IGEA

interactive games & entertainment association

Submission to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Response to Statutory Review of the Online Safety Act 2021

July 2024

IGEA acknowledges and pays respect to the past and present Traditional Custodians and Elders of this land and the continuation of cultural, spiritual, and educational practices of Aboriginal and Torres Strait Islander peoples. We would like to extend our acknowledgments to the indigenous people from countries overseas and recognise their strength, wisdom, and creativity.

Contents

1. Introduction

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the Department of Infrastructure, Transport, Regional Development, Communications & the Arts (Department), on the statutory review of the *Online Safety Act 2021* (Cth) (OSA Review), led by Ms Delia Rickard PSM.

Since the OSA commenced in 2021, there have been many changes in the online safety regulatory landscape, both domestically and internationally. This has included an increasing expansion of various regulations and regulatory powers being made available to the online safety regulator in Australia (eSafety). However, this has also created a complex and, at times, confusing regulatory framework, presenting challenges for eSafety and industry stakeholders to understand and agree on suitable measures to reasonably meet their obligations.

Further, while there have been regulatory changes over this time, regulatory instruments in online safety are still in their infancy. This short period suggests that there has not been sufficient time allocated for regulatory instruments to be implemented.

We would, therefore, be concerned if new obligations were introduced under the OSA Review. The OSA Review offers a timely opportunity to seriously review and simplify an unnecessarily complex regime, promote online safety as everyone's responsibility, and build effective and genuine trusted collaboration between affected stakeholders rather than create unnecessary division.

Nevertheless, despite these regulatory challenges, the video game industry has long been at the forefront of ensuring online player safety, established well before the existence of the OSA and eSafety. It is not only for ethical reasons, but a business imperative for the industry, in a highly competitive global market. As part of providing a safe online space for users, this has led to well-established global industry best practices, with the industry effectively implementing measures to safeguard all users, especially younger players, for decades. And like the film industry, the video game industry follows strict age-appropriate standards around the world, including Australia. Accordingly, video game services have pioneered parental control capabilities to address child access to age-inappropriate games, amongst other measures.

It also important to recognise that the primary purpose of video games is in its name – to play video games and entertainment, offering immersive experiences, adventure, activities and storytelling. Indeed, some games provide ways to communicate with other players, although the focus tends to be on the game itself and interactive activities. Where user interactions are allowed, they will generally be limited (for example, to enable real-time gameplay coordination), often brief, and governed by parental controls or the age appropriateness of the game.[1] This is in contrast to socialising in a manner synonymous with other online platforms where they may be primarily intended for user communication. What this means is that games include tools for users to manage in-game chats, including the ability to disable or restrict communications; and once logged out of a game, these chats are deleted. This is not to discount the value of socialising, which occurs through actual gameplay, rather than relying on communication features. To this end, online games, especially with multiplayer and in-game communication features are vastly different from other online services. Moreover, due to the industry's longstanding commitment to combating illegal and broadly unacceptable content within their services, built with inherent safety-by-design considerations with respect to in-game communications, we believe our industry has a lower risk of hosting illegal and harmful content.

[1] For example, see: https://www.comeback.world/2023/05/12/difference-between-social-media-video-games/.

1.1 About IGEA

IGEA is the industry association representing and advocating for the video game industry in Australia, including the developers, publishers, and distributors of video games, as well as the makers of the most popular game platforms, consoles and devices. IGEA has over a hundred members, from emerging independent studios to some of the largest technology companies in the world.

Amongst other things, IGEA also organises the annual Games Connect Asia Pacific (GCAP) conference for Australian game developers and the Australian Game Developer Awards (AGDAs) that celebrate the best Australian-made games each year.

Video games are a beloved Australian activity and significantly benefit Australian game players, the wider community, and the economy. Video game developers and publishers are the innovators, creators and business leaders reimagining entertainment and transforming how we learn and play. More than four out of five Australians play games, mainly for enjoyment and relaxation, and games are increasingly being used for serious and educational purposes, including by governments. Video games provide a digital outlet for Australian art, culture, stories and voices, and Australian-made video games are among Australia's most successful and valuable cultural exports. Our medium also brings kids into STEM and helps them build technology skills that will feed Australia's workforce needs.

In supporting local content, the video game industry is a major contributor to the Australian digital economy. According to our data, video games are worth around $4.4 billion annually in Australia,[2] while Australian-made games brought in $345.5 million in largely export revenue last year.[3] Moreover, because the video game sector uniquely sits at the intersection of entertainment, the arts and technology, video game companies hire a wide range of artistic, technical and professional roles and are thus a wellspring of high-quality sustainable careers, and are an engine for growth in the Australian national economy. Indeed, Australian game developers are internationally renowned, and ours has the potential to be one of Australia's most important future growth industries and an integral component of the Government's vision for Australia to be a top 20 digital economy and society by 2030.

1.2 Video game industry's serious approach to online safety

For the video game industry, creating safe and welcoming online spaces for players is essential. It is also a business imperative, in a highly competitive global market, with players having access to numerous free alternatives. Games with an unsafe reputation will quickly lose their audience.

This is why the video game industry has been at the forefront of ensuring online player safety. This is demonstrated by its strong commitment to consumer protection through a long history of self-regulatory solutions. With well-established practices, the industry has effectively implemented measures to safeguard all users, especially younger players, for decades.

The industry adheres to strict domestic and international data and consumer protection laws, supplemented with an age-appropriate video game content labelling scheme, along with other measures. The industry also leads in empowering players and parents with easy-to-use tools, including for managing playtime, spending, online privacy, online gameplay, and access to age-

[2] '2023 Australian video game consumer sales continue stable growth' (IGEA Media Release, 3 June 2024), https://igea.net/2024/06/2023-avgcs/.

[3] 'Aussie game developers pull in $345.5 million for local economy' (IGEA Media Release, 18 December 2023), https://igea.net/2023/12/2023-agds/.

appropriate games. The industry's serious commitment and responsibility to these protections are built around global industry best practices.

It is also important to highlight the unique dynamics of the video game industry, which differs significantly from other online services. Similar to the film industry, the video game industry follows strict age-appropriate standards, and user interactions are often limited and subject to parental controls or age restrictions. The video game industry takes a further greater step in protecting player privacy, by collecting and storing gameplay data anonymously, without directly linking it to individual players' identities. These measures complement the industry's compliance with domestic and international classification and privacy laws, including in Australia.

In this regard, we wanted to acknowledge IGEA's longstanding, constructive working relationship with the government for over two decades on video game classification. We have collaborated with the Classification Board and Classification Branch, first in the Attorney-General's Department and then later when it was transferred to the Department of Communications & the Arts (later to evolve and become this Department). We have worked closely with the Board and Branch to ensure industry compliance with classification regulation, to support the effective and efficient operation of the Scheme and to advocate for appropriate legal and policy reforms. It is important to recognise the invaluable knowledge, expertise and experience, as well as the relationships and trust which has been developed over this extensive period between the key government agencies and stakeholders in the industry and the wider community. Notwithstanding this, we continue to advocate for the importance of a robust classification system, with the current Stage 1 reforms being implemented and Stage 2 under development.

Additionally in Australia, over the last several years since the inception of the Online Safety Act in 2021, IGEA and its members have been heavily engaged in and contributed to the development of the various industry online safety codes that were registered by eSafety (including for App Distribution Services and Equipment Codes), as well as the Draft Relevant Electronic Services (RES) Code that was declined for registration by eSafety (and subsequent Draft RES Standard that has only recently been published by eSafety during the OSA Review consultation period).

1.3 Good public policy design and best practice regulation

As a matter of good public policy design and best practice regulation, any regulatory obligation and measure set by the online safety framework under the OSA (including via subordinate legislation) should be well-defined, reasonable and clearly scoped. It should also provide sufficient flexibility that is future-proofed for evolving technologies and be supplemented by relevant industry guidance to enable sufficient regulatory clarity and certainty.

It is also critical to ensure that the online safety framework avoids unnecessary regulatory duplication and conflict with both existing and future regulations, including the Phase 1 industry online safety standards and codes for Class 1 material, Basic Online Safety Expectations (BOSE) Determination, the other provisions under the OSA, Phase 2 industry online safety codes for Class 2 material, and current reforms to the National Classification Scheme (NCS). Minimising such duplication not only ensures administrative efficiency, such as reducing associated regulatory costs, regulatory burden and complexity, but also mitigates inadvertent inconsistencies between the regulatory instruments. This is also important for ensuring improved safety outcomes for Australians rather than just focusing on regulatory processes.

In our recent submissions to eSafety on the Draft RES Standard and the Department on the Draft BOSE Amendment Determination,[4] we recommended the significant benefit of providing further clarity through relevant guidance and other explanatory material to support the Draft RES Standard (eSafety intentionally omitted such guidance from its consultation stage) and amended BOSE Determination. There would be value in providing guidance on how the Determination, codes, standards and any other regulatory instruments (including the NCS) could work together in practice, especially when each instrument is arguably intended to set the industry benchmark for ultimately promoting online safety. For example, there appears to be significant duplication in the industry codes and standards and the BOSE Determination.

While it may be the policy intent for there to be sufficient clarity and collaboration in promoting online safety, it is also important to ensure that this is reflected in practice such as how certain regulatory instruments are enforced and information gathered. For instance, the BOSE Determination was originally designed with the intention of providing a basic set of expectations for service providers to broadly demonstrate online safety practices for service providers. However, in practice, it has often been weaponised as a naming and shaming tool, trial by media and politicisation. There is also a risk of information shared by service providers being improperly handled without sufficient safeguards. As a matter of procedural fairness, impartiality and promoting genuine collaboration, the OSA Review can ensure that these regulatory deficiencies do not become the norm, raising the bar to enable good policy design and best regulatory practice.

