IGEA

interactive games & entertainment association

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

Consultation on a Bill for a new Online Safety Act

February 2021

Table of contents

Background

Who is IGEA?

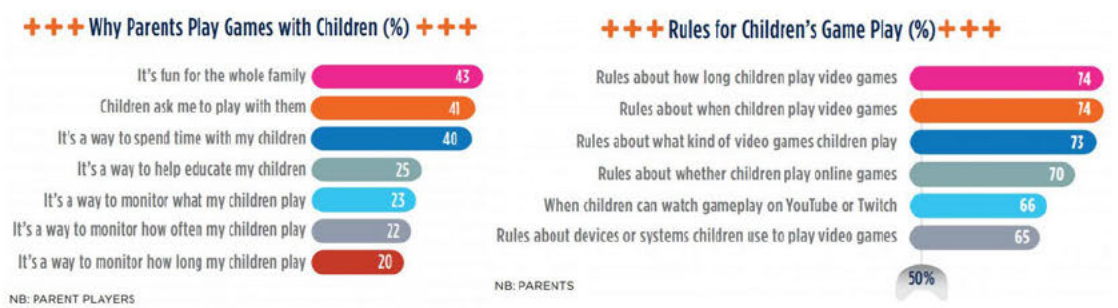
The Interactive Games & Entertainment Association (IGEA) is the industry association representing and advocating for the video games industry in Australia, including the developers, publishers and distributors of video games, as well as the owners of the most popular gaming platforms, consoles and devices. IGEA also manage The Arcade in South Melbourne, Australia's first, not-for-profit, collaborative workspace created for game developers and creative companies that use game design and technologies. IGEA organises the annual Game Connect Asia Pacific (GCAP) conference for Australian game developers and the Australian Game Developer Awards (AGDAs) that celebrate the best Australian games each year. IGEA's full list of members is available on our website.

Video games in the Australian community

Video gaming is one of the most popular ways for Australians to unwind and enjoy their time. According to our Digital Australia 2020 research, conducted by Bond University, approximately two-thirds of all Australians play video games. The vast majority of Australian video game players are adults, comprising almost four out of every five players, with the average age of players being 34 years old. While many Australians play games to have fun, they also play for other important reasons, including to de-stress, to keep their minds active, to take a break from their day, or simply to pass time positively. Especially during the past year of COVID disruption and necessary lockdown measures, our sector unexpectedly provided a vital role for encouraging and helping people to self-isolate by keeping them positive, occupied and connected to their family and friends via the social and community features of games, devices and consoles.

Our research has also found that parents are highly (and increasingly) engaged in how their children play games. Most parents and carers play games in the same room as their children, while over half even play games with them online. Most parents are either mostly or completely familiar with the family controls on their game systems, and only around one in ten said that they were unfamiliar with them. The overwhelming majority of parents said that they have talked to their children about playing games safely, while a similar majority also said that they had set rules around how their children play.

Australian parents and video games



Source: IGEA, Digital Australia 2020

Our sector's commitment to online safety

The Australian and global video games industry is committed to ensuring that the community can enjoy games in a fun and safe way. We believe that no other segment of the digital industry has invested in or has implemented as many specific technologies and design features aimed at delivering online safety as the video games sector. We have highlighted these in detail in our March 2020 submission to the Department's earlier consultation on a proposed new Online Safety Act (the "earlier consultation"), but for ease of reference, we have included an updated summary here in this submission.

Classification and IARC

Video games are subject to comprehensive and precise 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 (the Board), an independent government body, before they can be made available to the public. Since the start of the NCS in 1995 and the creation of IGEA shortly thereafter, Australian video game companies have followed a policy of strict compliance to ensure that games that are bought and played in Australia have been appropriately classified. Over the past decade, IGEA has worked in partnership with the Department and the Board to ensure that digitally-distributed games such as online and mobile games are classified. The result is the International Age Ratings Coalition (IARC) classification tool, which was built by our industry in collaboration with government and non-government ratings authorities around the world, and is now co-governed by the Department's Classification Branch. Through IARC, millions of games and non-game apps have been classified on Google Play and other major gaming platforms.

Online safety features on consoles, devices and in games

Video game consoles, devices, platforms and games provide a multi-level framework of online safety features to provide a safe environment for game players and their families, with many such features unparalleled in the online sector and unique to our sector.

These include:

- Family and child accounts with specific (and often customisable) privacy, communication, content and online safety settings
- The use of PIN codes, passcodes and other security measures to ensure the integrity of child accounts
- Parental tools for monitoring or setting parameters and limits regarding gaming and media activities, often controllable from their smartphones via companion apps
- Visibility settings for gaming accounts to enable players to easily set themselves as available, busy, hidden or offline as desired
- The ability for players to hide their own activity feed posts, and filter posts from others
- Player accounts that are almost always de-identified or anonymous (in contrast to identity-linked social media and communications app accounts)

- Automatic, pre-emptive and/or customisable text filters for player-to-player communications, often implemented via algorithms that are constantly updated and implemented across multiple languages
- Chat features that are generally limited to peer-to-peer text communication between friends or ephemeral chat lobbies, and functionality that overwhelmingly prevents mass communications (eg. public posts) or the ability to send images and other non-text media
- The ability for players to easily mute or block communications from other players at any time for any reason
- The ability to create restricted or closed servers, game lobbies, clans and levels for private play between family and friends (which are often administered by parents)
- Clear and transparent community standards established by games companies through Terms of Services, Community Charters and Codes of Conduct
- The ability to report other players for violations of rules or Codes of Conduct
- Strong compliance, enforcement and disciplinary tools, including warnings, account suspensions and bans, and
- Incentive systems to encourage positive game-related behaviour, including through rewards and player-to-player endorsement.

