IGEA

interactive games & entertainment association

Submission to the Department of Communications and the Arts

Response to Online Safety Legislative Reform Discussion Paper

February 2020

Interactive Games & Entertainment Association

Introduction

The Interactive Games & Entertainment Association (IGEA) is the peak industry association representing the business and public policy interests of Australian and New Zealand companies in the interactive games industry. Our members publish, market, develop and distribute interactive games and entertainment content and related hardware.

IGEA welcomes the opportunity to provides its views on the proposed new online safety legislative model. Our industry shares the Government's policy priority of keeping Australians, and especially Australian children, safe while exploring, enjoying and learning through the online world. We will continue to contribute to policy discussions on this important topic, just as we have participated in previous consultations on the development of the current Enhancing Online Safety Act (the Act), the 2018 Briggs Review, the Online Safety Charter, the Safety by Design framework and the concurrent consultation on the review of the National Classification Scheme. We also sit on the eSafety Commissioner's Online Safety Consultative Working Group.

We are pleased to provide this submission on the proposed direction of new legislation and would be pleased to talk through any points that are raised in our response during or following the consultation process. Given the high-level nature of the discussion paper and the significant scale of the proposed reforms, we anticipate further discussions will be needed following this consultation process, including on precise legislative design and exposure draft legislation. We look forward to these discussions throughout 2020.

Riot Games, creators of League of Legends, one of the most popular games of all time, launched its 'Learn With League' initiative in 2019 in collaboration with education and cyber safety partners in Australia and New Zealand to promote positive and productive behaviours and digital skills

Background and context

The social impact of online gaming

While online video gaming may still sometimes be regarded by some in government and the media as a relative 'new' phenomenon, as of 2020 we are entering the fourth decade in which this social activity has existed. For 14 years IGEA has conducted research into game-playing in the community, making our research the longest running such series of research in the world. Our latest research conducted in 2018 found that the average age of an Australian game player is 34 years old and that over three quarters of Australian players are adults, not children or teenagers. Australians who play games are also almost as likely to be female as male. 42 per cent of Australians aged 65 and over play video games, with older Australians amongst the fastest growing cohort of game players. Our full Digital Australia 2020 research can be found here.

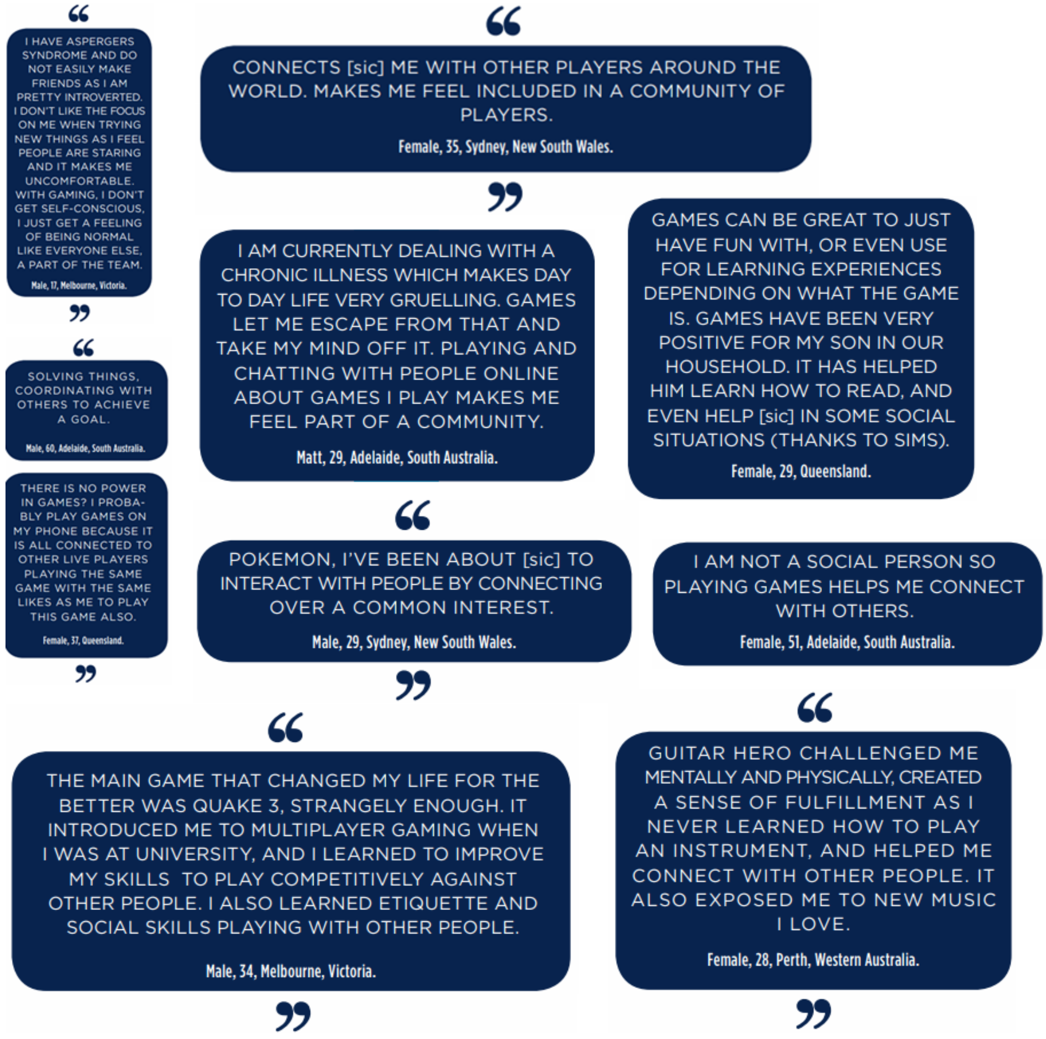
One of the reasons why video games are so popular is the diversity of our medium. Games come in all shapes and sizes, from aesthetic mindfulness games for relaxing, to brainteasing puzzle games that a person can 'snack' on while commuting on a bus, to highly thoughtful games where a person can build worlds and multiplayer game where friends and family members can spend time together. An important contributor to the popularity of games is their power for connectivity and social inclusion. Our Digital Australia research has told us so much about how games have helped families to connect with each other, with 43 per cent of parents playing online games with their children.

A quarter of adult gamers said that they play online games with their partners and a quarter also said that they played games with their friends online. Our research tells us many stories about how games provided people with a way to help them bond with their families, while others told us how games literally were the only way in which they could spend quality time with far-away friends and family. Critically to this consultation, while many games allow some degree of interactivity or communication with other players, this interactivity is always highly limited and secondary to the playing of the game itself.