Internationally, the government must consider the changed global regulatory landscape since the OSA was first published. To align with the broader aim of making Australia an attractive destination for the video game industry to invest in, international regulatory coherence is crucial. More importantly, international alignment ensures a better user experience in a global online environment. Given the small Australian market, it is important that Australia gives proper consideration to overseas approaches, including lessons learnt, rather than trying to lead in areas or reinventing the wheel in regulation. For example, it would be more prudent to refer to overseas requirements such as the EU Digital Services Act (DSA) and UK Online Safety Act (OSA), and how that is being implemented and regulated in practice. Nevertheless, it is important to acknowledge that these requirements are relatively new, and may have teething issues that need to be resolved through lessons learnt.

In the absence of adequate clarification on how these regulatory instruments work together, domestically and internationally, there is a risk of creating suboptimal and unintended outcomes that do not achieve the intended goal of enhancing user safety. It should be in everyone's interest that this does not occur, and the Government has a leading role in ensuring that as much regulatory clarity is provided to help service providers meet their online safety regulatory obligations properly, rather than automatically resorting to the threat of regulatory "sticks" for inadequate compliance in the first instance.

Further, it would be prudent to take pause and reflect on the multiple regulatory instruments in place. Currently, this includes the draft online safety standards for Class 1A and 1B material having

[4] IGEA submission to Draft Relevant Electronic Services Standard (January 2024), https://igea.net/2024/02/igea-submission-to-draft-relevant-electronic-services-standard/; IGEA submission to Draft Online Safety (Basic Online Safety Expectations) Amendment Determination 2023 (February 2024), https://igea.net/2024/02/igea-submission-to-draft-online-safety-basic-online-safety-expectations-amendment-determination-2023/.

only just been registered by eSafety,[5] BOSE Amendment Determination having just been approved,[6] the Stage 2 reforms of the NCS underway,[7] recently announced age assurance trial,[8] as well as other interrelated regulatory announcements by the government (such as doxxing[9] and deepfakes[10]). It should therefore come as no surprise that these are presenting a dynamically unstable and uncertain regulatory environment for affected service providers to address, let alone consideration in the OSA Review. The timing of these concurrent activities, while the OSA Review is underway, highlights a symbolic need for a more holistic and coordinated approach to online safety. These multiple overlapping reforms demonstrate that it has not been reflected in practice, inadvertently leading to a crisscrossed patchwork of fragmented approaches towards online safety, despite theoretically operating under the same overarching online safety framework under the OSA.

Acknowledging that the Australian online safety framework is a complex regime, this makes it difficult for service providers to meet their obligations. Government should be ensuring that service providers properly meet their obligations, rather than waiting for them to fail and threatening penalties for non-compliance. There is a proactive collaboration element that is missing from this framework. This has led to stakeholder confusion and frustration at times. It would be inappropriate and unhelpful to characterise this issue as simply big tech companies versus the community. We need greater leadership from all sides to avoid politicising this subject and focus on meeting the OSA objectives, which can be achieved if everyone works together in good faith.

1.4 Overview of submission

Overall, we support the intention behind the online safety framework under the OSA. As stated above, the video game industry takes consumer online protection extremely seriously built around global industry best practices. We have also worked closely with government, eSafety and other stakeholders to develop industry online safety codes (e.g. Equipment and App Distribution Services Codes) over the last several years, and exploring ways to promote Safey-By-Design.

We strongly consider it too premature to introduce new obligations to the regime, given the relative infancy of the various regulatory instruments. Nevertheless, the OSA Review presents a timely opportunity to improve upon the operation of the legislation and associated regulatory instruments. This includes streamlining, simplifying and bringing order and stability to an unnecessarily complex and over-populated landscape and crisscrossing patchwork of fragmented regulations and reforms. This also reflects a changing regulatory environment both domestically and internationally.

Our submission therefore focuses on reforms that would enable best practice regulation and good policy design.

[5] eSafety, 'Industry standards to tackle worst-of-the-worst online content a key step closer' (Media Release, 21 June 2024), https://www.esafety.gov.au/newsroom/media-releases/industry-standards-to-tackle-worst-of-the-worst-online-content-a-key-step-closer.

[6] Minister Michelle Rowland, 'Online safety expectations to boost transparency and accountability for digital platforms' (Media Release, 30 May 2024), https://minister.infrastructure.gov.au/rowland/media-release/online-safety-expectations-boost-transparency-and-accountability-digital-platforms.

[7] Minister Michelle Rowland, 'Modernising Australia's National Classification Scheme' (Media Release, 4 April 2024), https://minister.infrastructure.gov.au/rowland/media-release/modernising-australias-national-classification-scheme.

[8] Australian Government, 'Tackling online harms' (Joint Media Release, 1 May 2024), https://minister.infrastructure.gov.au/rowland/media-release/tackling-online-harms.

[9] Attorney-General Mark Dreyfus, 'National consultation on laws to combat doxing now open' (Media Release, 11 March 2024), https://ministers.ag.gov.au/media-centre/national-consultation-laws-combat-doxxing-now-open-11-03-2024.

[10] Attorney-General Mark Dreyfus, 'New criminal laws to combat sexually explicit deepfakes' (Media Release, 5 June 2024), https://ministers.ag.gov.au/media-centre/new-criminal-laws-combat-sexually-explicit-deepfakes-05-06-2024.

Below is a summary of our recommendations in response to the Department's issues paper questions.

Key themes raised in issues paper	**IGEA's recommendations**
Australia's regulatory approach to online services, systems and processes	• Interaction between Online Safety Act (OSA) and National Classification Scheme (NCS): To provide greater clarity, it should be clearly stated in the OSA (and subordinate instruments) that it only addresses illegal and unclassifiable online content (such as the majority of user-generated content), while the NCS (along with the Restricted Access System Declaration) deals with classified and classifiable content (which is particularly applicable to video games like the film industry). • Basic Online Safety Expectations (BOSE): o The BOSE Determination currently captures a huge range of service types given all Social Media Services (SMS), RES and Designated Internet Services (DIS) are considered to be in scope. The Determination should allow for greater flexibility for the various services captured by the Determination to meet the expectations in ways that make sense for that service type, giving adequate consideration to the nature of potential harms on the service. o The BOSE Determination process should be simplified and streamlined with other concurrent regulatory instruments including industry online safety codes and standards. Government should explore ways to streamline such requirements to avoid unnecessary regulatory duplication and conflicts. • Phase 2 industry online safety codes: o Given that there are so many moving parts in online safety reform, this has made it difficult to keep up with the various factors influencing policy considerations such as age assurance. Greater attention should be given to simplifying and streamlining each area so service providers are clear on the parameters and expectations. o For the Phase 2 industry online safety codes development process to be effective, it is important that there be sufficient time allocated to the process, flexibility for consideration of relevant issues, clearly scoped and avoid overlapping requirements between the Phase 2 codes and other regulatory instruments (e.g. NCS), and mutual transparency between the regulator and industry stakeholders to ensure a more productive process. • Terms of use: The service provider should be given the flexibility in how it enforces breaches of terms of use. The video game industry has long-established clear terms of service and removes any content or interactions that violate these terms, including illegal content, complemented by appropriate penalties and other preventive and reactive industry safeguards. • Risk-based approach: Generally, a proportionate approach for regulatory obligations should be based on the level of risk of the service and its users, as opposed to arbitrary definitions and thresholds. However, proper consideration of a risk assessment should be to evaluate the real risk of illegal content appearing on the service, taking into account current mitigation measures. Further, when evaluating the risk level of an identified potential harm, it should not be based merely on one isolated incident or a technical possibility of an incident occurring. Instead, it should take into account relevant factors such as the frequency or probability of incidents, the degree of harm, the proportion of verified complaints related to the harm, and the mitigation measures in place.

Key themes raised in issues paper	**IGEA's recommendations**
Protecting those who have experienced or encountered online harms	• Restriction to children's access: o We caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing age assurance technologies. We would be keen to understand whether these concerns are addressed from the age assurance trial. o Like the film industry, the video game industry has long spearheaded parental control capabilities in video game services to address child access to age-inappropriate games, based on global industry best practice. However, the video game industry takes a further greater step in protecting player privacy by collecting and storing gameplay data anonymously, without directly linking it to individual players' identities. Ensuring children's safety online hinges on parental and caregiver consent. Our industry has led the way in creating effective parental control tools across different devices and platforms. Parents and carers are therefore empowered to use technological and/or non-technological means to help manage their children's viewing and playing experiences, as opposed to deferring to the government. This nuance needs to be better appreciated in how online safety is approached for video games by government. • Bystanders' reporting: In principle, there could be merit in considering bystanders who may not be directly affected to report to eSafety regarding illegal or seriously harmful material. Consideration should be given to existing laws in place that already offer similar arrangements. There should be proper safeguards to ensure that bystanders are properly protected (such as privacy) and legitimate reports are only accepted (avoid disingenuous complaints). • eSafety's current powers: o eSafety does have sufficient powers that are reasonably limited by jurisdictional boundaries and what can be reasonably implemented by the service provider. It is also important that the technically feasible limits of service providers are reflected in practice (such as when making and interpreting subordinate legislation). o Should the Government wish to address the jurisdictional limits of the online safety framework, then it would be better served through international regulatory coordination such as the Global Online Safety Regulators Network. • Education and research: eSafety has a powerful educational role to raise public awareness about online safety, and developing research on trends such as types of online safety issues and solutions. Such research can be better informed through improved collaboration with industry and experts to ensure rigorous and robust representation. This would be the most effective way to proactively empower online safety with the community. We have been exploring collaboration opportunities with eSafety with respect to the video game sector.
Penalties, and investigation and information gathering powers	• Regulatory powers: o The OSA does not need to create more regulatory powers, given the plethora of regulatory instruments in place, while other new reforms are also underway or planned. o There should be a focus on simplifying the overall online safety framework. This can then flow down to how regulatory instruments are implemented in practice including development, enforcement and interpretation. o There should also be emphasis on developing harm-agnostic frameworks that are able to adapt to new and emerging threats, some of which we may not yet even