Industry advocacy, awareness-raising and collaboration

Our sector takes a proactive approach to raising awareness and undertaking education around parental controls and responsible game play. Our website has a parental resources hub that provides information on parental controls, and we regularly issue public communications to remind the community about all the tools available to players and their parents and carers to help them play games in both a fun and safe way. We also research how Australian players and their parents and carers engage in online safety to inform our own and our members' activities. Together with our international counterparts, we have further established the Universal Principles for Fun & Fair Play which outline four core values setting our sector's approach to esports: safety and well-being, integrity and fair play, respect and diversity, and positive and enriching game play.

In addition, video game companies directly invest in awareness-raising and engaging with their own communities on online safety. For example, many video game companies including IGEA members have formed groups such as the Fair Play Alliance which enables gaming professionals and companies to exchange learnings on methods to encourage healthy and positive communities and player interactions in online gaming.

Many companies also invest in individual initiatives, such as Electronic Arts' Positive Play program, which includes the launch of its own parents' resource hub, a Positive Play Charter with its player community and its Building Healthy Communities summits and Player Council, which provide forums for the player community to share feedback on combatting disruptive behaviour.

EA's Building Healthy Communities Summit in 2019

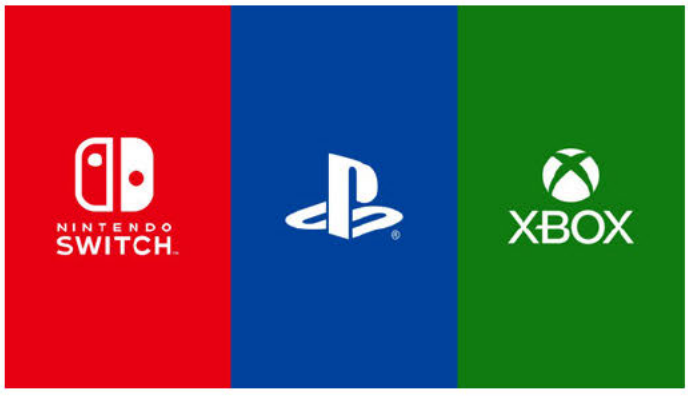
Source: https://www.ea.com/news/building-healthy-communities-summit

To demonstrate the persistent and ever-strengthening nature of our sector's commitment and transparency to the community on online safety, in December 2020, Nintendo, Sony and Microsoft each announced a new set of Shared Online Safety Principles (see below) that demonstrate their aligned belief that protecting players online requires a multidisciplinary approach that combines the benefits of advanced technology, a supportive community, and skilled human oversight. The new principles outline three themes - prevention, partnership and responsibility – that will help guide the console makers as they each continue working towards the same goal of improving player safety and each continue investing in their own initiatives to achieve this goal.

The Shared Online Safety Principles

The three overarching principles:

- "**Prevention**: Empower players and parents to understand and control gaming experiences.
- **Partnership**: We commit to partnering with the industry, regulators, law enforcement, and our communities to advance user safety.
- **Responsibility**: We hold ourselves accountable for making our platforms as safe as possible for all players."



To read the full Shared Online Safety Principles:

- Nintendo Switch: nintendo.com/online-safety-principles
- Sony PlayStation: www.sie.com/en/blog/shared-online-safety-principles
- Microsoft Xbox: news.xbox.com/en-us/2020/12/14/shared-safety-principles

Submission to the prior consultation

As mentioned, in March last year, IGEA made a submission to the Department's earlier consultation. Key points that were made in our submission included:

- Of all the various sections of the digital environment, the video games sector has implemented the most significant range of online safety features (all being industry-led) and is already highly resistant to the risks that a proposed Online Safety Act would seek to address.
- We support well-designed and evidence-based reforms. However, it was our view that there is insufficient evidence for why such a significant proposed expansion of the eSafety Commissioner's (the Commissioner) regulatory scope and powers was considered necessary, especially considering how little its existing powers have been used.
- We did not believe that the proposed extension of the cyber-bullying takedown scheme to video games was needed, likely to be effective, or proportionate to the risk as it relates to our sector. Communications between game players are already restricted, ephemeral, filtered, reportable, pseudonym-based and able to be deleted and turned off. We also noted that the Commissioner has never reported receiving cyber-bullying complaints involving video games, let alone complaints where a video game company was unable or unwilling to voluntarily provide assistance once they were notified of a potential issue.
- While it was a step in the right direction, we also did not believe that the proposed reform of the Online Content Scheme went far enough to achieve its goal of long-term modernisation. For example, the model outlined in the Discussion Paper retained some of the double-regulation of the current framework, where games need to comply with both the National Classification Scheme and the Online Content Scheme for the same content even though both schemes have the same policy objective (of preventing children from accessing non-age-appropriate content). This has caused significant confusion for industry and consumers alike.
- For example, under the revised framework proposed in the Discussion Paper, an online video game at the R18+ level would need to:
    - be classified by the Board or a classification tool and comply with state and territory classification enforcement laws, which were written in a pre-digital age but are nevertheless still enforceable online, and
    - comply with the rules outlined in the Online Content Scheme (noting that the Commissioner's view of what constitutions R18+ content may differ to the Board's view), which are not the same as the requirements under the National Classification Scheme and also differ depending on whether the content is hosted in Australia or overseas.
- Other points that we made in our submission in response to the earlier consultation's Discussion Paper included:
    - We considered there was potential for confusion and regulatory overlap between the Basic Online Safety Expectations (BOSE), the Online Safety Charter and the eSafety Commissioner's 'Safety by Design' framework.