While video games are generally regarded as entertainment products, they also play a far more complex cultural and social role in the community and, increasingly, a tool for wellbeing. According to our research, while fun is still the most important reason why Australians play games, Australians also play games to reduce stress and – particularly for older Australians – to keep their minds sharp. Most people we surveyed also believed that games can help to improve thinking, dexterity and pain management. Government and the health and education sectors are increasingly recognising the broader application of games for 'serious' purposes. Examples of Australian-made 'serious' games include:

- *Sound Scouts*, a game to aid the process of detecting hearing difficulties in young children which has received $4 million in Australian Government funding for a national rollout.

- *ReachOut Orb* by SMG Studio for the youth mental health organisation ReachOut to teach Australian students about wellbeing.
- *Smartstep*, a step-based game developed by Neuroscience Research Australia to assist people with MS strengthen their balance and agility.
- *Bring Back The Beat*, a game developed by 3rd Sense for Cochlear to encourage young implant users to test their devices in fun ways.
- *Bleached Az*, a game developed by Chaos Theory Games to promote ocean health awareness and conservation – with 20 per cent of in-game revenue going towards combating global warming.



I HAVE ASPERGERS SYNDROME AND DO NOT EASILY MAKE FRIENDS AS I AM PRETTY INTROVERTED. I DON'T LIKE THE FOCUS ON ME WHEN TRYING NEW THINGS AS I FEEL PEOPLE ARE STARING AND IT MAKES ME UNCOMFORTABLE. WITH GAMING, I DON'T GET SELF-CONSCIOUS, I JUST GET A FEELING OF BEING NORMAL LIKE EVERYONE ELSE, A PART OF THE TEAM.

Male, 17, Melbourne, Victoria.

CONNECTS [sic] ME WITH OTHER PLAYERS AROUND THE WORLD. MAKES ME FEEL INCLUDED IN A COMMUNITY OF PLAYERS.

Female, 35, Sydney, New South Wales.

SOLVING THINGS, COORDINATING WITH OTHERS TO ACHIEVE A GOAL.

Male, 60, Adelaide, South Australia.

THERE IS NO POWER IN GAMES? I PROBABLY PLAY GAMES ON MY PHONE BECAUSE IT IS ALL CONNECTED TO OTHER LIVE PLAYERS PLAYING THE SAME GAME WITH THE SAME LIKES AS ME TO PLAY THIS GAME ALSO.

Female, 37, Queensland.

I AM CURRENTLY DEALING WITH A CHRONIC ILLNESS WHICH MAKES DAY TO DAY LIFE VERY GRUELLING. GAMES LET ME ESCAPE FROM THAT AND TAKE MY MIND OFF IT. PLAYING AND CHATTING WITH PEOPLE ONLINE ABOUT GAMES I PLAY MAKES ME FEEL PART OF A COMMUNITY.

Matt, 29, Adelaide, South Australia.

GAMES CAN BE GREAT TO JUST HAVE FUN WITH, OR EVEN USE FOR LEARNING EXPERIENCES DEPENDING ON WHAT THE GAME IS. GAMES HAVE BEEN VERY POSITIVE FOR MY SON IN OUR HOUSEHOLD. IT HAS HELPED HIM LEARN HOW TO READ, AND EVEN HELP [sic] IN SOME SOCIAL SITUATIONS (THANKS TO SIMS).

Female, 29, Queensland.

POKEMON, I'VE BEEN ABOUT [sic] TO INTERACT WITH PEOPLE BY CONNECTING OVER A COMMON INTEREST.

Male, 29, Sydney, New South Wales.

I AM NOT A SOCIAL PERSON SO PLAYING GAMES HELPS ME CONNECT WITH OTHERS.

Female, 51, Adelaide, South Australia.

THE MAIN GAME THAT CHANGED MY LIFE FOR THE BETTER WAS QUAKE 3, STRANGELY ENOUGH. IT INTRODUCED ME TO MULTIPLAYER GAMING WHEN I WAS AT UNIVERSITY, AND I LEARNED TO IMPROVE MY SKILLS TO PLAY COMPETITIVELY AGAINST OTHER PEOPLE. I ALSO LEARNED ETIQUETTE AND SOCIAL SKILLS PLAYING WITH OTHER PEOPLE.

Male, 34, Melbourne, Victoria.

GUITAR HERO CHALLENGED ME MENTALLY AND PHYSICALLY, CREATED A SENSE OF FULFILLMENT AS I NEVER LEARNED HOW TO PLAY AN INSTRUMENT, AND HELPED ME CONNECT WITH OTHER PEOPLE. IT ALSO EXPOSED ME TO NEW MUSIC I LOVE.

Female, 28, Perth, Western Australia.

Some of the personal stories written by Australian respondents and provided to IGEA for our Digital Australia 2020 research project

Commitment to online safety

To help inform the broader context to our submission and our industry's views, we have provided some information about the current video gaming environment and how it is one of the safest ways that Australians are spending their time online. Much of the following summary has already been provided to the Government in our submission to the consultation on the Online Safety Charter and other prior submissions, but we consider it important to also include it in this response. We have also updated our advice with new initiatives, given the significant resources that are invested by the industry every day to continually make online gaming as safe as it is enjoyable for the community.

The video games industry takes its obligation to protect game players seriously and its priority is to ensure that games provide both a fun and safe space for children and adults alike. It achieves this objective through a multi-level approach involving strong compliance with the National Classification Scheme, implementing safety features directly on the consoles and devices where people play games, providing further targeted safety features within games themselves and engaging with broader cultural, education and awareness-raising campaigns directed at the public, gaming community, children and their parents and guardians – including by direct engagement and listening to the community. These are addressed in turn.

National Classification Scheme

First, unlike most other kinds of digital content, video games are already subject to very precise and thorough regulation under the National Classification Scheme (NCS), a cooperative arrangement between the Australian Government and state and territory governments where video games must be classified by the Classification Board, an independent government body, before they can be made available to the public. Since the start of the NCS in 1995, Australian video games publishers have maintained a policy of strict compliance to ensure that games that are bought and played in Australia have been appropriately classified. Just as importantly, the requirements of the NCS and corresponding ratings systems all around the world already play a key role in shaping the content of games and help to drive how games are designed, developed, distributed and marketed.

Under the NCS, video games are classified against six classifiable elements - violence, sex, nudity, drug use, coarse language and themes – and assigned a classification ranging from G (General) to R18+ (Restricted to persons aged 18 and above). The Classification Board also has the discretion to assign specific consumer advice, or warnings, that must be displayed with the classification category on a game. The Board has absolute discretion to provide any consumer advice it considers appropriate and, relevantly, currently provides consumer advice of “online interactivity” on games that allow players to interact with others online so that parents and guardians are aware of this.

Other ratings systems overseas even make “online interactivity” a formal aspect of the ratings process, such as the ESRB in the United States, an approach that could be considered here and may be raised for discussion under the current review of the NCS. However, while included in the formal application for classification, it is not tied to a specific (or predetermined) level of classification. The inclusion of ‘online activity’ does not in itself determine the level of classification. In effect, similarly to Australia, this is a feature descriptor and not a classification determinant.