Key themes raised in issues paper	IGEA's recommendations
	conceptualise. This removes the need for constant updates to the Act and its secondary instruments which is time consuming for the government, regulator and all stakeholders. o When service providers are required to share information with eSafety, there should be appropriate safeguards in how the regulator manages such information in accordance with due process, transparency, confidentiality, and privacy. For instance, there needs to be protections in place to safeguard commercially sensitive industry data. Also, service providers should not be compelled to provide data to third parties via the regulator (such as researchers) – this ensures that the use of such data is properly managed and understood by the information provider and receiver. The regulator should also make clear the reasons why it is seeking this information and the manner in which that information will be treated. • <u>Sanctions:</u> The OSA should not grant eSafety the power to impose sanctions. Sanctions are a foreign policy instrument subject to international law and conventions. The decision to sanction must remain in Commonwealth agencies with the appropriate capabilities and expertise.
International approaches to address online harms	• <u>International regulatory coherence:</u> Given the global nature of the video game industry, it would be prudent to refer to overseas approaches such as the EU Digital Services Act (DSA) and UK Online Safety Act (OSA), and how that is being implemented and regulated in practice. Nevertheless, it is important to acknowledge that these requirements are relatively new, and may have teething issues that need to be resolved through lessons learnt. The Global Online Safety Regulators Network, including eSafety, could be an avenue to have regard to such matters. However, it would be beneficial for the government to consider industry input into such discussions, especially those subject to these overseas requirements. • <u>Transparency in regulatory decision-making:</u> o Given that eSafety regulates content, having regard to classified and classifiable content under the NCS, this requires appropriate expertise and capability to review content. The regulator's personnel charged with reviewing content should be properly trained including understanding treatment and context. o A proportionate mechanism should be in place to enable procedural fairness and review of decisions by eSafety. We therefore recommend a new review body be established to review eSafety's decisions (in addition to current judicial and merits review mechanisms), should a service provider challenge their decisions. This should be specified in legislation to ensure that there are proportionate checks-and-balances in the regulatory decision-making process to provide more public and industry confidence in the online safety regime. • <u>Online Safety Advisory Panel:</u> If the process is well-designed, consideration could be given to establishing an Online Safety Advisory Panel, comprising of experts and industry representatives (similar to the Classification Advisory Panel currently being considered in the context of the Stage 2 NCS reforms). It would not be a decision-making body, but would advise the government on online safety trends, informed by an evidence-based and community considered approach. It would be independent of the regulator, with support resources provided by ACMA. Such a body should include representation from civil society organisations or human rights groups to ensure due process considerations are factored in.

Key themes raised in issues paper	**IGEA's recommendations**
Regulating the online environment, technology and environmental changes	• Targeted groups: Further information is needed to understand how groups would be defined and targeted by eSafety. Consideration will need to be given to the context and treatment of the content, and governance around who is authorised to determine the targeted groups. • Privacy and security considerations: As a general rule of good public policy design and best regulatory practice, specific regulatory measures and obligations intended to promote online safety should not be introduced if it infringes upon privacy and security. • Technology neutrality: As a general rule of good public policy design and best regulatory practice, regulatory measures and obligations proposed to promote online safety should be technology neutral, as well as technically feasible. • Cost recovery: o As a matter of good public policy design and best regulatory practice, allowing for eSafety to cost recover for its activities from online service providers raises significant concerns with respect to barrier to access regulatory services, and proportionality and accountability issues, which could lead to unintended and perverse consequences. o Consideration should be given to public funding of bodies such as industry associations to develop industry online safety codes, which is currently unaccounted for.

2. Australia's regulatory approach to online services, systems and processes

2.1 *Q1. Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?*

IGEA does not consider changes are required at this stage to the current objects of the OSA.

2.2 *Q2. Does the Act capture and define the right sections of the online industry?*

IGEA does not consider changes are required at this stage regarding sections of the online industry.

2.3 *Q3. Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?*

The OSA should continue to be clearly separated from, while aligned with, the NCS as well as relevant legislation such as the Privacy Act. This would then enable eSafety to properly execute its functions appropriately in accordance with the OSA.

The Stevens Review clarified the role of eSafety:[11]

> *The eSafety Commissioner would continue to have responsibility for responding to online content that is illegal, including content that would be Refused Classification under the National Classification Scheme. Further: … the Office of the eSafety Commissioner would continue to focus on taking action on illegal and harmful content online, including websites and user-generated content.*

In this regard, to avoid any doubt and potential overlap with the NCS, we recommend that it be clearly stated that the OSA would only address illegal and unclassifiable online content (such as the majority of user-generated content), while the NCS (along with the Restricted Access System Declaration) deals with classified and classifiable content.

Further, the modernisation of the NCS has been built on the primary guiding principle that "adults should be able to read, hear, see and play whatever they want". Accordingly, with respect to video games, they are designed and have regard to age appropriate levels. Therefore, not all games are designed to be targeted at children (and nor should they be) and are therefore rated accordingly.

Nevertheless, there is now the explicit inclusion of "the best interests of the child" requirement as an additional expectation in the BOSE Determination for service providers to "take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children". If interpreted broadly, this could suggest that all video games should be designed with children as an audience, even when they would be classified at a restricted level and therefore not appropriate for children. Such an interpretation would create a perverse outcome and conflict with the NCS objectives.

We therefore reiterate our position that it would be better served for any language in the OSA and other subordinate legislation where reference is made to "best interest of the children" that this be reflected as follows:

- With respect to the BOSE Determination (and any other regulatory instrument) that require service providers to take reasonable steps to ensure the best interests of the child, this should be referring to the design and operation of any service that is '***targeted at, or***

[11] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Review of Australian classification regulation' (Report, May 2020), led by Neville Stevens AO (Stevens Review), pp. 39, 120, https://www.infrastructure.gov.au/sites/default/files/documents/review-of-australian-classification-regulation--may2020.pdf.

directed to*, children**' (as opposed to 'likely to be accessed by*** **children**'). Similar terminology has been used overseas in legislation (e.g. US federal statute COPPA) which industry considers to be unambiguous.[12]

- In contrast, the '*likely to be* accessed by' terminology is still vague and potentially broad in meaning. We note that the 'likely to be accessed by children' terminology has been used in some overseas statutes, which has been problematic.

Recommendation: To provide greater clarity, it should be clearly stated in the OSA (and subordinate instruments) that it only addresses illegal and unclassifiable online content (such as the majority of user-generated content), while the NCS deals with classified and classifiable content (which is particularly applicable to video games like the film industry).

2.4 *Q4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?*

According to the Explanatory Memoranda to the OSA, the BOSE provision was included in the Act to "encourage the prevention of online harms by technology firms and digital platforms, and would improve the transparency of actions taken by social media services".[13] By its name, this is essentially a basic set of expectations for service providers to broadly demonstrate online safety practices. Since then, there appears to be a significant departure from this approach under the BOSE, arguably shifting to "enforcement" through not only civil penalties, but also naming-and-shaming and other adversarial regulatory actions.[14] Over time, this approach may cause service providers to be reluctant to share information to the fullest degree for fear of being publicly shamed.

The Department considers that the BOSE sets "a benchmark for online service providers to take proactive steps to protect the Australian community from abusive conduct and harmful content online" and is "an essential part of driving transparency and accountability across online services".[15] While the OSA does not impose penalties for service providers not complying with the BOSE, there are significant civil penalties attached for failure to comply with a reporting notice issued by eSafety.[16] Compounded to this, eSafety can also make public (include providing running media commentary which is then naturally amplified by the media) on non-compliance findings against service providers who do not sufficiently report on the BOSE, according to eSafety's expectations.[17] eSafety can also, yet not obliged to, publicly name-and-shame those that do not meet the BOSE, even if service providers are not contravening the BOSE Determination.

With all that being said, according to eSafety, while service providers may not be penalised for reporting non-compliance with the BOSE, failure to comply with an expectation under the

[12] https://www.law.cornell.edu/uscode/text/15/6501.

[13] Explanatory memorandum to Online Safety Bill, p. 11, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr6680%22.

[14] eSafety, 'Federal court proceedings involving eSafety', https://www.esafety.gov.au/industry/federal-court-proceedings-involving-esafety.

[15] Department's issues paper, p. 14, https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-act-2021-review-issues-paper-26-april-2024.pdf.

[16] As the Department's issues paper notes, "a service provider that fails to comply with a reporting notice or determination issued by the Commissioner may be subject to a formal warning or a civil penalty of up to 500 penalty points (currently $782,500) for corporations." (Department's Issues paper, p. 15.)

[17] eSafety, 'Responses to transparency notices', https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices.

Determination may result in other enforcement action by eSafety.[18] This suggests that eSafety has expanded the original policy intention for the BOSE Determination.

Further, we note that the inaugural BOSE Determination was introduced during a time when the industry online safety codes were yet to be developed and in place.[19] Unlike the BOSE, compliance with the industry online safety codes and industry standards requires mandatory minimum compliance measures that eSafety is able to enforce through the courts, as well as through other means.

Notwithstanding the different ways in which the BOSE Determination and industry online safety codes and standards operate and are enforced, there are overlapping requirements. This is likely due to similar policy objectives that ultimately set minimum online safety requirements. This naturally leads to confusion and complexity in the application of the various regulatory instruments under the OSA.