- The ideas proposed in the Discussion Paper generally adopted a 'one size fits all' approach that treated the games sector like an extension of social media and messaging services, despite the very significant differences between the services, especially in terms of community online safety risks.
- The proposed reforms also imposed the same or similar regulatory burden on small businesses, such as an indie studio making its first game, as it did on major multinationals with more users and resourcing.
- We questioned the heavy focus of the reforms on increasing regulation and the Commissioner's powers, even though many of the Commissioner's existing powers appear to have never been used. Instead, as the Government's Briggs Review recommended, we supported a greater focus on prioritising and strengthening the Commissioner's collaborative approaches and education and awareness-raising functions.
- The Discussion Paper was, understandably, light on the specific details of how the new regulations and powers that were being proposed would work (we note that the release of the present Exposure Draft of the bill is an effort to address this).

Summary of key points

Our approach in this submission

We thank the Department for the opportunity to provide comment on the Exposure Draft of the Online Safety Bill (the "draft bill"), after having previously provided a substantial submission responding to the Discussion Paper during the earlier consultation. We also thank the Department for its high level of communicativeness during this consultation and recognise the high amount of work and consultation that has been carried out.

We note that the draft bill largely reflects the policy proposals outlined in the original Discussion Paper without any significant change of direction. As a result, we do not believe that many of the overarching concerns that we had raised in our previous submission about the proposed reforms, as summarised in the previous section, have been addressed. However, we do acknowledge and appreciate that aspects of the draft bill appear to have been drafted with thought given to address some of the specific issues that we raised in our prior submission.

While we continue to have strong reservations about the proposed reforms, in the interests of positive dialogue and recognising the advanced nature of the Government's policy-making process as evident in the draft bill, we have dedicated the rest of this submission to identifying and proposing specific changes to the text of the draft bill so that the proposed reforms can be implemented and run as effectively and as least-problematically as possible. We are happy to discuss these suggestions further in person or via videoconference if it would be helpful. Given the significance and scope of the proposed reform, to the extent that is possible or practicable, we would welcome the opportunity to review any future revised draft bill before it is introduced into Parliament.

As the draft bill is complex and we have had to prepare this submission within a limited period of time (due to multiple concurrent policy consultations), we apologise in advance for any errors in this document or anything in our views that misunderstands the proposed operation of the provisions of the draft bill.

Overarching themes of our submission

The specific changes that we have sought in the draft bill as detailed in the tables on the following pages can generally be grouped into the following overarching themes.

<u>It is vital that sufficient time be given to industry to implement the reforms</u>

The draft bill proposes a significant expansion of almost all aspects of the Commissioner's scope, role and powers, all of which will impact our own industry and many others. Despite this, the timeframes outlined in the bill are short. The legislation could come into effect as soon as a Proclamation is made. Further, just six months has been given to industry to prepare industry codes, or if the Commissioner requests that a code be made, just 120 days. Given the complexity of the regulation involved, the fact that many aspects of the proposed regulatory framework are world-first, and the technical challenges that would come with compliance in many cases, longer timeframes are necessary and reasonable.

The need for parameters and predictability in the future regulatory framework

Despite being the primary legislation, the draft bill sometimes provides only minimal guidance, direction or limits around the regulation that it foreshadows. For example, the draft bill facilitates the creation of BOSE and includes minimum requirements around what they might include, but does not balance this with limits on their scope. With industry codes, the bill provides almost no parameters around what they might be expected to contain, providing only an extensive list of non-exhaustive examples, and gives the Commissioner with almost limitless discretion in terms of determining whether a code is satisfactory. Similarly, the definition of 'restricted-access system', which is vital for industry to understand, is not in the legislation but will be determined solely by the Commissioner.

All of this means that much of the detail of the future regulatory framework is still unknown, and there is currently limited transparency, certainty or predictability of the regulation for industry and what providers will need to do to achieve compliance. It also means that there are few checks and balances against potential regulatory overreach in future that could be beyond the intention of the current Parliament. While we acknowledge that it is important for Government to be able to respond flexibly to a changing online environment, this needs to be balanced with some degree of baseline certainty and predictability for industry.

The need for flexibility in how industry can comply with online safety requirements

While overarching direction is absent in some parts of the draft bill regarding how aspects of the proposed regulation will work, there is also, perhaps, an unnecessarily high level of prescriptiveness of detail in others. These include the lengthy and very specific minimum requirements of the BOSE, as well as the multiple pages of (non-exhaustive) examples of issues that industry codes could deal with. We are concerned that this specificity could translate to highly prescriptive requirements which, when combined with the wide scope of the regulation, the breadth of sectors it covers, and its equal coverage of both very large and very small providers alike, means that full compliance for some providers will be difficult or impossible to achieve. Highly specific (rather than more principles-based) requirements may also lose their relevance quicker as the online environment evolves, and could also discourage industry from innovating with new ways of strengthening online safety. One suggestion that we have made against a few parts of the bill that would assist in addressing this challenge is to make it explicit that taking reasonable steps to comply with obligations under the proposed legislation should be sufficient, as well as the further availability of a 'reasonable excuse' defence.