We have also worked in partnership with the Australian Government to ensure that there is an effective tool to classify digitally distributed games, which includes online and mobile games. The International Age Ratings Coalition (IARC) classification tool was built by the video games industry in collaboration with government and non-government ratings agencies around the world and has now been rolled out on Google Play, the Microsoft Windows and Xbox stores, the Nintendo eShop, Electronic Arts' Origin and the Oculus store, with the implementation of IARC on the PlayStation Store currently rolling out across regions.

Hundreds of thousands of games, if not millions, have now been classified by the IARC tool, as well as countless non-game apps on Google Play. In addition to implementing IARC on the Google Play Store, Google Play also allows parents and guardians to restrict what content can be downloaded or purchased from Google Play based on maturity level. Please see here for more information on the IARC classification tool.

Safety features on consoles and devices

All of the major video game consoles and devices provide a range of safety features to provide a safe environment for game players and their families – many of which are world leading and unique to the games industry.

Features of the Microsoft Xbox One console include:

- Creating family and family accounts with special privacy and online safety settings
- Setting screen limits for children on Xbox and PC, including for both games and shows
- Setting age limits for content by choosing from preset recommendations by age
- Blocking inappropriate websites through a web filter
- Using customisable text filters for Xbox messages, with the highest level of filtering set as default for child accounts
- Preventing unauthorised purchases by children, including through the use of a passkey
- Functionality to mute or block other players
- Setting standards and expectations through the Microsoft Services Agreement and Code of Conduct and ability to report other players for violations
- Safety and wellbeing resources including access to a free 24/7 Crisis Text Line
- Ability to hide and filter activity feed posts

Features of the Nintendo Switch device include:

- A Nintendo Switch Parental Controls smart device app to provide parents and guardians easy access to parental controls
- Download, content and console feature restrictions that can be set by choosing from three pre-set categories or by adjusting settings separately
- Time limits, cut-off times, alarms and a 'suspend software' feature
- Ability for parents and guardians to see what games their children have been playing and for how long, as well as monthly play reports
- Ability to prevent children from playing games that are inappropriate for their age, based on age ratings
- Ability to restrict communication with users or the posting of screenshots of games to social media services
- Option for Nintendo eShop to prevent game purchases by children

Features of the Sony PlayStation 4 console include:

- "Family on PSN" settings to customise account restrictions for individual family members, parental controls and spending limits
- "Play Time" controls to give parent and guardians the ability to set limits on when during the day and for how long children can access the system
- Setting age rating levels for games as well as for Blu-ray and DVDs
- Setting monthly spending limits
- Restricting access to network features, such as disabling access to communicating with other players or viewing content created by others
- Disabling child access to the Internet Browser or PlayStation VR headset
- Availability of a PlayStation App to make it easier to customise parental settings

Microsoft, Nintendo and Sony all provide clear, transparent and easy-to-find information on their safety features and parental controls through their Australian websites: Microsoft, Nintendo and Sony.

Safety features within games

Most games with a communications functionality use a range of measures to combat the risk of coarse language or the harassment of players. As previously mentioned, unlike other digital platforms like social media and messaging services, communication is always an ancillary function to gameplay itself and more heavy-handed approaches to filter or block inappropriate communications are often the norm. The limited functionality of communication in games means that risks in community behaviour are easier to address, safety can remain uncompromised and the enforcement of community harms like language and abuse can be efficient and effective.

Some examples of safety features that have been deployed in games include:

- Strong community codes of conduct and terms of service (eg. EA Play by Fair rules)

- Pre-emptive profanity filters in text chat (eg. *Battlefield V*)
- Pre-emptive prevention of personal information being posted (eg. *Roblox*)
- Providing automated feedback after profane language (eg. *Rainbow Six Siege*)
- Various options for muting other players in a game (eg. *Red Dead Redemption*)
- Ability to customise or turn off graphic content (*eg. Call of Duty: Modern Warfare)*
- Ability for gamers to report other players (eg. *StarCraft II*)
- Enforcement and penalties including the suspension or banning of users (eg. *FIFA 19*)
- Endorsement systems to encourage positive gamer behaviour (eg. *Overwatch*)
- Disciplinary systems to discourage negative gamer behaviour (eg. *League of Legends*)

Industry advocacy, awareness-raising and collaboration

The video games industry has taken a proactive approach to raising awareness and education around parental controls and responsible gaming. Our website provides information on parental controls and will always support other organisations in Australia that help to promote the use of these controls. IGEA has previously published videos educating parents about gaming and also support the www.askaboutgames.com resource and parents' guides developed by our global industry counterparts. Together with our fellow industry associations from around the world, we have established www.healthyvideogaming.com which provides a portal to guidance for parents and guardians for safety features and controls that they can use on the most popular platforms. The portal also provides our perspective on other issues like screen time and healthy gaming. Our website, and many of the websites of our members also provide links to external resources, including the Office of the eSafety Commissioner's online resources.

Through our bi-annual Digital Australia report, we regularly conduct research with players, parents and guardians that helps to identify contemporary issues that are of most concern in the media, including in games. We work hand-in-hand with Bond University to undertake this research to ensure that it is robust, balanced and consistently-conducted so that we can track changes in perception over time. The results of our research are provided to our members to help them appreciate and address risks and opportunities with online safety in their games. We particularly recognise the importance of parents and guardians monitoring and playing games with their children. We encourage this type of play and are pleased that families are increasingly enjoying gaming together and taking control of their online safety. Our Digital Australia 2020 research found that:

- 59 per cent of parents play with their children in the same room
- 43 per cent of parents play online games with their children

- 81 per cent of parents are familiar with family controls on game systems, with 54 per cent completely or mostly familiar, and
- 83 per cent of parents have talked with a child about playing safely online.

In addition to the IARC classification tool as an example of industry leadership, many of the largest video game companies in the world, including the parent companies of many IGEA members, work together with other stakeholders in a variety of forums to share best practices and learnings. One such group is the Fair Play Alliance, where gaming professionals and companies committed exchange learnings on methods to encourage healthy and positive communities and player interactions in online gaming.

By way of further example, Electronic Arts (EA), a key member of IGEA, runs the Building Healthy Communities Program. This program establishes a Player Council which, in turn, provides ongoing feedback to inform EA programs, policies and suggestions but also supplies additional avenues for community feedback. In partnership with players, EA develops new anti-toxicity tools and in-game features to more easily manage and effectively report disruptive behaviour across its services. Through keeping their player community informed on a quarterly basis, new initiatives are communicated and toxicity is mitigated.