A simple solution would be if service providers were meeting specific requirements under either the BOSE Determination or industry online safety codes or standards, they should not need to be subject to duplicated requirements. For instance, transparency reporting of online safety measures features in these regulatory instruments, as well as the OSA. As a matter of administrative efficiency, Government should explore ways to streamline these requirements to avoid unnecessary regulatory duplication and conflicts.

Finally, we consider that the BOSE should be written in more harms-agnostic language to ensure that it is able to respond to new and emerging harm types without needing to be constantly reviewed.

In our recent submission to the BOSE Amendment Determination, we offered several recommendations to address some of these issues. We encourage the Department to reconsider these, which we have included in Appendix A of this submission.[20]

Recommendations:

- **The BOSE Determination currently captures a huge range of service types given all SMS, RES and DIS are considered to be in scope. The Determination should allow for greater flexibility for the various online services captured by the Determination to meet the expectations in ways that make sense for that service type, giving adequate consideration to the nature of potential harms on the service.**
- **The BOSE Determination process should be simplified and streamlined with other concurrent regulatory instruments including industry online safety codes and standards. Government should explore ways to streamline such requirements to avoid unnecessary regulatory duplication and conflicts.**

[18] eSafety, 'Basic Online Safety Expectations: Regulatory Guidance' (September 2023), p. 11, https://www.esafety.gov.au/sites/default/files/2023-09/Basic-Online-Safety-Expectations-Regulatory-Guidance-updated-September-2023_0.pdf.

[19] Note: The BOSE Determination cannot amend the Online Safety Act or extend the Commissioner's functions and powers beyond what is contained in the Act. It can only operate within the scope it is empowered to cover under Part 4 of the Act. There are no civil penalties for failure to comply with the expectations outlined in the BOSE Determination, nor does the BOSE Determination impose a duty that is enforceable by court proceedings.

[20] IGEA submission to Draft Online Safety (BOSE) Amendment Determination 2023, https://igea.net/2024/02/igea-submission-to-draft-online-safety-basic-online-safety-expectations-amendment-determination-2023/.

2.5 Q5. Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?

With respect to industry codes, there are certainly lessons that can be learnt from the Phase 1 industry online safety codes development process.

Beginning with the challenges, the following are several key issues that arose during the Phase 1 development process:

- <u>New considerations:</u> From the outset, it should be recognised that the process to co-developing the codes was novel. The scope and timeframe had to continually change as both eSafety and industry adjusted to new understandings and considerations, including what was practically and realistically feasible.
- <u>Unrealistic timeframes:</u> Time allocated for developing codes were extremely ambitious. It ended up taking almost 24 months to develop these codes, significantly different from the originally planned length of six months specified in legislation.[21]
- <u>Lack of transparency:</u> Despite working with eSafety throughout the codes development process, of the eight industry online safety codes that were developed, two were rejected by eSafety. Many hours and resources were expended by industry to develop those codes which were in turn rejected. This then led to development of draft standards which lacked clear context, direction, expectations and explanations upfront (including draft guidelines which were intentionally omitted from the consultation). Therefore, it was difficult to ascertain why certain draft provisions differed from the draft codes.

Reflecting on these issues from Phase 1, we are also concerned that this will be even more challenging for the pending Phase 2 code development process, raising open-ended questions such as the relationship between the age assurance trial and the codes. As with the Phase 1 codes development process, proper consultation with wider industry stakeholders will be critical for Phase 2.

We anticipate there will be other and likely newer issues with Phase 2 codes development process. Not only will industry stakeholders need to have regard to these such as the concurrent age assurance trial, but it will also be challenging for industry to productively develop a code for Class 2 content if the Phase 2 timelines are unreasonably tight as before (under Phase 1), and while the Stage 2 NCS reforms are currently underway.

Additionally, there are multiple moving parts, with the amendment to the BOSE Determination having been recently passed, RES and DIS Standards only just registered (during this OSA Review consultation period), and other multiple government announced reforms. These arguably overlap with the Phase 2 codes development process, making it difficult to ensure regulatory coherence and stability under the OSA.

Setting aside the multiple reforms underway, the following are our recommendations for enabling a more productive approach to the Phase 2 codes development process:

- <u>Sufficient time:</u> More time needs to be built into the development of the codes, rather than shortening them. For procedural fairness and as a matter of good policy design and best regulatory practice, we strongly recommend that sufficient time be allocated by eSafety to

[21] Online Safety Act, section 137(2)(a).

undertake public consultation, especially with directly affected stakeholders, before eSafety decides to update its Position Paper.

- Flexibility to consider relevant issues: Ideally, there should be a clearer idea of the specific measures and obligations developed between industry and eSafety at the beginning of the process. However, there should be flexibility to appreciate that some expectations will not become fully realised until they are tested in the drafting of the codes.
- Scope: It would be helpful for the Position Paper to address how the proposed codes for Phase 2 would work alongside the NCS in its current form and how the codes may need to adapt to any changes to the NCS. The NCS, along with the Restricted Access System (RAS) Declaration, should be sufficient to address classified and classifiable content, while the industry online safety codes should be used to address unclassifiable online content (such as the majority of user generated content). This is consistent with what eSafety has previously set out in their position paper where they stated the following: "The codes will not apply to game content which has been classified in Australia. However, the codes will apply to content imported into a game environment via the game's interactive tools which is separate to the game itself and which is likely to be classified as class 1 or class 2 material. The codes will also apply to game content which has been recorded and posted elsewhere on the internet."[22]
- Dialogue and transparency: Transparency is imperative to both enable trust as well as productive engagement from impacted stakeholders. It is therefore critical that frank and open discussions occur in a safe environment to ensure proper collaboration in developing the codes.

Recommendations:

- **Given that there are so many moving parts in online safety reform, this has made it difficult to keep up with the various factors influencing policy considerations such as age assurance. Greater attention should be given to simplifying and streamlining each area so service providers are clear on the parameters and expectations.**
- **For the Phase 2 industry online safety codes development process to be effective, it is important that there be sufficient time allocated to the process, flexibility for consideration of relevant issues, clearly scoped and avoid overlapping requirements between the Phase 2 codes and other regulatory instruments (e.g. NCS), and mutual transparency between the regulator and industry stakeholders to ensure a more productive process.**

2.6 *Q6. To what extent should online safety be managed through a service providers' terms of use?*

As a general comment, the service provider should be given the flexibility in how it enforces breaches of terms of use, especially if it relates to low impact issues compared to high impact issues at the other end of the spectrum.

In the context of video games, the video game industry is committed to creating safe and enjoyable online spaces for players. Over decades of experience, the industry has cultivated environments

[22] eSafety, 'Development of industry codes under the Online Safety Act: Position Paper', p. 33, https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf.

where players feel welcome, safe and secure, leading to a strong history of self-regulatory measures to enhance online safety. These include implementing parental controls on all major platforms and funding consumer information campaigns on safe online play.

As part of global industry best practice, the industry has long-established clear terms of service and removes any content or interactions that violate these terms, including illegal content. Game platforms and publishers enforce robust terms of use to ensure safe and inclusive behaviour, disciplining disruptive players accordingly. They also implement preventive and reactive technical safeguards such as content filters, reporting mechanisms, and dedicated moderation teams to maintain a secure and sophisticated online environment. These measures are backed by well-developed enforcement policies, allowing companies to issue temporary or permanent bans to offenders proportionately.

Recommendation: The service provider should be given the flexibility in how it enforces breaches of terms of use. The video game industry has long-established clear terms of service and removes any content or interactions that violate these terms, including illegal content, complemented by appropriate penalties and other preventive and reactive industry safeguards.

2.7 *Q7. Should regulatory obligations depend on a service providers' risk or reach?*

As a general comment, a proportionate approach to regulatory obligations should be based on the service's level of risk, as opposed to arbitrary definitions and thresholds. However, further considerations are needed to appropriately assess the risk and identified harm.

The purpose of a risk assessment is to evaluate the real risk of illegal content appearing on the service, taking into account current mitigation measures. Ignoring these measures would mean assessing a different service altogether. A proper risk assessment process should guide companies in identifying areas needing more attention to mitigate residual risks to users. Once these actions are taken, companies can update their risk assessments accordingly. This should be made clearer in the OSA framework.

Similarly, when evaluating the risk level of identified potential harm, a single occurrence should not automatically classify the harm as a higher risk. While such an incident may suggest a potential risk, this should be considered in the context of all available evidence. Factors like the frequency or probability of incidents, the degree of harm, the proportion of verified complaints related to the harm, and the mitigation measures in place must be taken into account. It would be unreasonable to label a service as a higher risk, and impose additional obligations, based solely on an isolated incident or even a technical possibility of an incident occurring.

For example, we discuss this concept in our Draft RES Standard submission to eSafety, where the Standard includes predefined categories, including for gaming services with and without communications functionality, along with associated obligations.

On the one hand, we appreciate the intention to provide regulatory clarity and certainty for service providers on whether they should be categorised as gaming services with communications functionality and those with limited communications functionality. If that is the case, the service provider may decide to accept this predetermined assessment and comply with their applicable obligations.

However, some flexibility should be allowed in the circumstance where gaming services meet the definition of those with communications functionality, aligned with a more proportionate risk-based approach that promotes and incentivises a Safety-by-Design approach for "a gaming service with communications functionality".

There are already well-established principles for conducting risk assessments based on severity and probability of harm. Communications functionality can significantly vary from one gaming service to another. The severity and likelihood related to child sexual abuse material (CSAM) or pro-terror material (PTM) can be influenced by many factors including: whether the communication is transient; who plays the particular game or uses the particular service; effectiveness of existing measures already in place; and the types of communications possible.

A solution we put forward in our Draft RES Standard submission is that if a service provider were deemed to be "a gaming service with communications functionality" (and therefore subject to associated obligations), they should be given a rebuttable assumption. That is, they should be given the option to undertake a risk assessment to prove that they have a different (lower) risk profile, such as Tier 2 or 3 (and subject to those associated obligations). Alternatively, the service provider may elect not to undertake a risk assessment and accept the default obligations of "a gaming service with communications functionality".