Balancing the focus towards complainants and end-users - not just platforms

The main mechanism by which the bill seeks to address inappropriate online content is by targeting digital platforms and services rather than the individuals responsible for this behaviour. While we believe all stakeholders have their role to play, including industry and users, the reforms appear to signal a further shift in the Commissioner's focus away from individuals towards platforms. For example, parts of the draft bill would enable the Commissioner to 'name and shame' providers for the behaviour of their users even when they have taken all reasonable steps to prevent and to respond to it. Concerning link-deletion and app-removal notices, the proposed regulation even targets search engines and app marketplaces that are two steps removed from the online material. We

recommend a recalibration of the regulation where needed so that the Commissioner's functions and powers focus not only on providers but on individuals, and are also reasonable and proportionate in terms of how they deal with providers.

Focussing on online material with an Australian connection only

It is clearly the Government's intention that the proposed regulation should only extend to cyber-bullying, cyber-abuse and other relevant material when it involves an Australian complainant or target only. While this need for an Australian nexus and jurisdictional connection is reflected in most parts of the draft bill, there are some areas where it is implied but not necessarily made explicitly clear. This includes the Commissioner's powers to request certain information from providers, such as statistics on complaints about breaches of terms of use, as well as personal data on end-users. In relation to the latter, we also strongly believe that providers should not be compelled to provide sensitive personal information concerning end-users outside of Australia, even where they relate to a complaint originating from Australia, as it raises significant legal and jurisdictional concerns.

The inclusion of commercial R18+ rated content within Class 2 remains problematic

While we are pleased to see that the draft bill sensibly excludes MA15+ material from the scope of the Online Content Scheme, we believe R18+ material should likewise be excluded. There is a significant gulf in both policy and practical terms between material that has or would be classified RC (and even X18+) on one hand, and R18+ material on the other. R18+ material is legal and permissible material that is already regulated under the National Classification Scheme. Including R18+ material within the scope of the Online Content Scheme will result in double regulation, which we and others including the ACMA have previously pointed out. Further, we strongly urge the Government to prioritise the modernisation of the National Classification Scheme. As a result of outdated perceptions of video games from the 1990s, video game content is classified harsher than film and other kinds of media, meaning that some content could be subject to a removal or remedial notice if it is in a video game, but would fall outside of the scheme if it is presented in a film – even if it is the exact same content with the same impact.

Increasing the Commissioner's transparency as well as its powers

Under the proposed reforms, the Commission will be given significant powers to obtain information from providers, particularly under the BOSE, its information-gathering powers and its investigative powers. Like a law enforcement or criminal intelligence agency with coercive powers, there is even a new criminal penalty of 12 months imprisonment if a provider does not answer a question, give evidence, or produce a document under the Commission's investigative powers under Part 14. Despite this significant proposed strengthening and expansion of the Commissioner's powers, there are very few transparency or reporting obligations imposed on the Commissioner, even at a basic statistical level, including on its activities and use of powers. Doing so will not only help the public, industry and the Government to understand the scale and characteristics of the online safety issues that Australians face, but it will also help to ensure that the regulatory framework and the Commissioner's use of its powers remain fit-for-purpose, adequate and proportionate.

Part 1 – Preliminary

Section 2 – Commencement

1. The whole of this Act — A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	The proposed reforms outlined in the draft bill are numerous and substantive. Industry will need at least 6 months to implement them, and at least 12 months for industry codes. We suggest amending this section so that the Act cannot commence within the period of 6 months beginning on the day the Act receives the Royal Assent. Alternatively, to provide certainty for industry, the section could fix the commencement date at 6 months after Royal Assent.

Section 5 - Definitions

access-control system, in relation to material, means a system under which: (a) persons seeking access to the material have been issued with a Personal Identification Number that provides a means of limiting access by other persons to the material; or (b) persons seeking access to the material have been provided with some other means of limiting access by other persons to the material.	Currently and into the future, the video games industry will continue to innovate with new and increasingly-effective ways to implement systems that empower and enable parents and carers to better restrict the kinds of content that their children can access. This kind of innovation is necessary, is the only sustainable solution to content-regulation, and should be encouraged. Therefore, we ask whether the definition of 'access-control system' should be clarified to make it clearer that parental controls and features, such as in apps and on devices, that provide parents with the means of limiting their children's access to material, are an 'access-control system' (we understand that it is the Government's intention that they are). Alternatively, this could be dealt with as a legislative note within this section, or if more appropriately, highlighted in the Explanatory Memorandum to a future Act. At paragraph (a), we also suggest including "**password, or other security mechanism**" after the reference to Personal Identification Number.

relevant electronic service means any of the following electronic services: (a) a service that enables end-users to communicate, by means of email, with other end-users; (b) an instant messaging service that enables end-users to communicate with other end-users; (c) an SMS service that enables end-users to communicate with other end-users; (d) an MMS service that enables end-users to communicate with other end-users; (e) a chat service that enables end-users to communicate with other end-users; (f) a service that enables end-users to play online games with other end-users; (g) an electronic service specified in the legislative rules.	Paragraph (f) should use the same test of 'communicate' as used in paragraphs (a)-(e) so that it is amended to: "a service that enables end-users to play online games **and communicate** with other end-users". Many online games enable a player to play with others without the ability to talk, chat or otherwise communicate with them (eg. an online chess game with no chat function). There are zero risks of cyber-bullying, cyber-abuse or other online safety harms in such games and they should not be within the scope of regulation under the proposed reforms.