The video games industry is also implementing steps to ensure esports, one of the fastest growing sectors in the video games industry, prioritises its responsibility for safeguarding its participants and its viewers. Together with our international counterparts, we have established the Universal Principles for Fun & Fair Play which outlines four core values applicable in all aspects of the global esports environment: safety and well-being, integrity and fair play, respect and diversity, and positive and enriching game play.

A Nintendo how-to guide for parental controls on the Nintendo Switch console, published in five languages with a combined total of over 48 million views on YouTube.

Response to discussion questions: Basic online safety expectations

IGEA recognises that policy should always be an evolving process and supports well-designed, evidence-based reforms. Some of the proposals, such as the greater use of industry codes and expansion of the eSafety Commissioner's powers, would naturally have an impact on our industry. In this submission we have tried to provide comprehensive responses to the discussion questions that are relevant to us to assist the Department in taking a well-informed and balance perspective as it designs the future online safety legislative scheme. In particular, we have tried to focus our commentary around the proposed policy approaches on where we see the greatest opportunities for benefit but also where we anticipate potential practical challenges in implementation or where we consider a particular policy direction could be better informed. In some of our responses to the reform options, we have also highlighted policy or regulatory issues where we consider more information is needed for industry before implementation can occur.

However, in saying that, it would be remiss not to highlight that the discussion paper has not provided compelling evidence to suggest that there is a problem with video games that would warrant increased regulatory intervention. The only 'evidence' we can see offered up in the Discussion Paper is that 'research into youth and gaming found that 17 per cent of multiple player gamers experienced in-game bullying.'

While this statement acknowledges that a minority of players have had an experience that they consider to be 'bullying' (though we aren't clear on how that is defined in the survey), it fails to address if any of these players took advantage of the tools immediately available to them in-game and, if so, whether the matter resolved. In fact, it wasn't clear from the evidence if there was a feeling that the experience was even serious enough to warrant the need for regulatory intervention.

Like most competitive sports, online gaming can at times be adversarial by nature. When highlighting that there has been an experience of bullying, we need to consider the context of the game and determine if the reported behaviour is actually bullying, menacing, harassing or offensive conduct, or (as mentioned in this paper), conduct that would fall outside these areas of concern such as "colourful language, 'trash-talking', verbalised frustrations and sometimes arguments between players".

If a new policy setting is required, is this because of a proven and demonstrable failure of the industry? Does the reported 17% level make video games stand out from other environments in the 'real world' where similar (or perhaps even greater) levels of competition and potential 'bullying' exist?

Question 3. Is there merit in the BOSE concept?

Question 4. Are there matters (other than those canvassed in the Charter) that should be considered for the BOSE? Are there any matters in the Charter that should not be part of the BOSE?

We note from the discussion paper and the BOSE fact sheet that it is intended to apply to social media services only. However, we also acknowledge that under this proposal, the eSafety Commissioner would have a power to determine that expectations apply to other specified type of service providers in the future, which could include a wider range of digital companies. While we note that video games would not be covered by the default scope of the BOSE under this proposal, given that the eSafety Commissioner has the power to expand this scope we wish to take this opportunity to provide some commentary on this conceptual idea.

While the BOSE could be a helpful concept in principle, we respectfully note that it is the third similar 'expectations-setting' online safety concept that the Government has announced in the past 12 months, following the Online Safety Charter and the Safety by Design guidelines, and we raise for discussion whether there is some potential risk of duplication. For example, the discussion paper states that the BOSE might use the Online Safety Charter as a basis, raising the question of whether two separate documents with such similar purposes is necessary or helpful. Despite some commentary in the discussion paper and fact sheet seeking to explain the inter-relationship between the three concepts, from our perspective there is still some lack of clarity about their roles and some likely duplication of scope and purpose. More critically, there is potential for confusion among industry, both in Australia and abroad. For example, we are aware that the Online Safety Charter and Safety by Design framework were drafted separately, which led to some inconsistencies that we have addressed in our feedback on both.

An alternative approach that may help to address these risks would be to consolidate or at least streamline the three concepts into a single cohesive framework. This would help to ensure that the Government's expectations and messaging are unified and easily communicable to the broader range of stakeholders that the Government is hoping to influence. This single concept could potentially comprise high level expectations set by the Minister followed by some more articulated guidance maintained by the Department or the eSafety Commissioner that would give the Minister's expectations clarity, updated as needed. While this would be a departure from the current approach, it may provide a simpler and more supportive model of Government leadership and industry responsibility.

Should the current proposed approach be retained, we hope that any future BOSE will take a flexible, principles-based approach, noting that there is no single digital industry or archetype digital business, platform or service in Australia or around the world. Rather, technology firms come in all shapes and sizes, from global multinationals that employ tens of thousands of people around the world managing multiple products, to Australian start-ups with a handful of workers. As a result, we do not consider that a 'one size fits all' approach is possible when promoting online safety and in fact, advice that is appropriate for one sub-sector may be inappropriate for another given their vastly different products and service. Following the previous consultation on the Online Safety Charter, we note that the charter was amended to recognise that it is not intended to have universal application to everyone equally, recognising differences in both services and scale. It would seem consistent (and logical) in that case, that this approach should also apply to the proposed BOSE.

Subject to the views above and below, we do not have any particular views on what a potential BOSE should or should not include initially, but welcome assessing in detail any future drafts. However, we are aware that the discussion paper includes discussion around an expectation that online service providers making online apps, games and services marketed to children default to the most restrictive privacy and safety settings at initial use or set-up. The paper also notes that the Government is considering giving the eSafety Commissioner powers to specify certain services that must default to the most restrictive and safety settings. We are not aware of any other territory that has considered this approach so if there is consideration of including this expectation in any future BOSE, we believe that it requires further analysis and dialogue with industry, in particular around the evidence-base for this proposal and to identify its full impacts and specific implications.

The idea of defaulting to the most restrictive privacy and safety settings seems like an uncontroversial idea in principle, and indeed many services, devices and games already have defaults for child settings. However, it is also a very difficult principle to define and one that has the potential to cause confusion among industry. For example, does ‘children’ in this context mean young people, or anyone under the age of 18?

The standard established in the United States by The Children's Online Privacy Protection Act (COPPA) is 13 years of age. If similar regulations were to be introduced in Australia, the COPPA standard should be considered since it has been in place for many years, works well, is regularly reviewed, is regularly enforced, and most multinational companies have already built systems to comply with the COPPA requirements.

Further, is a product “marketed to children” if it has broad demographic appeal, or is marketed to adults but also has popular among children? Like COPPA, any requirement should be clear that it applies only to sites and services where children are the targeted or primary audience rather than general or mixed audience sites that may include some children. Whether children are the primary audience may be determined based on factors, including whether children are the intended or actual audience and various aspects of subject matter, including the content, language and activities.