Such an approach would balance between providing regulatory certainty and clarity in the operation of the RES Standard insofar as they apply to the categories for gaming services, while offering some flexibility for gaming service providers who are categorised as having communications functionality to prove – if they choose to do so – that their risk level is proportionately targeted.

This approach would not diminish the risk assessment for online safety, while providing flexibility in addressing online safety.

Unfortunately, our preliminary review of the RES Standard (which has only just been registered by eSafety during this OSA Review period) suggests that eSafety did not accept this. We therefore wish to elevate this issue as part of the OSA Review.

Recommendation: Generally, a proportionate approach for regulatory obligations should be based on the level of risk of the service and its users, as opposed to arbitrary definitions and thresholds. However, proper consideration of a risk assessment should be to evaluate the real risk of illegal content appearing on the service, taking into account current mitigation measures. Further, when evaluating the risk level of an identified potential harm, it should not be based merely on one isolated incident or a technical possibility of an incident occurring. Instead, it should take into account relevant factors such as the frequency or probability of incidents, the degree of harm, the proportion of verified complaints related to the harm, and the mitigation measures in place.

3. Protecting those who have experienced or encountered online harms

3.1 *Q8. Are the thresholds that are set for each complaints scheme appropriate?*

No comment at this stage.

3.2 *Q9. Are the complaints schemes accessible, easy to understand and effective for complainants?*

No comment at this stage.

3.3 *Q10. Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?*

No comment at this stage.

3.4 *Q11. Does the Commissioner have the right powers to address access to violent pornography?*

In short yes, violent pornography is directly addressed as part of the Phase 2 codes development process for Class 2 material that includes pornography and other restricted content (from R18+ and above).

However, we would caution when having regard to restricted content that may not be limited to pornography, especially if these are already addressed under the NCS. This becomes more of a challenging issue when considering restricted content under the "themes" classifiable element, which need to be determined according to context and treatment. There are also practical questions such as the appropriate regulatory expertise to assess content that has not been classified to determine whether they may be Class 2 material, and whether eSafety's decisions can be reviewed under the online safety framework (which would otherwise be available under the NCS framework).

3.5 *Q12. What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?*

As noted above, the trial for age assurance has recently been announced.

Public commentary from experts suggests the likelihood of policy failure with such a trial due to the lack of feasibility of these technologies, which can be easily circumvented by users and legitimate public concerns regarding privacy and security.

The use of circumvention technology to bypass online safety measures was recently considered in the Federal Court.[23] Here, eSafety contended that X Corp did not sufficiently comply with its removal notice by geo-blocking 65 URLs. The public were still able to access these URLs via Virtual Private Networks (VPNs). The court ultimately found the case in favour of X Corp, as discussed in Question 15 below. Nevertheless, circumvention technologies will be a live and ongoing challenge for any proposed age assurance system.

We reiterate caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing such age assurance technologies. This was previously acknowledged by the Government in response to eSafety's Roadmap for Age Verification. In particular, the Roadmap found that age assurance technologies were immature and presented their own privacy, security, effectiveness and implementation issues; hence the Government was

[23] eSafety Commissioner v X Corp [2024] FCA 499 [38], https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2024/2024fca0499.

unable to mandate age assurance at the time.[24] We do not consider that technology would have advanced dramatically in less than a year to address those legitimate concerns. However, we would be interested to see if the trial suggests otherwise.

With respect to the video game industry, the Stevens Review acknowledged that gaming consoles have robust parental control capabilities to address child access to age-inappropriate games that would be pertinent to online safety.[25] The Stevens Review also recognised that parents and carers wished to ultimately play a role and make judgements about what their children watch or play; it should not be for the classification regime (or in this case, eSafety) to essentially become the substitute parent or carer of their children. In this regard, the Stevens Review agreed that parental controls coupled with adult supervision would be the better alternative than maintaining a problematic legal restriction on content online.

These conclusions from the Stevens Review should come as no surprise, given that the video game industry has long spearheaded self-regulatory measures for safe online play, including parental controls.

Like the film industry, the video game industry follows strict age-appropriate standards, and user interactions are often limited and subject to parental controls or age restrictions. The video game industry takes a further greater step, protecting player privacy by collecting and storing gameplay data anonymously, without directly linking it to individual players' identities.

In advocating for responsible gaming, the video game industry supports the significance of parental and caregiver participation, enabling them to play an active role in setting up parental controls. With default settings prioritising safety and privacy, parents and carers can make informed choices regarding content access and online interactions, tailored to their child's age and maturity level. This approach facilitates meaningful communication and oversight between parents or carers and their children in online activities.

Ensuring children's safety online hinges on parental and caregiver consent, and our industry has led the way in creating effective parental control tools across different devices and platforms. These tools enable parents and caregivers to customise content access, oversee in-game spending, and supervise online communication based on their preferences and their child's requirements.

Our industry endeavours to offer transparent and dependable guidance to users and their parents or carers through age-specific account types and thorough pre-contractual information. The industry's commitment to responsible gaming practices, demonstrated by its adherence to age rating systems globally, including in Australia, implements objective content assessment, responsible advertising, consumer grievance mechanisms, and rigorous privacy standards.

Preserving robust privacy policies and nurturing a secure online gaming atmosphere are fundamental principles of our industry, empowering users to retain control over their personal information and to resolve any privacy issues that may arise.

Recommendations:

- **We caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing age assurance**

[24] Australian Government response to the Roadmap for Age Verification, (August 2023), p. 2, https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf.

[25] Stevens Review, p. 69.

technologies. We would be keen to understand whether these concerns are addressed from the age assurance trial.

- **Like the film industry, the video game industry has long spearheaded parental control capabilities in video game services to address child access to age-inappropriate games, based on global industry best practice. However, the video game industry takes a further greater step in protecting player privacy by collecting and storing gameplay data anonymously, without directly linking it to individual players' identities. Ensuring children's safety online hinges on parental and caregiver consent. Our industry has led the way in creating effective parental control tools across different devices and platforms. Parents and carers are therefore empowered to use technological and/or non-technological means to help manage their children's viewing and playing experiences, as opposed to deferring to the government. This nuance needs to be better appreciated in how online safety is approached for video games by government.**

3.6 Q13. Does the Commissioner have sufficient powers to address social media posts that boast about crimes or is something more needed?

From a video game industry perspective, this is not a relevant question for our industry so we do not have any comments.

3.7 Q14. Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?

In principle, there could be merit in considering bystanders who may not be directly affected in the context of reporting to eSafety.

We understand that criminal laws exist in most states and territories in Australia that require adults to report known child sexual offences.[26] In this case, consideration could be given to whether eSafety should be included (if it is not already, and to avoid duplicated requirements and agencies), or whether there are sufficient law enforcement agencies engaged already.

Beyond child sexual offences, this raises other questions for further consideration around whether there also exists similar bystander laws for other criminal offences that might also extend to other illegal or seriously harmful material under eSafety's purview, and how that might operate in practice.

If bystanders were to be contemplated in scope to raise a complaint, there should also be appropriate privacy protections in place. Other proper safeguards should be in place to ensure that volume of complaints do not arise that are disingenuous (e.g. spammy, vexatious or malicious), at the cost of genuine complaints.

Recommendation: In principle, there could be merit in considering bystanders who may not be directly affected to report to eSafety regarding illegal or seriously harmful material. Consideration should be given to existing laws in place that already offer similar arrangements. There should be proper safeguards to ensure that bystanders are properly protected (such as privacy) and legitimate reports are only accepted (avoid disingenuous complaints).

[26] Australian Institute of Family Studies, 'Mandatory reporting of child abuse and neglect' (Resource sheet, August 2023), https://aifs.gov.au/resources/resource-sheets/mandatory-reporting-child-abuse-and-neglect.

3.8 *Q15. Does the Commissioner have sufficient powers to address harmful material that depicts abhorrent violent conduct? Other than blocking access, what measures could eSafety take to reduce access to this material?*

Yes, eSafety does have sufficient powers that are reasonably limited by jurisdictional boundaries and what can be reasonably implemented by the service provider. It is also important that the technically feasible limits of service providers are reflected in practice (such as when making and interpreting subordinate legislation). Within this scope of power, eSafety can block, and seek enforceable undertakings and injunctions.[27]

It is important that the Government accepts that there are geographical limits to domestic legislation. As recently stated by Kennett J, "Courts rightly hesitate to make orders that cannot be enforced, as it has the potential to bring the administration of justice into disrepute".[28] This boils down to the general presumption and "well settled rule of construction" in interpretation of legislation of the "comity of nations".[29] In this case, it was "a clear case of a national law purporting to apply to persons or matters over which, according to the comity of nations, the jurisdiction properly belongs to some other sovereign or State".[30] And to paraphrase, for eSafety to require a service provider to implement measures "everywhere in the world is *not* a step that it is reasonable … is [a] powerful [argument]".[31]

The Federal Court case provides a telling lesson that should be informative for any policymaker, regulator or legislation that seeks to operate beyond its jurisdictional limits. As a matter of public policy that goes well beyond the narrow lens of online safety, those implications should not be underestimated.

While not immediately addressing the broader policy issues arising from the case, Kennett J made the following observations:[32]

> *Apart from questions concerning freedom of expression in Australia, there is widespread alarm at the prospect of a decision by an official of a national government restricting access to controversial material on the internet by people all over the world. It has been said that if such capacity existed it might be used by a variety of regimes for a variety of purposes, not all of which would be benign.*

Additionally, Australia must consider the precedent set if it was able to order global content takedowns. Other countries with less stringent human rights frameworks may seek to replicate such an approach with severe impacts on the freedom of expression of citizens and potentially quashing the important documentation of crimes by the state or crimes against humanity.