Section 13 – Social Media Services

(4) For the purposes of this section, a service is an ***exempt service*** if: (a) none of the material on the service is accessible to, or delivered to, one or more end-users in Australia; or (b) the service is specified in the legislative rules.	Our reading of section 13 is that only Social Media Services can be an 'exempt service'. If this is correct, we suggest that this section be amended so that 'relevant electronic services' may also be an 'exempt service'.
(5) If the Commissioner is satisfied that: (a) an electronic service has controls on: (i) who can access material, or who can be delivered material, provided on the service; or (ii) the material that can be posted on the service; and (b) those controls will be effective in achieving the result that none of the material provided on the service could be cyber-bullying material targeted at an Australian child; the Commissioner may, by writing, declare that the service is an ***exempt service*** for the purposes of this section.	If an electronic service satisfies paragraphs (5)(a) and (5)(b), we consider it to be appropriate that not only may the Commissioner declare that a service is an 'exempt service', but also that it "**must**" make such a declaration if asked by a provider that satisfies the definition. This would help strengthen the predictability of the bill's regulatory impact, which we believe should be a core objective of modernising the Act.

Part 4 – Basic online safety expectations

Section 45 – Basic online safety expectations

(2) The Minister may, by legislative instrument, determine that the basic online safety expectations for each relevant electronic service included in a class of relevant electronic services specified in the determination are the expectations specified in the determination.	Within the bill, we suggest providing industry with a period of grace or compliance adjustment period to enable services to comply with all new and amended BOSE (eg. 6 months). New BOSE requirements and even small changes to the BOSE may require significant changes to a service's internal systems that will necessarily take time to implement and be made effective.
	The previous Discussion Paper indicated that the BOSE would initially target social media services (although it envisaged that they may apply to other digital sectors in future). If this is still the Government's plan, we recommend reflecting this in the draft bill to aid transparency and predictability.

Section 46 – Core expectations

(1) A determination under section 45 must specify each of the following expectations: (a) the expectation that the provider of the service will take reasonable steps to ensure that end-users are able to use the service in a safe manner; (b) the expectation that, in determining what are such reasonable steps, the provider will consult the Commissioner;	We suggest removing paragraph (b), which theoretically would mean that the creator of any social media service or relevant electronic service globally would be expected to consult specifically with the Commissioner when designing their services. This would technically encompass tens of thousands of companies worldwide, including those that make low-risk services expected to have only a handful of Australian users. We are not aware of any such equivalent expectation anywhere else in the world. We believe that the expectation around reasonable steps in paragraph (a) is sufficient.
(e) the expectation that the provider of the service will ensure that the service has clear and readily identifiable mechanisms that enable end-users to report, and make complaints about, any of the following material provided on the service: (i) cyber-bullying material targeted at an Australian child; (ii) cyber-abuse material targeted at an Australian adult; (iii) a non-consensual intimate image of a person; (iv) class 1 material; (v) class 2 material; (vi) material that promotes abhorrent violent conduct; (vii) material that incites abhorrent violent conduct; (viii) material that instructs in abhorrent violent conduct; (ix) abhorrent violent material;	We suggest removing sub-paragraph (v). Unlike all the kinds of content detailed in each of the other sub-paragraphs, Class 2 material (at the R18+ level at least) is permissible and non-controversial online content and should not be treated in the same way as, for instance, non-consensual intimate images or abhorrent violent material.

(g) the expectation that, if the Commissioner, by written notice given to the provider of the service, requests the provider to give the Commissioner a statement that sets out the number of complaints made to the provider during a specified period (not shorter than 6 months) about breaches of the service's terms of use, the provider will comply with the request within 30 days after the notice of request is given;	A provider's terms of use will in all circumstances cover a far wider range of topics than just online safety (eg. copyright violation). It is not appropriate for the Commissioner to be able to request information about breaches of a provider's terms of use that are not relevant to its role. We suggest amending the relevant part of (g) as follows: "… about breaches of the provider's terms of use **relating to the online safety**…". Alternatively, the definition of 'terms of use' in section 5 of the bill could be amended so that they only relate to its online safety provisions specifically. Further, we strongly suggest amending the relevant part of paragraph (g) so that it reads: "…sets out the number of **genuine** complaints **from Australian end-users** made to the provider …". First, some of our members have reported that they often receive vexatious reports that are not found to be substantiated. This could occur, for instance, when a player reacts poorly to a loss against another player. Video game companies should not be required to report on vexatious or failed complaints as doing so would cause unjustified reputational damage. As the Commissioner's role is limited to the online safety of Australians, it is also not appropriate for providers to report on complaints that have originated from outside of Australia. More broadly, we see a disconnect between the heavy transparency obligations that the BOSE would impose on providers under paragraphs (g), (h) and (i) on one hand, and on the other hand, a lack of even basic transparency requirements in the bill for the Commissioner to report on its own activities and use of powers. Please see our comments regarding section 217 at the end of this submission for our specific suggestions.

	We urge the Government to keep the BOSE (and the minimum requirements of a BOSE in the bill) as high level and as least-prescriptive as possible. We do not see it being the role of the BOSE to impose specific requirements, which can, where needed, be dealt with more appropriately via industry codes which provide a more flexible mechanism.

Section 47 – Consultation

(1) Before making or varying a determination under section 45, the Minister must: (a) make a copy of the draft available on the Department's website; and (b) publish a notice on the Department's website: (i) stating that the Minister has prepared a draft of the determination or variation; and (ii) inviting interested persons to give written comments about the draft to the Minister within the period specified in the notice. (2) The period specified in the notice must run for at least 30 days after the publication of the notice. (3) Subsection (1) does not apply to a variation if the variation is of a minor nature. (4) If interested persons have given comments in accordance with a notice under subsection (1), the Minister must have due regard to those comments in making or varying the determination.	Considering the scale and scope of the BOSE, we suggest including an additional paragraph (c) requiring the Minister (or their delegate) to write to all relevant providers and industry bodies drawing their attention to the new or varied draft determinations.

