides limited circumstances in which personal information can be provided to law enforcement. In response to feedback, the Codes have been amended to make clear that these requirements supplement existing reporting obligations in State and Territory legislation.
238	Uniting Church of Australia Synod of Victoria		Removal of accounts for breach of Ts and Cs	Compliance measure 3 SMS	Under compliance measure 3, the social media service should not terminate an end-user's account where a law enforcement agency has asked for the account not to be terminated. Further, the account should not be terminated if doing so would mean the end-user would not be able to be identified, because the social media service allows users to use false identities to create accounts	We consider that the drafting of measure 3 of Schedule 1 addresses the concern about the need for SMS providers to retain accounts where directed to do so by law enforcement.
239	Uniting Church of Australia Synod of Victoria		Provision of information to users about eSafety	Compliance measure 21 SMS	compliance measure 21, the information about how to make a complaint to eSafety should be easily accessible and should not require a person to hold an account with the social media provider.	Compliance measure 21 of Schedule 1 requires information to be accessible. Since many accounts on SMS services and some SMS services are not public, the requirement is limited to Australian end-users.
240	Uniting Church of Australia Synod of		Complaint mechanisms	compliance measures 23,	compliance measures 23, 24 and 25, a person should be able to access the complaint	See above.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
	Victoria		should be accessible to non-account holders	24 and 25, SMS	mechanism without holding an account on the social media platform. The Canadian Centre for Child Protection (CCCP) reported on the experience of survivors of child sexual abuse in trying to get images and videos of their abuse removed. They found there was an inability to report publicly visible CSEM content without first creating (or logging onto) an account on the platform. The requirement was found to be a barrier to some reporting of CSEM material.	
241	Uniting Church of Australia Synod of Victoria		Complaint handling; point of contact	compliance measure 26, SMS	Under compliance measure 26, a staff member of the social media service should inform a complainant that their complaint has been received and provide a point of contact for the complainant to follow up on the complaint	Please see guidance in this measure about how providers should implement this measure including indicative time frames for complaints handling.
242	Uniting Church of Australia Synod of Victoria		RES Schedule 2	section 8, compliance measure 8 RES	Under section 8, compliance measure 2, the electronic service should be required to report the detection of CSEM and/or pro-terror materials to an appropriate entity within 24 hours unless it is certain the material has already been reported or, in the case or pro-terror material, is historical and no longer relevant as a threat. The electronic service should not be in a position not to report the presence of CSEM on its platform because it has assessed that the material is not an immediate threat to the life or physical health or safety of an Australian adult or child. The Synod does not believe electronic services have the skills and powers to make such an assessment.	These provisions were drafted to take into account the need for services to comply with the Privacy Act 1988 (Cth) which provides limited circumstances in which personal information can be provided to law enforcement.
243	Yourtown	Supports the development of the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) (the Codes) and the inclusion of Safety by Design principles. We also support the enhancement of online protections to reduce access and exposure to	Consultation to cover telehelp providers. Concerned creates risk for victims seeking help	General	The Codes should not be finalised without direct consultation with digital service providers in the community, and children and young people directly impacted by the proposed Codes, to ensure critical services are not negatively or inadvertently impacted. Consultation should be supported by accessible and easy to understand versions and supporting information.	Non-profits that work with children have provided input into the consultation process both via the submissions process and roundtable conducted by the Steering Group. More extensive consultation was not possible due to the timetable for registration set by the eSafety Commissioner under the OSA. In response to feedback, we have clarified in the DIS that providers of support services will be classified as Tier 3 and therefore moist compliance measures for these services are optional.

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		online material promoting child sexual exploitation and abuse, terrorism, crime and violence, and drug-related content. Specific issue with how Codes may impact Telesupport providers				
244	Yourtown		Drafting approach	General	Draft Codes and supporting documentation is the highly technical and in parts, obscure nature that they have been presented in,hampering full engagement with the proposed Codes	The approach to the Codes was informed by the eSafety Commissioner (both the Position Paper and feedback provided by eSafety through the drafting process) and by the OSA. As a result, the scope of the Codes is primarily on Class 1 Materials. Note this resulted in the industry using technical concepts in the OSA such as definitions of different categories of services regulated by the Codes and adopting a Code structure based on the eSafety Commissioner's Position Paper.
245	Yourtown		Scope/exclusions	General	Online counselling and health services including helplines, or professional counselling services, such as Kids Helpline and Parentline, should be expressly excluded from the Codes where storage, descriptions, or expressions of Class 1A or Class 1B material are used for the purpose of seeking, or receiving counselling, or support.	The question of how a service is categorised under the Codes must be determined by services in accordance with the definitions in the OSA. eSafety feedback to industry during the drafting process was that these definitions should not be altered by these Codes including by providing exemptions for any service category. We note that exemptions from some service categories can be made by legislative instrument under the OSA. See above as to how we responded to the concerns about how the Codes impact support services in the DIS Code (Schedule 3).
246	Yourtown		Age assurance	General	The Codes should exclude Helplines, and online support, or counselling services from requirements to obtain a user to register with a phone number, email address or other identifier to ensure: • anonymity is available for therapeutic purposes and • a child is not endangered or restricted from seeking help by virtue of having to provide details for registration, and • a child is not restricted from having access to electronic services (such as a phone or internet) in order to seek counselling, support services, or help in a crisis.	See above.
247	Zoom Video Communications	Supportive We appreciate that eight separate Codes have	Risk assessment approach	RES	We welcome the RES Code's proposal to require concerned services to undertake a risk assessment, based on reasonable criteria that	Noted. In response to feedback Schedule 2 has been amended to specify that enterprise services are subject to limited measures concerning their agreements with

#	Submitter (in alphabetical order)	General tenor (e.g., endorsement / rejection of Codes)	Topic / Issue	Code section/MCM if applicable (clearly identify Code first)	Submitter's comment	Industry associations' comment consideration
		been developed for various industry segments, including Social Media Services, App Distribution Services, Internet Search Engine Services, and Relevant Electronic Services (RES). We note in particular the eSafety Office's commitment to measures, such as the RES Code, that "have been designed to take into account the differences between the purpose, functionality and user-base of each type of service; and the need for flexibility in the implementation." We also note from the standpoint of a global service provider and an organisation that seeks to design a frictionless customer experience across our product suite, we prefer regulatory approaches that distinguish based on product features rather than based on the target customer segment.			includes functionality (potential for virality), intended audience, and scale. This would incentivise all stakeholders to take a responsible approach towards tackling CSAM and pro-terror material, and identify any blind spots in their content moderation practice. We would also welcome further guidance on the approach to calculating "active Australian end-users" of a service in the risk assessment framework in Clause 6(c) of the RES Code. In particular we would support a clarification that end-users associated with enterprise accounts are excluded from these calculations.	enterprises and the provision of a statement of compliance with this measure to eSafety on request,
248	Zoom Video Communications		Proactive detection measures for RES optional	Outcome 1	We recommend that proactive detection with regards to "first-generation CSAM" remain optional and voluntary for now	Noted.