Furthermore, under a technical implementation of this requirement, would a digital platform like a game that offers both offline and online modes be required to disable the online mode by default? Finally, our sector has been innovative in often proving a rich range of privacy and safety modes in games, consoles and advices, allowing easy and significant control of customisation. One of the unintended consequences of a rigid ‘default’ expectation could be the reduction in the range of options that are available if the most restrictive setting is one that does not make the game playable or practical for most.

Question 5. What factors should be considered by the eSafety Commissioner in determining particular entities that are required to adhere to transparency reporting requirements (e.g. size, number of Australian users, history of upheld complaints)?

One of the difficulties of responding to this question is that the BOSE has not been drafted yet, so the precise details are unknown. It is therefore unclear how broad the expectations or how detailed the transparency reporting requirements might be. We would recommend consulting again on this question once there is greater clarity around the BOSE concept, should it proceed. At the outset, however, we note that depending on what is encompassed in a proposed BOSE, the transparency reporting requirements might impose a very onerous burden and a significant technical challenge for implementation, particularly for smaller platforms and service providers.

For example, some such smaller service providers may not even collect the data that would be subject to reporting or even be in a position to collect the data from a technical perspective, notwithstanding that they have online safety policies and resources in place. Furthermore, we note that some service providers might not even know the location of their users, such as which users are Australian, or keep chat logs, including for privacy reasons. The factors that should be considered by the eSafety Commissioner should certainly include size and number of Australians, but also the type of service, demonstrated level of online safety risk, what controls are already in place and reasonable practicability of compliance.

A decision by the eSafety Commissioner to determine that particular entities must adhere to transparency reporting should not be taken lightly. It would be a significant requirement and one that we are not aware that any other regulator in the world currently has the power (or will) to impose. The fact that the requirement is not technically enforceable does not take away from the burden of the expectation, especially given that the Government may still 'name and shame' businesses. Nor is it a compelling rationale to implement policy that sets an expectation that would otherwise be considered unreasonable but for the fact that there are no pecuniary penalties for non-compliance. The transparency reporting requirements should be a measure of last resort and after there has been a demonstrated history of upheld complaints to the eSafety Commissioner, with the business afforded reasonable opportunity to explain and/or remedy any perceived deficiencies.

Question 6. Should there be sanctions for companies that fail to meet the BOSE, beyond the proposed reporting and publication arrangements?

As outlined in our response to question 5 above, a decision by the eSafety Commissioner to determine that particular entities must adhere to transparency reporting is a very significant decision with major consequences, including potential negative impacts on reputation together with the heavy cost of compliance. Linking sanctions with the BOSE is also inconsistent with the cooperative nature of the Online

Safety Charter and Safety by Design framework. Furthermore, the eSafety Commissioner already has a broad range of regulatory powers under the existing legislation – more so than any other online regulatory scheme in a liberal democracy – including significant penalties for non-compliance. If the proposed reforms that are subject of this consultation proceed, those powers will be even more imposing. Sanctions should only be imposed in the context of carefully articulated regulatory frameworks, not against the kind of high-level expectations and principles that we would expect to be listed in the proposed BOSE. Not only is determining whether breaches of high level and imprecise expectations fraught with difficulty, it would also be contrary to the BOSE's purpose as a flexible and collaborative concept.

Response to discussion questions: Cyberbullying scheme

Question 7. Is the proposed expansion of the cyberbullying scheme for children to designated internet services and hosting services, in addition to relevant electronic service and social media services, appropriate?

We note the proposal to expand the cyberbullying scheme not only in terms of the eSafety Commissioner's powers, but also in terms of its scope to cover a wide range of digital sectors. The reform is not just expanding the cyberbullying scheme to designated internet services and hosting services, but by removing the tier system it is expanding the scope of the eSafety Commissioner's powers over potentially all forms of internet communications involving Australians.

As an industry that prioritises online safety, we understand and agree with the overarching objective of the reform to improve the Government's ability to help combat cyberbullying across platforms. We have consistently supported regulatory policies that are evidence-based, balanced and effective. However, it is difficult to provide an informed view on the appropriateness of the specific proposed expansion as there are still details that need to be clarified around how it would work and there has been little transparency to date around the operation or the effectiveness of the current cyberbullying scheme over its years of operation.

For example, we understand that the eSafety Commissioner has never exercised any of its two main enforcement powers under the scheme – the section 29 removal notice or a section 42 end-user notice (the latter of which can be used on game players) – in the almost five years since the current legislation has been in effect. While there may be good reasons for this, we are not sure whether this statistic has ever been examined and perhaps call into question the practical usefulness of these powers. It also calls into question why such a significant expansion of the scheme is needed at this time. We note that the proposed scale of the reformed scheme would be very expansive, and, given the Briggs Review noted a fair degree of consensus that the existing legislative powers and functions of the eSafety Commissioner are adequate,[1] we think it is fair to say that there should at least be demonstrable and compelling evidence-based reasons for their expansion.

Given the lack of formal action being undertaken and reported on, there is little transparency around how the cyberbullying scheme works in practice, or whether any evaluation has ever been conducted. The Briggs Review was unable to shed any more light on this, and in fact the lack of available data that could otherwise help to inform the review was a criticism highlighted by the author in the final report.[2] For example, while the eSafety Commissioner does provide some reporting each year on the operation of the scheme, it is generally limited to data around the nature of the complaints received, not how they were effectively dealt with.

It is also therefore unknown to us the extent to which the current focus or scope of the scheme or the tier system has prevented the eSafety Commissioner from

[1] Lynelle Briggs AO, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 of the Broadcasting Services Act 1992 (Online Content Scheme)*, October 2018, p. 27

[2] Briggs, p. 24

responding effectively on cyberbullying, thus the degree to which such an aggressive expansion as is currently being proposed is needed, or would even be effective. For example, we are not aware of the Office of the eSafety Commissioner receiving any complaints involving a game or gaming platform, let alone one in which the publisher or platform-holder was unable or unwilling to voluntarily assist once they were notified. Coming from industry, this question of transparency and justification for reform is not one that we are able to answer but we do expect that they are being considered by the Department as part of the current policy development process. Under any reform, given the highly regulatory nature of the scheme, we would also recommend increased reporting around the operation of the scheme.

Looking at what we understand about the cyberbullying scheme, which to its foundations has been largely designed with social media and communication services in mind, we do not believe that it will be particularly well-suited to the online gaming environment. Many of the cyberbullying risks that are more common in social media and communication services simply do not exist, or have a significantly lower risk profile, in games and gaming platforms. Where risks remain, gaming companies, and most importantly users themselves, already have a range of tools that other kinds of services may not have, and that are likely to be more effective than the rapid removal scheme that is at the heart of the cyberbullying scheme. We explain the rationale for our view below.