Section 48 – Service provider notifications

(2) If the Commissioner is satisfied that the provider of a service has contravened one or more basic online safety expectations for the service, the Commissioner may: (a) prepare a statement to that effect; and (b) give a copy of the statement to the provider of the service; and (c) if the Commissioner considers that it is appropriate to publish the statement—publish the statement on the Commissioner's website.	To ensure there is transparency, fairness and that industry is given the opportunity to respond to any concerns so that they can be resolved, we recommend including a requirement for the Commissioner to consult with the provider first before it can take the action outlined in subsection (2).

Section 49 – Periodic reporting notice

Subsection (2): (b) prepare those periodic reports in the manner and form specified in the notice; and	We suggest changing paragraph (2)(b) so that it reads "prepare those periodic reports in **a reasonable** manner and form **as** specified in the notice". This will help to enhance the predictability of the regulation and to avoid unnecessarily onerous or unreasonable reporting requirements.
(4) A period ascertained in accordance with the notice as mentioned in subparagraph (2)(c)(i) must not be shorter than 28 days after the end of the interval to which the periodic report relates.	Under subsection (4), it appears that while a provider must be given 28 days from the end of the reporting period to prepare the report, there is no minimum period between receipt of the notice and the date that a report is required to be made by. Therefore, we suggest also making it a requirement in subsection (4) that the period must not be shorter than

	28 days after the receipt of the notice to ensure the provider is given a reasonable amount of time to prepare the required report in compliance with the notice. See the wording of subsection 56(4) as an example: "**The period specified in X must not be shorter than 28 days after the notice is given**".
(5) In deciding whether to give a notice under subsection (2) to the provider of a service, the Commissioner must have regard to the following: (a) the number of occasions during the previous 12 months on which complaints about material provided on the service were made to the Commissioner under this Act; (b) whether the provider has previously contravened a civil penalty provision of this Division; (c) whether there are deficiencies in the provider's practices, so far as those practices relate to the capacity of end-users to use the service in a safe manner; (d) whether there are deficiencies in the service's terms of use, so far as they relate to the capacity of end-users to use the service in a safe manner; (e) whether the provider has agreed to give the Secretary regular reports relating to the capacity of end-users to use the service in a safe manner; (f) such other matters (if any) as the Commissioner considers relevant.	To help manage the regulatory burden, we would support including additional relevant matters under subsection (5) that the Commissioner must have regard to when deciding whether to give a periodic reporting notice, such as: • Whether the information to be sought has been, or can be, sought from the provider without a need for a formal notice • Whether any or all of the information sought is already public information, and • The size and scale of the provider, the reasonable ability of the provider to give the information sought, and the regulatory impact of giving a notice to the particular provider.

Section 50 – Compliance with notice

A person must comply with a notice under subsection 49(2) to the extent that the person is capable of doing so.	We consider that it would be appropriate to include a "reasonableness" component here, which would not reduce the effectiveness of compliance but would help make the requirement fairer and more practicable for providers to comply (ie. changing the section so that it reads "… to the extent that the person is **reasonably** capable of doing so").

Section 52 – Periodic reporting determination

Subsection (2): (b) prepare those periodic reports in the manner and form specified in the notice; and	See comment in relation to paragraph 49(2)(b) above, which is also relevant here.
(4) A period ascertained in accordance with the notice as mentioned in subparagraph (2)(c)(i) must not be shorter than 28 days after the end of the interval to which the periodic report relates.	See comment in relation to subsection 49(4) above, which is also relevant here.

	We see no reason for not including a list of matters that the Commissioner must have regard to before it can make a determination under this section - similar to the list at subsection 49(5) regarding periodic reporting notices. Just as periodic reporting notices should only be given to a provider when the Commissioner identifies a supposed problem with the provider, periodic reporting determinations should only be issued when it identifies a supposed systemic problem with an industry or part of an industry.

Section 53 – Compliance with determination

A person must comply with a determination under subsection 52(2) to the extent that the person is capable of doing so.	See comment in relation to section 50 above, which is also relevant here.

Sections 56-8 (relating to non-periodic reporting notice)

See our comments for section 49 periodic reporting notices above, which are also relevant here.

Sections 59-61 (relating to non-periodic reporting determinations)

See our comments for section 52 periodic reporting determinations above, which are also relevant here.

Part 5 – Cyber-bullying material targeted at an Australian child

Section 65 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

(1) If: (a) material is provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the material was the subject of a complaint that was made to the provider of the service; and (c) the material was not removed from the service within: (i) 48 hours after the complaint was made; or (ii) such longer period as the Commissioner allows; and (d) a complaint has been made to the Commissioner under section 30 about the material; and (e) the Commissioner is satisfied that the material is or was cyber-bullying material targeted at an Australian child; the Commissioner may give the provider of the service a written notice (a ***removal notice***) requiring the provider to: (f) remove the material from the service; and (g) do so within: (i) 24 hours after the removal notice was given to the provider; or (ii) such longer period as the Commissioner allows.	We suggest there is a compelling case for including an additional requirement in subsection (1) that the Commissioner may only give the provider a written notice if "**the complainant is unable to take reasonable steps to remove the content themselves**". In the video gaming environment, it is often possible for a player to bar or block a player with a click of a button at their end, which automatically deletes all communication between the parties. Given that in most circumstances it is a far better solution to empower recipients of potential cyber-bullying material with the ability to directly deal with that material themselves, the scheme should through its design encourage such action. It would also encourage providers to invest in building systematic design-focused solutions to address cyber-bullying that potentially remove the need for (or reduce reliance upon) inefficient manual removal processes.
	There should be a requirement in this section that the material must be identified in the removal notice in a way that is sufficient to enable the provider to comply with the notice, a requirement that is included for several other notices in the draft bill.