Should the Government wish to address the jurisdictional limits that "properly belongs to some other sovereign or State", then it would be better served through international regulatory coordination such as the Global Online Safety Regulators Network that includes eSafety.

[27] eSafety, 'Abhorrent Violent Conduct Powers: Regulatory Guidance' (December 2021), https://www.esafety.gov.au/sites/default/files/2022-03/Abhorrent%20Violent%20Conduct%20Powers%20Regulatory%20Guidance.pdf.

[28] eSafety Commissioner v X Corp [2024] FCA 499 [58], https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2024/2024fca0499.

[29] Ibid [48]-[51].

[30] Ibid [50].

[31] Ibid [48].

[32] Ibid [40].

Recommendations:

- **eSafety does have sufficient powers that are reasonably limited by jurisdictional boundaries and what can be reasonably implemented by the service provider. It is also important that the technically feasible limits of service providers are reflected in practice (such as when making and interpreting subordinate legislation).**
- **Should the Government wish to address the jurisdictional limits of the online safety framework, then it would be better served through international regulatory coordination such as the Global Online Safety Regulators Network.**

3.9 Q16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

The regulator should work closely with key stakeholders, including industry associations, to develop informed research and educational materials. The video game industry is strongly committed to creating fun and safe gaming experiences for all and advocates for healthy gameplay by providing evidenced-based practical guidance. IGEA is having ongoing discussions with eSafety, as with other regulators and agencies, to explore collaborative activities. For example, as part of Safer Internet Day this year, we supported and promoted eSafety's research into video gaming and online safety. The IGEA Trust & Safety Hub provides educational resources for players and their families, including information on SafetyTech that are built into video games, to prevent and mitigate harmful behaviours. The Trust & Safety Hub's collaboration page features information on eSafety's work and its reporting mechanisms.[33]

More generally, eSafety has a powerful educational role with the public to raise awareness about online safety, as does police when it comes to 'Stranger Danger', and developing research on trends such as types of online safety issues and solutions. Such research can be better informed through improved collaboration with industry and experts to ensure rigorous and robust representation, which we discuss in Question 24 below. This would be the most effective way to proactively empower online safety with the community, and arguably better use of public money. In contrast, the costly exercise of reactively regulating and litigating against service providers has no guaranteed prospects of success and not a prudent use of public funded resources.

Recommendation: eSafety has a powerful educational role to raise public awareness about online safety, and developing research on trends such as types of online safety issues and solutions. Such research can be better informed through improved collaboration with industry and experts to ensure rigorous and robust representation. This would be the most effective way to proactively empower online safety with the community. We have been exploring collaboration opportunities with eSafety with respect to the video game sector.

[33] https://igea.net/trust-safety/.

4. Penalties, and investigation and information gathering powers

4.1 *Q17. Does the Act need stronger investigation, information gathering and enforcement powers?*

The OSA does not need to create more regulatory powers, given the plethora of regulatory instruments in place (some relatively new, as discussed above), while other new reforms are also underway or planned.

Instead, as discussed earlier, the focus should be on simplifying the process. The operation of the OSA warrants improvement and reform in how regulatory instruments that flow from the OSA are implemented in practice, including development, enforcement, and interpretation. This includes how online content is regulated, such as understanding treatment and context when classifying content. Examples where these issues have arisen include with respect to PTM.

It is also imperative that any obligations on service providers have appropriate safeguards in place. For example, when service providers are required to share information with eSafety, there should be appropriate safeguards in how the regulator manages such information in accordance with due process, transparency, confidentiality, and privacy. For instance, there needs to be protections in place to safeguard commercially sensitive industry data. Also, service providers should not be compelled to provide data to third parties via the regulator (such as researchers) – this ensures that the use of such data is properly managed and understood by the information provider and receiver. The regulator should also make clear the reasons why it is seeking this information and the manner in which that information will be treated.

Similar safeguards operate in other areas such as under the *Security of Infrastructure Act 2018* (Cth) (SOCI Act). To enable sharing of information under the SOCI Act, policymakers accepted the importance of protecting information, especially those that are commercially sensitive, that is used and disclosed by the authorised regulatory agencies.[34] It also helps to establish greater transparency and mutual trust between the information provider and receiver.

Recommendations:

- **The OSA does not need to create more regulatory powers, given the plethora of regulatory instruments in place, while other new reforms are also underway or planned.**
- **There should be a focus on simplifying the overall online safety framework. This can then flow down to how regulatory instruments are implemented in practice including development, enforcement and interpretation.**
- **There should also be emphasis on developing harm-agnostic frameworks that are able to adapt to new and emerging threats, some of which we may not yet even conceptualise. This removes the need for constant updates to the Act and its secondary instruments which is time consuming for the government, regulator and all stakeholders.**
- **When service providers are required to share information with eSafety, there should be appropriate safeguards in how the regulator manages such information in**

[34] Department of Home Affairs, Cyber and Infrastructure Security Centre, 'Protected Information: Industry guidance for critical infrastructure assets' (Fact sheet, July 2023), https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-protected-information.pdf.

accordance with due process, transparency, confidentiality, and privacy. For instance, there needs to be protections in place to safeguard commercially sensitive industry data. Also, service providers should not be compelled to provide data to third parties via the regulator (such as researchers) – this ensures that the use of such data is properly managed and understood by the information provider and receiver. The regulator should also make clear the reasons why it is seeking this information and the manner in which that information will be treated.

4.2 *Q18. Are Australia's penalties adequate and if not, what forms should they take?*

Australia's penalties are adequate.

4.3 *Q19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?*

As discussed in response to Question 15 above, there are jurisdictional limits to any Australian legislation or regulation, albeit in legal theory it can be applied anywhere versus reality, as found in the recent Federal Court case.[35]

It is therefore important when designing any regulatory regime in Australia that it factors international regimes. Ideally, Australia should be following international approaches rather than trying to be a leader in regulation, as that approach could more likely drive compliance for companies based overseas, given their global scale of operations compared to in Australia. We discuss this further in response to Question 21.

Further, as a general comment, regulating companies in Australia which may differ to overseas, inadvertently creates an unfair obligation on Australian based entities and therefore commercial and competitive disadvantage compared to overseas operators.

4.4 *Q20. Should the Commissioner have powers to impose sanctions such as business disruption sanctions?*

No, the OSA should not grant the Commissioner the power to impose sanctions. Sanctions are a foreign policy instrument subject to international law and conventions, therefore the decision to sanction must remain in Commonwealth agencies with the appropriate capabilities and expertise.

We note that in 2021, the Federal Government reviewed Australia's sanctions regime with input from the bipartisan, Joint Standing Committee on Foreign Affairs, Defence & Trade. Under the new changes,[36] Magnitsky-style sanctions can be imposed over severe human rights violations by nation-states. Here, it could be argued that the government is not seeking state-based sanctions.

Nevertheless, sanctions can be imposed on persons and entities responsible for significant cyber security incidents. In instances of significant cyber security incidents, the decision to upward escalate such incidents falls under the remit of the Australian Signals Directorate (ASD).

However, the proposed addition of business disruption sanctions to the scope of powers for eSafety would be akin to national security functions as a last resort power, which we strongly suggest would be regulatory over-reach in the context of online safety and should remain outside the remit of the Commissioner.

[35] eSafety Commissioner v X Corp [2024] FCA 499 [58], https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2024/2024fca0499.

[36] https://www.dfat.gov.au/sites/default/files/issues-paper-review-of-australias-autonomous-sanctions-framework.pdf.

Recommendation: The OSA should not grant eSafety the power to impose sanctions. Sanctions are a foreign policy instrument subject to international law and conventions. The decision to sanction must remain in Commonwealth agencies with the appropriate capabilities and expertise.

5. International approaches to address online harms

5.1 *Q21. Should the Act incorporate any of the international approaches identified above? If so, what should this look like?*

Given that Australia is arguably spearheading the charge in online safety regulation compared to its overseas counterparts, we cannot offer more that Australia can do compared to others.

However, regulatory coherence with overseas approaches would be the most logical step. Internationally, the government must consider the changed global regulatory landscape since the OSA was first published. To align with the broader aim of making Australia an attractive destination for the video game industry to invest, international regulatory coherence is crucial. More importantly, international alignment ensures a better user experience in a global online environment. Given the small Australian market, it is important that Australia give proper consideration to overseas approaches, including lessons learnt, rather than trying to lead in areas or reinventing the wheel.

It would therefore be prudent to refer to overseas requirements such as the EU Digital Services Act (DSA) and UK Online Safety Act (OSA), as many video game companies operate globally. This will help to ensure that international requirements between different sources of law are aligned. This can be effectively addressed by taking into consideration concepts/definitions similar to the EU DSA and UK OSA, as well as similar approaches to implementing obligations and regulation. Nevertheless, it is important to acknowledge that these requirements are relatively new, and may have teething issues that need to be resolved through lessons learnt. In this regard, we understand there is a Global Online Safety Regulators Network, including eSafety, which has recently released a position statement on regulatory coherence, which could be an avenue to have regard to such matters. However, it would be beneficial for the government to consider industry input into such discussions, especially those subject to these overseas requirements.

Recommendation: Given the global nature of the video game industry, it would be prudent to refer to overseas approaches such as the EU Digital Services Act (DSA) and UK Online Safety Act (OSA), and how that is being implemented and regulated in practice. Nevertheless, it is important to acknowledge that these requirements are relatively new, and may have teething issues that need to be resolved through lessons learnt. The Global Online Safety Regulators Network, including eSafety, could be an avenue to have regard to such matters. However, it would be beneficial for the government to consider industry input into such discussions, especially those subject to these overseas requirements.