- Video games are quite unlike social media services, the sector that the reform currently covers, and communication services, the new sector that the proposed reform is most likely intended to target. Most games have highly limited user-to-user communications and networking functionality that only exist to support the playing of video games.
- While many games and devices do have a degree of communications functionality, this functionality is generally limited to approved friends lists or a specific temporary environment like a game session or game lobby chatroom. Any communications in a game session or lobby chat, for instance, is generally ephemeral – sometimes lasting just a few seconds – and the entire conversation thread will disappear entirely when the game starts or finishes. This is in stark contrast to social media and communications services where communications often become permanent public records.
- Many games also provide very specific ways to create particularly safe spaces to enjoy the gameplay experience. These include private groups, private 'clans' and even private servers. Not only does this mean that groups of friends and family members can enjoy the game just playing amongst themselves, but these are tools that parents can use to create fenced areas where they can also directly monitor their children (as well as enjoy playing the game with them). Access to these private spaces may be by invitation only and/or password protected.
- While the discussion paper suggests that the ephemeral nature of online communications in games means that it cannot be easily reported to the eSafety Commissioner, we think that a far more relevant argument is that the ephemeral nature of this kind of content more importantly means that post-

incident reporting is not helpful as there is nothing to take down. Rather, immediate reporting via the game or gaming platform itself is far more effective.

- Unlike social media and communication services, in-game text is often heavily protected by text filters, often involving highly complex and evolving algorithms in multiple languages. As a result of these controls, the level of coarse or insulting language that is possible in games is generally far more sanitised than the language permitted on social media and communication services. In many instances, not only is inappropriate content immediately hash-censored, blanked or left unsent, the sender may be counseled via an automated message or given an explanation that will help them to reflect on their behavior. Sometimes different levels of filters are offered to the gamer, noting different tolerances for robust language in the community.
- Inappropriate behaviour and language can generally be reported or deleted by the user themselves, while other people that users do not wish to interact with can easily be blocked. Many games and platforms do not even allow user-to-user messaging unless they are approved friends first. Finally, most games and platforms also allow games to be played with communication functionality turned off or allow users to remain invisible in chat (this is sometimes the default setting).
- Where games allow voice-to-voice communication, this is almost always optional with players also able to mute talking or restrict talking to friends or teammates.
- With social media and communications services, a person's online identity is often - and sometimes necessarily - tied to their real-world identity, increasing the risks of conflict in the schoolyard or elsewhere being brought into the digital world. On the other hand, profiles and identities in games are often limited to avatars and 'gamer tags' that provide little to no real-life identifying information. Anonymity is a widely accepted way of online engagement in games, which can protect users in ways that are impossible in other online media. Quite often users are automatically 'dark' and only become contactable if they wish. Identities and communications on games platforms are literally designed just for supporting gameplay, talking with friends and sharing achievements.
- This anonymity also means that it will be often very difficult, if not impossible, to identify end users for the purpose of the end-user notice scheme. Platforms may not even collect identifiable personal information, for many reasons including for data protection and international privacy laws relating to children, and disclosure of any such information to third parties for non-law enforcement purposes may potentially comprise a serious breach of domestic and overseas legislation.
- Finally, and perhaps most important from a practical perspective, many of the more dynamic functionalities of social media or electronic communications services that present the highest risks for cyberbullying simply are not a part of the video gaming world. This includes posting messages publicly, posting images and videos, re-broadcasting, forwarding or sharing messages,

tagging third parties or mass-messaging, which are simply not available capabilities in most games and gaming devices.

- Similarly, many of the more serious concerns of young Australians as outlined by the eSafety Office, including cyberbullying as an extension of real-life inter-relationships, fake or imposter accounts of victims, sex-tortion and image-based abuse present far less of a risk within the gaming environment than in others.

Question 8. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

As discussed in our response to question 7, we expect that the video games sector would be subject to very few, if any, take-down requests. This is because in-game communication is often ephemeral, subject to filters, only allowed between friends, easily deleted or easily reported – or subject to all of these. While we do not have a specific position on this question, we note that this question and some others in this discussion paper highlight the fact that many of the proposed reforms including the expansion of the cyberbullying scheme seek to cover almost any digital service that has a communications functionality.

For these questions, we urge the Government to recognise that digital businesses cover a range of businesses, not only the enormously well-resourced social media services with hundreds of millions if not billions of users that are currently being covered by the cyberbullying scheme, and that the cyberbullying scheme was originally designed to target. Some of these services literally have thousands of people on a worldwide cycle dedicated to continued content moderation and budgets in the tens or hundreds of millions of dollars to invest in compliance. These services may well be able to comply with the current 48-hour or even the proposed 24-hour takedown period.

By contrast, not all game publishers have the ability to dedicate this level of resourcing, an example being a multiplayer game with just a few thousand users, limited communications functionality and compliance resources comprising just the original developers who may not speak English or have different standards for inter-personal conflict and coarse language and who may only work business hours and therefore are unable to respond quickly. Regulation as broad and deep as the cyberbullying scheme must also be flexible, proportional, appropriate and subject to discretion to take into account these wide contrasts in the digital industry.

Finally, as we also noted in our response to question 7, we are not aware that any take-down notices have been issued in the almost five years since the current scheme has been in effect and a reasonable question to ask would be why a halving of the proposed take-down period to 24 hours (or even shorter) is considered a necessary reform. One of the reasons that we imagine the current 48-hour period was originally agreed upon was that, in some circumstances at least, cyberbullying is not as simple as removing an offending message but involve complexity, context and conflict between two parties and more nuanced approach may be needed (this is further discussed in our response to question 10). In many such instances, time is needed to understand whether removal of the content in question is the appropriate response or if perhaps another solution is needed.

The examples provided in the discussion paper around international practice, namely that platforms in Germany are required to remove illegal content in 24 hours and that platforms in French are required to remove overly hateful content within 24 hours, are only partly useful for comparative purposes. The kinds of material that these schemes are designed to target are often vastly different in terms of content and more unequivocal compared to some of the kinds of content that fall within the scope of the cyberbullying scheme. Those schemes would more usefully be compared to the Online Content Scheme or 'hate speech' laws.

Question 9. What are the likely compliance burdens of the proposed changes to the cyberbullying scheme on small and large businesses?

As we've discussed in our response to the previous questions, the real impact of the compliance burden on small and larger businesses can differ significantly. While we would expect few, if any, takedown requests to be issued to video games businesses, we do think it would be useful to consider the potential compliance burden nonetheless as that is what businesses need to plan for, no matter how unlikely it will be for them to be directly affected. In many cases, given the global nature of digital product development and management, the compliance burden would extend to all markets that the business has users in, despite the fact that no other country has decided to follow Australia's path of a cyberbullying scheme to date.