Section 67 – Compliance with removal notice

A person must comply with a requirement under a removal notice given under section 65 or 66 to the extent that the person is capable of doing so.	We consider that it would be appropriate to include a "reasonableness" component here, which would not reduce the effectiveness of compliance but would help make the requirement fairer and more practicable for providers to comply (ie. changing the section so that it reads "… to the extent that the person is **reasonably** capable of doing so").

Section 73 – Service provider notifications

(1) If: (a) material is provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the Commissioner is satisfied that the material is or was cyber-bullying material targeted at an Australian child; and (c) a complaint has been made to the Commissioner under section 30 about the material; the Commissioner may, with the consent of the complainant, give the provider of the service a written notice that: (d) identifies the material; and (e) states the Commissioner is satisfied that the material is cyber-bullying material targeted at an Australian child. (2) If the Commissioner is satisfied that there were 2 or more occasions during the previous 12 months on which: (a) cyber-bullying material targeted at an Australian child was provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the provision of the material contravened the service's terms of use; the Commissioner may: (c) prepare a statement to that effect; and (d) publish the statement on the Commissioner's website; and (e) give a copy of the statement to the provider of the service.	We are generally not supportive of the approach taken by parts of the draft bill, including here, that seeks to take punitive action against providers (in the case of this section, by public naming and shaming under paragraph (2)(d)) for the actions of their users where the provider has taken all reasonable steps to address such actions. If an individual wishes to say something inappropriate to someone else online, no system will or even should always be able to prevent it, just as there is no way to prevent it in the playground, sporting field, at work or anywhere else people interact in the physical world. It is far more appropriate for providers to be measured for the reasonable steps they have taken to prevent or respond to such behaviours. In this way, we ask that subsections (1) and (2) be amended so that notices and statements can be given not when there has simply been cyber-bullying material posted, but when there has been cyber-bullying material posted and the provider has not reasonably dealt with it. However, if the current wording is kept, we believe there should be a positive onus on the Commissioner to consult with the provider before they can be satisfied that material is or was cyber-bullying material under paragraph (1)(b), or that there were 2 or more occasions of cyber-bullying during the previous 12 months under subsection (2). There may be other information that the Commissioner is not aware of that would be relevant (eg. if the complainant harassed the other end-user initially).

Exempt cyber-bullying material

We suggest that consideration be given to whether there should also be a category of exempt cyber-bullying material, similar to the "exempt post of an intimate image" at section 86, having regard to, for example, the nature and content of the cyber-bullying material, the relationship between the end-users, and the overall context of the material.

Part 7 – Cyber-abuse material targeted at an Australian adult

Section 88 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

(1) If: (a) material is, or has been, provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the Commissioner is satisfied that the material is or was cyber-abuse material targeted at an Australian adult; and (c) if the provider of the service is known to the adult—the material was the subject of a complaint that was made to the provider of the service; and (d) if such a complaint was made—the material was not removed from the service within: (i) 48 hours after the complaint was made; or (ii) such longer period as the Commissioner allows; and (e) a complaint has been made to the Commissioner under section 36 about the material; and (f) the material was posted on the service by an end-user of the service; the Commissioner may give the provider of the service a written notice, to be known as a ***removal notice***, requiring the provider to: (g) take all reasonable steps to ensure the removal of the material from the service; and (h) do so within: (i) 24 hours after the notice was given to the provider; or (ii) such longer period as the Commissioner allows.	Please see our comments regarding section 65 above, which are also relevant here.
(2) So far as is reasonably practicable, the material must be identified in the removal notice in a way that is sufficient to enable the provider of the service to comply with the notice.	Please see our comments regarding section 65 above, which are also relevant here.

Section 89 – Removal notice given to an end-user

(1) If: (a) material is, or has been, provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the Commissioner is satisfied that the material is or was cyber-abuse material targeted at an Australian adult; and (c) if the provider of the service is known to the adult—the material was the subject of a complaint that was made to the provider of the service; and (d) if such a complaint was made—the material was not removed from the service within: (i) 48 hours after the complaint was made; or (ii) such longer period as the Commissioner allows; and (e) a complaint has been made to the Commissioner under section 36 about the material; and (f) the material was posted on the service by an end-user of the service; the Commissioner may give the end-user a written notice, to be known as a ***removal notice***, requiring the end-user to: (g) take all reasonable steps to ensure the removal of the material from the service; and (h) do so within: (i) 24 hours after the notice was given to the end-user; or (ii) such longer period as the Commissioner allows.	We suggest that paragraph (1)(d) be removed. We question why end-user notices may only be provided after 48 hours has passed from when a complaint has been made to the provider of the service. We envisage that there will be circumstances where, if it is practicable, it will be in the best interests of both the complainant and the end-user (who posted the material) that the end-user be initially approached to remove that material, rather than the provider. In such circumstances, the Commissioner should not be prevented from issuing an end-user notice as early as possible.