5.2 *Q22. Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?*

As discussed above, there are already regulatory instruments in place that we do not consider further measures necessary. This is especially the case for the current arrangements that are relatively new and too early to reassess, with the most recent being the BOSE Amendment Determination and industry online safety industry standards (including RES).

5.3 *Q23. Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?*

We have discussed in Question 4 about the various transparency reporting requirements that arise through multiple regulatory instruments in the online safety framework.

The industry online safety codes and standards development process could see some improvement in the transparency by the regulator to facilitate productive and genuine collaboration to properly develop these codes and standards, as discussed above in Question 5.

In the process of providing information to eSafety, safeguards are needed to protect the information that is provided, as well as more transparency from the regulator as to the purpose and reason that it is collecting information from services providers, as discussed in Question 17.

Given that eSafety regulates content, having regard to classified and classifiable content under the NCS, this requires appropriate expertise and capability to review content. It is therefore important to ensure that the regulator's personnel charged with reviewing content are properly trained including understanding treatment and context. This is our experience with how the Classification Board approaches content, which has been built through many years of experience, expertise, and engagement with industry. However, the Classification Board does not operate without unfettered accountability, and service providers have the avenue to seek a review of the Board's decision through the Classification Review Board (although this function may move to another agency such as ACMA, as part of the Stage 2 NCS reforms).

In the context of online safety, there are expensive options to seek an impartial review for eSafety's decisions via judicial and alternative dispute mechanisms such as the Federal Court, Administrative Appeals Tribunal and ombudsman. We understand that it could be argued that eSafety may deal with live and user-generated content that may not traditionally be classified by the Classification Board, which could take several days to be reviewed by the Board depending on the sense of urgency and volume of complaints. However, a proportionate mechanism should still be in place to enable procedural fairness and review of decisions. We therefore recommend a new review body be established to review eSafety's decisions, should a service provider challenge their decisions.

More generally, a lack of public trust in regulatory decisions can be attributable to a lack of regulator transparency, governance and accountability, compounded with how that information is handled and treated. This can be addressed through building into legislation more accountability mechanisms to ensure that regulators do not operate without unfettered power.

In the case of eSafety, assurances that it does not intend to operate beyond its powers on legitimate public concerns (such as not breaking encryption)[37] are welcomed; however, this would be better addressed through legislation. In particular, building proportionate checks-and-balances into the OSA regime in the regulatory decision-making process should provide more public and industry confidence in the online safety regime.

Such an approach is not without precedent, especially for areas in which the public may consider a government's or regulator's actions to be intrusive, which has also invoked other concerns such as freedom of speech and political discourse, warranting a need for proper accountability mechanisms:[38]

> *Public consent to intrusive laws depends on people trusting the authorities, both to keep them safe and not to spy needlessly on them … Trust in powerful institutions depends not only on those institutions behaving themselves (though that is an essential prerequisite), but on there being mechanisms to verify that they have done so. Such mechanisms are*

[37] eSafety, 'Statement on end-to-end encryption and draft industry standards' (Media release, 19 December 2023), https://www.esafety.gov.au/newsroom/media-releases/statement-on-end-to-end-encryption-and-draft-industry-standards.

[38] David Anderson QC, Independent Reviewer of Terrorism Legislation, 'A question of trust: Report of the Investigatory Powers Review' (June 2015) (quoted in a report by Dr James Renwick CSC SC, Independent National Security Legislation Monitor, 'Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters' (June 2020), p. 23).

> *particularly challenging to achieve in the national security field, where potential conflicts between state power and civil liberties are acute, suspicion rife and yet information tightly rationed … Respected independent regulators continue to play a vital and distinguished role. But in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency.*

Recommendations:

- **Given that eSafety regulates content, having regard to classified and classifiable content under the NCS, this requires appropriate expertise and capability to review content. The regulator's personnel charged with reviewing content should be properly trained including understanding treatment and context.**
- **A proportionate mechanism should be in place to enable procedural fairness and review of decisions by eSafety. We therefore recommend a new review body be established to review eSafety's decisions (in addition to current judicial and merits review mechanisms), should a service provider challenge their decisions. This should be specified in legislation to ensure that there are proportionate checks-and-balances in the regulatory decision-making process to provide more public and industry confidence in the online safety regime.**

5.4 *Q24. Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?*

The Stage 2 NCS reforms are contemplating a Classification Advisory Panel consisting of experts to inform on trends in classification issues, as recommended in the Stevens Review. If well-designed (including proper industry stakeholder representation, with meaningful value and purpose), this could be an effective tool for informing the classification regulator on emerging issues and research. A similar body could be established for online safety.

If eSafety helps to drive online safety research, as discussed in Question 16, it would be prudent that this be strengthened through greater collaboration with stakeholders including with industry to ensure its research is rigorously tested, based on relevant and robust information. This will help to also ensure that any findings that may arise are well-informed and represented to properly inform policy makers and others. This would be an example where an Online Safety Advisory Body can play an important role.

In terms of access to data, as discussed in Question 17, eSafety already has powers to compel service providers for information. However, in providing this information, there should be appropriate safeguards in how the regulator manages such information in accordance with due process, transparency, confidentiality, and privacy. For example, protections need to be in place to safeguard commercially sensitive industry data, and prevention of third parties (such as researchers) having access to data provided by the service provider to the regulator. The regulator should also make clear the reasons why it is seeking this information and the manner in which that information will be treated.

Recommendation: If the process is well-designed, consideration could be given to establishing an Online Safety Advisory Panel, comprising of experts and industry representatives (similar to the Classification Advisory Panel currently being considered in the context of the Stage 2 NCS reforms). It would not be a decision-making body, but would advise the government on online safety trends, informed by an evidence-based and

community considered approach. It would be independent of the regulator, with support resources provided by ACMA. Such a body should include representation from civil society organisations or human rights groups to ensure due process considerations are factored in.

5.5 *Q25. To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?*

See our response to Question 23.

5.6 *Q26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?*

As a matter of good policy design and best regulatory practice, human rights principles are considered in any piece of legislation that is made in Australia.[39] The OSA has been no different.

Despite this, there are areas where good regulatory practice principles should be encapsulated in how the OSA is implemented in practice. This includes ensuring providing an opportunity for a right to a fair hearing, protection of civil liberties including freedom of speech, privacy and security, and respecting different value systems of other countries.

For example, consideration of PTM opens up conversations as to who determines what is considered to be PTM, which may differ between jurisdictions, and consideration of the age assurance technology trial opens up questions about adequately protecting privacy and security.

We discuss these issues in response to other questions in this submission.

[39] https://www.alrc.gov.au/publication/traditional-rights-and-freedoms-encroachments-by-commonwealth-laws-alrc-report-129/3-scrutiny-mechanisms/policy-development-and-legislative-drafting-2/.

6. Regulating the online environment, technology and environmental changes

6.1 Q27. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?

In practice, it has been unclear how service providers would be addressing issues such as pro-terror material (PTM) without understanding the context and treatment of the content, who determines what is deemed to be terror-related, and whether they are targeting individuals or groups.

Questions are also raised as to whether this would be over-stepping into the domain of national security for targeting particular groups, which may arguably be outside the scope of online safety.

It is also not clear what groups are being defined or categorised here.

Recommendation: Further information is needed to understand how groups would be defined and targeted by eSafety. Consideration will need to be given to the context and treatment of the content, and governance around who is authorised to determine the targeted groups.

6.2 Q28. What considerations are important in balancing innovation, privacy, security, and safety?

We are cautious around the language of "balance" as this infers that some level of privacy, security and safety in particular (innovation is another matter) would need to be sacrificed in order to give some legitimacy over another particular area. For instance, if regulatory measures and obligations were introduced to promote online safety at the expense of another, it suggests that more has not been done to rigorously explore options to avoid such conflicts from arising. In other words, this should not be a balancing exercise or a zero-sum game.

These issues have already arisen in relation to addressing PTM, technical feasibility provisions for enabling access to encrypted communications, and age assurance. This leads to a discussion about providing appropriate safeguards in regulator accountability, which we discuss in Question 23 above.

Recommendation: As a general rule of good public policy design and best regulatory practice, regulatory measures and obligations proposed to promote online safety should not be introduced if it infringes upon privacy and security.

6.3 Q29. Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?

Future-proofed and fit-for-purpose legislation should be technology neutral. While generative AI and deepfakes (and even recommender systems) are popular topics at the moment, the online safety framework should be sufficiently flexible to address these and other emerging technologies, without needing legislation and regulatory instruments to be continually updated to specify certain technologies. Otherwise, this would create an unstable regulatory regime that would be difficult for both regulators and stakeholders to effectively respond to.

Additionally, Safety-By-Design is already built into the role of eSafety, regulatory measures and other activities.

Therefore, as a matter of good policy design, the OSA should be technology neutral.

Recommendation: As a general rule of good public policy design and best regulatory practice, regulatory measures and obligations proposed to promote online safety should be technology neutral, as well as technically feasible.

6.3 *Q30. To what extent is the Act achieving its object of improving and promoting online safety for Australians?*

Establishing eSafety to promote online safety is important in Australia. For example, undertaking research and educating the community on online safety, and working with industry and other stakeholders to deliver its objectives. See Questions 16 and 24.

Regarding Australia's international engagement on online safety, we discuss this in Question 21.

6.4 *Q31. What features of the Act are working well, or should be expanded?*

The intent of the OSA should be to provide an overarching online safety framework to ensure alignment and coordination between the various regulatory instruments and their development and operation in practice to address online safety objectives. However, we have discussed throughout this submission where improvements can be made to the OSA (as opposed to creating new regulatory obligations and measures).

6.5 *Q32. Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?*

Throughout this submission, we have discussed good governance measures to enable transparency and accountability. For example, see Questions 5, 15, 17, 23, 24, 26 and 28.