The global video games industry, unlike social media and communication services which are dominated by a handful of large corporations, is comprised of thousands of companies and developers, from large platforms to micro studios and individual developers. The local Australian game development industry is particularly focussed on smaller independent studios creating online and mobile games. For example, while there are only a small number of social media services and communications services used by Australians, almost all of whom are well-resourced multinationals, there are hundreds if not thousands of video games played in Australia, many of which have been developed by small businesses. It is not unusual for a popular game to be created and run by a team of less than five, including some of the Australia's greatest video game exports with well over a billion combined players.

The current 'one size fits all' approach of the proposed cyberbullying reform means that the expectations placed on the most popular, highest risk and most resourced platforms are currently the same as the expectations placed on a much smaller and lower risk service. The strong powers that the eSafety Commissioner wields, together with the proposed 24-hour takedown period, means that digital business, particularly small businesses, may have to establish new systems and capabilities in place at significant cost. These may not be realistic for businesses in their early growth stage and may well be inconsistent with the Government broader 'better regulation' reform agenda.

The fact that few take-down requests are anticipated to our sector under an expanded cyberbullying scheme does not reduce the regulatory burden, particularly for high-compliance, reputation-driven industries like our sector. The reality is that Australia has already earned a reputation for its heavy-handed approach to regulating digital companies. While this reputation is not specific to online safety laws, they will only serve to add to it. In the gaming environment, we have already heard of overseas game developers and publishers who are considering withdrawing from the Australian market or are avoiding investing in or partnering with Australian businesses. This is unlikely to be the desired outcome of any reform.

Finally, the discussion paper does not clearly articulate how the penalties for non-compliance under the scheme will operate under a revised scheme. We encourage the Department to provide as much information about how the proposed scheme would work in detail as soon as it is available.

Question 10. What other tools could the eSafety Commissioner utilise to effectively address cyberbullying in the circumstances where social media service and end-user notices are not well suited to the particular service upon which the cyberbullying has occurred?

The background and context part of our discussion paper has outlined the many the tools that are already available at both the device and in-game level to mitigate and address the risk of cyberbullying and other online safety issues. These include proactive measures that are automatically implemented, measures designed to assist parents monitor and guide their children, and a range of tools that help empower users to immediately and effectively address inappropriate content or behaviour.

How a platform deals with a specific instance of cyberbullying may involve significant complexity and the appropriate response may differ on a case-by-case basis and involve a delicate balancing of judgement and discretion. In the case of games, platforms also need to consider that while harassment and abuse should not be tolerated, the competitive nature of gaming means that language may naturally be more robust, just as it may be on a sporting field, across a boardgame or in the playground in the physical world. An ephemeral insult in the context of a game on a private server will have a different impact on a child than the same insult posted publicly on social media or another online forum. More significantly, there may well be two sides of an online conflict, with only one side being initially presented in a complaint.

We also note that the discussion paper currently provides an example of an additional tool under consideration that the eSafety Commissioner may be given to compel a platform or service provider to enforce their terms of service or to apply account restrictions, presumably as outlined in the terms of service. We urge caution around this approach as to make terms of service enforceable by a third party is a significant shift in the common and legal understanding of how terms of services are used. We are not aware of any other regulation in Australia or around the world where a government body has the power to compel one party of an agreement to take a particular action against another in this way. It could have a profound global impact on how terms of services are written and a highly unintended consequence could be that some terms of services are amended to self-limit the kind of punitive action available to a platform if it would mean they could not be used with appropriate discretion.

Bearing all of this in mind, great care should be taken to giving a regulator powers beyond its current powers for seeking the removal of content. The eSafety Commissioner's current preferred approach of working collaboratively with industry to resolve complaints is likely to be the most effective approach in most circumstances. Given that no take-down or end-user notices have been issued in the almost five years that the cyberbullying scheme has operated, we doubt that the right answer is more regulation beyond removal of content. This is particularly true for regulation that seeks to compel platforms to take punitive action against end users, noting that the eSafety Commissioner has been reluctant to take action against end users itself, potentially due to concerns that 'perpetrators' of child cyberbullying may often be vulnerable minors or victims themselves who may need to be dealt with with sensitivity.

Rather than introducing more and more regulatory tools, a better policy approach may be to consider what other tools are needed after an evaluation of existing powers and if gaps are identified.

Response to discussion questions: Establishing a new cyber abuse scheme for adults

Questions 11. Is the proposed application of the cyberbullying and cyber abuse schemes to designated internet services and hosting services, relevant electronic service and social media services, appropriate?

Question 12. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

Please see our responses to questions 7 and 8, which are also relevant to these questions. The key point that we make is that while we will generally always support thoughtful, balanced and evidence-based reform, the reality in this instance is that a take-down focussed scheme is not suited to online games where communications are generally limited, private, ephemeral, filtered, optional and/or are already easily deleted and reportable.

Question 13. Do the proposed elements of a definition of adult cyber abuse appropriately balance the protection from harms with the expectation that adults should be able to express views freely, including robust differences of opinion?

We agree with the discussion paper that if an adult cyber abuse were to be implemented, a higher standard threshold should apply to determine what constitutes adult cyber abuse compared with the cyberbullying of an Australian child. An approach that mirrors the components and standard of the current criminal offence of using a carriage services to menace, harass or offend, taking into account all the circumstances, appears appropriate.

In the specific context of our sector, it is useful to again provide a reminder that games are not just for personal entertainment and to improve wellbeing, but also provide avenues for people to compete against each other in a healthy way. Just like in sport, play and countless other competitive hobbies and activities, there will always be colourful language, 'trash-talking', verbalised frustrations and sometimes arguments between players in video games. While there is no place in games for harassment or abuse, robust conversations and self-expression, particularly between adults, should not be outlawed or need to be moderated in the vast majority of gaming environments, just as they are not outlawed or moderated in real life. Behaviour and communications that are accepted or condoned in the real world and face-to-face society should not be regulated just because they are expressed online and, theoretically, easier to regulate.

Question 14. Should the penalties differ under a cyber abuse scheme for adults and the cyberbullying scheme for children?

We have no views on the penalties for end users, noting that the proposed reforms are not seeking to impose penalties under the cyberbullying scheme, much of which would likely target perpetrators who are themselves minors. As we have previously mentioned, the discussion paper does not clearly articulate how the penalties for service providers under the reforms will work, either under the proposed revised cyberbullying scheme or new cyber abuse scheme. We would encourage further transparency and dialogue about these as soon as is practicable during the early policy development process.

Question 15. What additional tools or processes, in addition to removal notices, could be made available to the eSafety Commissioner to address cyber abuse occurring across the full range of services used by Australians?

Please see our response to question 10. We believe our commentary around the existing tools and powers that are already available, as well as the complexity around regulating online communications and conflicts, are also relevant in the context of a proposed cyber abuse scheme. Given that a criminal offence already applies, and the proposed scheme would impose both a take-down as well as a civil penalty regime, we question whether further regulations are needed or would be helpful. A more useful policy approach may be to consider what other tools are needed after first an evaluation of the operation of a future scheme.

Response to discussion questions: Addressing illegal and harmful online content

Question 19. Is the proposed application of the take-down powers in the revised online content scheme appropriate?

Question 20. Are there other methods to manage access to harmful online content that should be considered in the new Online Safety Act?

We note that the Briggs Review recommended that the classification system applying to online content be changed, with the eSafety Commissioner to follow a new harm standard.[3] This recommendation recognised that the standards for classification, which are still largely designed with commercial film and video game entertainment products in mind, are not suited to online content regulation. The proposed concept of 'seriously harmful content' that would be the focus of the eSafety Commissioner is consistent with this recommendation.

However, we also note that the Online Content Scheme has not been entirely decoupled from the National Classification Scheme, with some characteristics of the current scheme to remain. In particular, there is now a concept of Class 2 content under the proposed new scheme, which covers content that would be classified as RC, X18+ and MA15+ under the National Classification Scheme. This means that the current impact of double regulation on our industry, which alongside film is technically subject to both the National Classification Scheme and the Online Content Scheme, would be retained.

This approach appears to us to be contrary to the recommendation of the Briggs Review, which recommended an alternative 'harm standard' that should be developed for certain online content rather than using classification standards (MA15+, R18+, X18+ and Refused Classification) [4] . This was also the recommendation of the eSafety Commissioner's submission to the review[5]. The content standards under the National Classification Scheme have been developed specifically with commercially-distributed films and video games in mind, and this will not change after the current review of that scheme has been completed. Films and computer games will continue to be regulated under the National Classification Scheme and we are concerned with the potential for regulatory overlap, uncertainty for industry and inconsistent and perhaps even contradictory compliance requirements if the same content remains subject to two separate schemes.

Instead, we believe that a separate standard entirely be adopted to define Class 2 content, focussing on the specific kinds of harms-driven content that the scheme has been be designed to target – which does not include commercial MA15+ and R18+ screen content. If the classification category model continues to be considered, we believe that 'traditional' content that is already subject to the National Classification Scheme should be excluded from the scope of the Online Content Scheme.

[3] Briggs, p.16
[4] Ibid.
[5] Briggs, p. 15

Under the proposed approach for Class 2 content, we are at least encouraged that the new regulatory framework appears to take a more flexible and principles-based approach, with the discussion paper noting that the new scheme will take into account the nature and characteristics of particular online services. We generally believe that a collaborative and co-regulatory code-based system that is less focused on specific requirements and compliance and more targeted towards building up a culture of digital best practices is the approach that is most likely to be effective. At this stage, much about how the code-based scheme will operate in practice is still unclear, and we know the details may not become clearer until the process of developing the codes with the eSafety Commissioner occurs, which is why we believe the legislative drafting process should be performed as thoughtfully as possible. Subject to further clarity around this proposed scheme, IGEA would be willing to work on a code for our sector if needed and appropriate.

Response to discussion questions: Role of eSafety Commissioner

Question 36. Are the eSafety Commissioner's functions still fit for purpose? Is anything missing?

Question 37. To what extent should the existing functions of the eSafety Commissioner be streamlined? Are there particular functions that need to be maintained, or new functions that should be specified?

Question 38. To what extent should the functions of the eSafety Commissioner be prioritised?

While we believe that the Government and the Minister, in his previous role, showed leadership in establishing the Act and the eSafety Commissioner role, we also believe strategic improvements can be made to its direction and operation. Many of these were considered in the final report of the Briggs Review but not all are captured in the discussion paper. Indeed, some of these issues will not be solved by legislative reform alone and the regulation-driven approach that is the focus of this consultation is only part of the solution.

In our submission to the Briggs Review, we noted that the scope of the Office had moved beyond its original intent and the enacting legislation, often duplicating the work of other organisations. We noted that the Office's focus should be on education and awareness raising of existing online safety tools and resources, in the process amplifying the range of established programs, tools and expertise, rather than focussing so heavily on its role as a regulator. We also noted that focus and consideration should be given to how the Office can drive behavioural change among users, the most important way that we believe online safety risks can be mitigated in the community.

We believe our views remain valid. Some of the other representations made during the Briggs Review, including from the non-for-profit sector, highlighted the risks of the eSafety Commissioner duplicating the efforts of existing foundations and initiatives that focus on improving online safety in the Australian community[6]. They highlighted, in other words, the risk of a government body that competes with rather than complements, supports or works with other organisations. These concerns were captured in the final report of the Briggs Review, which noted that many stakeholders had concerns that the eSafety Commissioner's continually increasing role and budget were cutting across the function of other bodies and their programs[7].

Similarly, many of the eSafety Commissioner's existing (and new) regulatory roles, particularly those focused on content removal, essentially duplicate or simply add a level of regulatory oversight over existing industry mechanisms that already exist to address that content. These have been covered at length in this submission. Unfortunately, there has been a lack of information about the effectiveness of these powers and an absence of any data and performance-based evaluation of existing

[6] Briggs, p. 28, 30-1
[7] Ibid.

schemes, which was not undertaken through the Briggs Review. As a result of this, we believe there is a limited evidence-base for driving such an expansion of the eSafety Commissioner's powers as has been proposed under these reforms.

We also believe the eSafety Commissioner should focus more on building relationships and improving cooperation with both the not-for-profit cybersafety sector as well as the industry which it seeks to regulate and influence. This was feedback that was also captured in the Briggs Review, which noted a greater need to improve strategy, coordination, positioning, relationship-management and partnership-building[8]. Unfortunately, we still see this as an area of priority focus. For example, we note that the eSafety Commissioner's Online Safety Consultative Working Group – its key vehicle for collaboratively bringing together key stakeholders in the not-for-profit sector and industry – did not meet at all in 2019.

Finally, we believe that the greatest opportunity for leveraging the eSafety Commissioner's expertise and resources is on education and prevention in the community. For example, the report of the Briggs Review noted that while technological intervention is necessary to address cyber-bullying, it cannot solve what is essentially a social issue which needs to be tackled in schools, in families and communities[9]. There is much that the Office of the eSafety Commissioner can achieve in fulfilling its naturally well-placed role to play a leadership role within schools and communities, project awareness of positive digital hygiene and practices and to amplify existing tools, portals and programs of both industry and not-for-profit sector.

Question 39. What are the likely impacts, including resource implications, on other agencies and businesses of a new Online Safety Act?

Our commentary on likely impacts on industry, including costs of compliance, have been covered in the relevant sections of this submission. We expect it is already planned, but given the significant expansion of powers that are envisaged as part of these reforms and the significant effect they will have on industry, we encourage the Department to conduct comprehensive cost/benefit and regulatory impact analysis processes as part of advising the Government on the proposed reforms and alternative options that may be available.

[8] Briggs, p.28-9
[9] Briggs, p.30