6.6 *Q33. Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?*

We consider that it would be more appropriate to provide sufficient funding to industry stakeholders that are required to develop industry online safety codes under the OSA. There are also other costs of compliance in meeting the multiple obligations under the online safety framework in Australia. In contrast, we understand that eSafety spends around $50m per annum for its various regulatory and non-regulatory activities, which are subject to government funding and scrutiny.[40]

As a general comment, we would be concerned if eSafety was afforded with a cost recovery mechanism from service providers, especially if this could lead to unintended and perverse consequences. These may include:

- Barrier to access regulatory services: For example, in the context of classification, it has been recognised that services costs to seek a review of decisions by the Classification Board creates a barrier for businesses to explore that avenue.
- Proportionality: For any regulation, there is usually a disproportionate burden placed on smaller companies compared to larger ones. There is also the cumulative effect of introducing a new government cost recovery mechanism in addition to existing regulatory costs, which makes it more difficult to attract investment in Australia compared to other jurisdictions.

[40] Portfolio Budget Statements 2024–25, p. 122, https://www.infrastructure.gov.au/sites/default/files/documents/2024-25_infra_pbs_00.pdf; Portfolio Budget Statements 2023-24, p. 156, https://www.infrastructure.gov.au/sites/default/files/documents/2023-24_infra_pbs_00.pdf.

- Accountability: How will eSafety be held accountable to maintain efficient costs and expenditure? Without government funding, there would be less incentive for government to scrutinise whether the regulator's expenses are being appropriately used in public interests.

Recommendations:

- **As a matter of good public policy design and best regulatory practice, allowing for eSafety to cost recover for its activities from online service providers raises significant concerns with respect to barrier to access regulatory services, and proportionality and accountability issues, which could lead to unintended and perverse consequences.**
- **Consideration should be given to public funding of bodies such as industry associations to develop industry online safety codes, which is currently unaccounted for.**

Thank you for allowing IGEA to contribute to the Department's consultation on the OSA Review. For more information on any issues raised in this submission, please contact us at [redacted].

Appendix A: Review of BOSE Amendment Determination against IGEA's recommendations

In IGEA's submission to the Department's BOSE Amendment Determination consultation, we offered several recommendations that we consider should be addressed or reconsidered as part of the OSA Review.[41]

Topic	IGEA Recommendations	Outcome and IGEA response
General	Avoid duplicating and conflicting requirements, and over-prescriptiveness and regulatory overreach: Consideration be given to rejecting certain proposed amendments to the BOSE Determination, where the requirements could lead to: duplication or conflict with requirements under the relevant online safety codes or standards (i.e. existing, under development or planned); over-prescriptiveness and inflexibility; or regulatory overreach. Defer to Online Safety Act Review: Consideration be given to deferring certain proposed amendments to the BOSE Determination, where new requirements would: not be covered under any online safety codes or standards; have a material impact on service providers (i.e. existing, under development or planned); and be better served as part of the forthcoming Online Safety Act review. Guidance material: Guidance material be produced to explain the scope and interoperability between the online safety regulatory requirements in practice for service providers i.e. how the online safety codes and standards, and BOSE Determination will operate together. Further consultation: We would welcome the opportunity to discuss further with the Department to understand the intent underlying the application of the BOSE Determination, alongside the online safety codes and standards that apply to online video game services.	We maintain that our recommendations to the BOSE Amendment Determination consultation should also apply to the OSA Review.

[41] IGEA submission to Draft Online Safety (Basic Online Safety Expectations) Amendment Determination 2023 (February 2024), https://igea.net/2024/02/igea-submission-to-draft-online-safety-basic-online-safety-expectations-amendment-determination-2023/.

Topic	**IGEA Recommendations**	**Outcome and IGEA response**
Generative AI capabilities	The proposed express inclusion of generative AI in the BOSE Determination runs counter to the overall technology-neutral approach of the BOSE. To enable a more holistic and coordinated approach to generative AI, we would recommend this be deferred to the broader Australian Government safe and responsible AI consultation.	Despite our reservations, the final version of the BOSE Amendment Determination includes generative AI under section 8A "Additional expectations—provider will take reasonable steps regarding generative artificial intelligence capabilities". We raise this issue in our discussion about technology neutrality in this OSA Review submission.
Unlawful or harmful material	Further clarification is required on the scope of "harmful material" throughout the BOSE Determination – in its current form, the term is extremely broad and ambiguous to interpret and comply in practice. Alternatively, consideration could be given to replacing references to "unlawful or harmful material" with "Class 1A and 1B material", which would be more aligned with the online safety codes and standards.	It is not clear that this issue has been addressed in the final version of the BOSE Amendment Determination. We recommend that this be resolved as part of the guidance material.
Recommender systems	To enable a more holistic and coordinated approach to recommender systems, we would suggest this be deferred to the broader Online Safety Act review. Should the Department wish to proceed with inclusion of recommender systems requirements in the BOSE Determination, the new requirement should enable sufficient flexibility for the service provider to demonstrate reasonable steps have been undertaken.	Despite our reservations, the final version includes a provision for recommender systems under section 8B "Additional expectations—provider will take reasonable steps regarding recommender systems". We raise this issue in our discussion about technology neutrality in this OSA Review submission.
User management and control	Where a service provider relies on an established user management and control system via a third party service provider that is already subject to the BOSE Determination or relevant online safety standard or code, this should be considered a reasonable step.	It is not clear that this has been addressed. We recommend that this be resolved as part of the guidance material.
Best interests of the child	With respect to the proposal for service providers to take reasonable steps to ensure the best interests of the child, this should be referring to the design and operation of any service that is "targeted at children" (as opposed to "used by, or accessible to, children"). The proposed introduction of a "reasonable step" example "to ensure	With respect to the Department's BOSE Determination proposal for service providers to take reasonable steps to ensure the best interests of the child, this should be referring to the design and operation of any service that is '**targeted at, or directed to, children**' (as opposed to '**likely to be used by, or accessible to, children**'). Similar terminology has been used overseas in legislation (e.g. US federal statute COPPA) which industry

Topic	IGEA Recommendations	Outcome and IGEA response
	that technological and other measures are in effect to prevent access by children to Class 2 material" by "implementing appropriate age assurance mechanisms", is out of scope and should not be included in the BOSE Determination consultation. For similar reasons, the proposed introduction of a "reasonable step" example "to ensure that technological and other measures are in effect to prevent access by children to Class 2 material" by "continually seeking to develop, support or source, and implement improved technologies and processes for preventing access by children to class 2 material", is also out of scope and should not be included in the BOSE Determination consultation.	considers to be unambiguous.[42] In contrast, the 'likely to be used by, or accessible to' terminology is still vague and potentially broad in meaning. Despite our concerns, the government decided to proceed with term "likely to be accessed by children". The Explanatory Statement to the BOSE Amendment Determination indicates that the term "likely to be accessed by children" establishes a standard and threshold that is intended to align with the UK Information Commissioner's Age Appropriate Design Code, "making it simpler for services to assess whether or to what extent the expectation applies to them". However, we maintain our view that this term is problematic and have raised this issue in this OSA Review submission.
Safety impacts of business and resourcing decisions	Any proposed obligations on service providers to share information with eSafety should ensure the regulator implements appropriate safeguards in managing such information in accordance with due process, transparency, confidentiality, and privacy. With respect to the safety impacts of business and resourcing decisions, we strongly caution against including a provision for this in the BOSE Determination. It sets a dangerous precedent for the regulator to seek information about sensitive commercial business decisions (including staff resourcing and investments) and the potential subsequent misuse or misrepresentation of that information to draw a causal link to online safety issues. Regarding the proposed inclusion of a reasonable step example relating to service providers "investing in systems, tools, and processes to improve the prevention and detection of material or activity on the service that is unlawful or harmful", the Determination should	Despite our reservations, the government still proceeded with their amendments. We maintain our view that safeguards need to be introduced and addressing regulatory duplication, which we discuss in this OSA Review submission.

[42] https://www.law.cornell.edu/uscode/text/15/6501.

Topic	IGEA Recommendations	Outcome and IGEA response
	either directly refer to the RES Standard or remove this requirement as it is already being considered as part of the RES Standard.	
Hate speech	The proposed inclusion of a reasonable step that requires the implementation of processes for detecting and addressing hate speech has its practical limitations if it relates to managing hate speech delivered orally (as opposed to in written form), due to limitations in technology. Therefore, inclusion of this reasonable step needs to be reviewed to ensure technical feasibility or otherwise be deferred for further consideration as part of the Online Safety Act review.	While not explicitly addressing our issue, the government decided to remove the definition of hate speech, "due to concerns about imposition on free speech, but included in the Explanatory Statement so that guidance could be given outside of the legislative context. Minor revisions were also made to improve clarity and flexibility."
Additional transparency reporting	Transparency reporting is a subject currently under consideration as part of the RES Standard consultation by eSafety, including issues relating to duplicated reporting requirements, and therefore not appropriate for additional consideration as part of the BOSE Determination.	The Government has accepted feedback that there were excessive reporting requirements. As it states in its Explanatory Statement: *The most significant revision following consultation was scaling down the publication of regular transparency reports from an 'additional expectation' to an 'example of a reasonable step' to ensure safe use of a service, due to industry concerns about efficacy relative to impost.* While we welcome this amendment, we would like to see streamlining of regulatory obligations reflected more broadly across the other instruments under the OSA.
Enforcement of terms of use	Terms of use, and end-user complaints and reporting mechanisms are currently under consideration as part of the RES Standard consultation by eSafety, and therefore not appropriate for additional consideration as part of the BOSE Determination.	Despite our reservations, the government has decided to move ahead with consideration of terms of use in the BOSE Determination. We maintain our view that terms of use is being considered in multiple instruments and this OSA Review submission discusses terms of use.