Section 93 – Service provider notifications

(1) If: (a) material is, or has been, provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the Commissioner is satisfied that the material is or was cyber-abuse material targeted at an Australian adult; and (c) a complaint has been made to the Commissioner under section 36 about the material; and (d) the material was posted on the service by an end-user of the service; the Commissioner may, with the consent of the complainant, give the provider of the service a written notice that: (e) identifies the material; and (f) states the Commissioner is satisfied that the material is cyber-abuse material targeted at an Australian adult. (2) If the Commissioner is satisfied that there were 2 or more occasions during the previous 12 months on which: (a) cyber-abuse material targeted at an Australian adult was provided on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the material was posted on the service by an end-user of the service; and (c) the provision of the material contravened the service's terms of use; the Commissioner may: (d) prepare a statement to that effect; and (e) publish the statement on the Commissioner's website; and (f) give a copy of the statement to the provider of the service.	Please see our comments regarding section 73 above, which are also relevant here.

Exempt cyber-abuse material

As per our comments regarding cyber-bullying material earlier, we suggest that consideration be given to whether there should also be a category of exempt cyber-abuse material, similar to the "exempt post of an intimate image" at section 86, having regard to, for example, the nature and content of the cyber-abuse material, the relationship between the end-users, and the overall context of the material.

Part 8 – Abhorrent violent material

Section 95 – Blocking request

(2) The following are examples of steps that may be specified in the blocking request: (a) steps to block domain names that provide access to the material; (b) steps to block URLs that provide access to the material; (c) steps to block IP addresses that provide access to the material.	To ensure that this very strong power is used as precisely as possible, we suggest making it a requirement in this section that the steps included in a blocking request be reasonable in the circumstances, or be limited to what is reasonably necessary to remove the abhorrent violent material without impacting on other unrelated content. For example, a blocking request should not create a requirement to block a top-level domain where simply blocking specific URLs may be sufficient (noting in other circumstances a domain-wide block may be necessary).
(5) In deciding whether to give the blocking request, the Commissioner must have regard to the following matters: (a) whether any other power conferred on the Commissioner could be used to minimise the likelihood that the availability of the material online could cause significant harm to the Australian community; (b) such other matters (if any) as the Commissioner considers relevant.	We suggest including an additional paragraph in subsection (5) of: "**whether the provider is already taking steps or has committed to taking steps to prevent access to the material online**". This would better reflect the fact that blocking requests are necessarily an extreme measure and should generally be used as a last resort.

Section 99 – Blocking notice

See our comments for blocking requests above, which are also relevant here.

Part 9 – Online content scheme

Section 106 – Class 1 material

Subsection 1: (e) material where the following conditions are satisfied: (i) the material is a computer game; (ii) the computer game has been classified as RC by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995*; or (f) material where the following conditions are satisfied: (i) the material is a computer game; (ii) the computer game has not been classified by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995*; (iii) if the computer game were to be classified by the Classification Board under that Act—the computer game would be likely to be classified as RC; or	In the absence of modernisation of the National Classification Scheme (NCS), which the Government has committed to doing, the current wording of this section treats video game material harshly and unfairly compared to film, publications, and content that is neither film, publications nor computer games (cumulatively, literally every kind of online material other than video games) due to the out-of-date definition of RC. As a result of the key legislation that underpins the NCS being drafted (and substantially unchanged) during the mid-90s when the moral panic around video games was arguably at its highest, video games are classified more stringently than films, and more harshly in Australia than in many other territories around the world, including in relation to RC, without just cause. We talk about this in detail in our submission to the then Department of Communications and the Arts in response to the recent review of Australian classification regulation. This is a genuine, practical issue as there have historically been several videos games that have been Refused Classification only in Australia and nowhere else. These out-of-date rules have been criticised by the previous Director of the Classification Board, and we understand that the Government's recent review of the NCS has recognised them as problematic. If the current approach of using RC as the standard for Class 1 materials is kept, we urge the Government to prioritise the completion of its classification review as soon as possible to prevent problems arising as a result of the draft bill.
	The proposed revised scheme does not currently provide for exempt material (except in a limited way concerning judicial or governmental material). By contrast, section 104 outlines material that is exempt abhorrent violent material. We recommend providing for

	material that is exempt from the Online Content Scheme in a similar way.

Section 107 – Class 2 material

Subsection 1: (j) material where the following conditions are satisfied: (i) the material is a computer game; (ii) the computer game has been classified as R 18+ by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995*; or (k) material where the following conditions are satisfied: (i) the material is a computer game; (ii) the computer game has not been classified by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995*; (iii) if the computer game were to be classified by the Classification Board under that Act—the computer game would be likely to be classified as R 18+; or	First, we provide our appreciation to the Department for listening to IGEA and other stakeholders, including the ACMA, who presented the point that MA15+ level content should not fall within the scope of the Online Content Scheme. However, we urge the Department to go further and to reconsider the definition of Class 2 material so that it also excludes R18+ content. As we argued in our prior submission, the Online Content Scheme should not impose regulation on content that is both legal and already subject to classification regulation. As the ACMA noted in its prior submission, the approach proposed in the Discussion Paper (which is continued in the draft bill with respect to R18+ material) creates regulatory duplication as it "could potentially require both the Office of the eSafety Commissioner and the relevant classification regulatory body (such as the ACMA) to assess classification or determine compliance for the same content", and would also cover material that "may no longer fall into the illegal and harmful content category in a contemporary media environment". Unreasonable regulation of R18+ content is inconsistent with the first and arguably most important tenant of Australian classification and censorship policy, being that adults should be able to read, hear, see and play what they want". (National Classification Code).
	If R18+ material is not removed from the scope of Class 2 material, however, our comments that we have made in relation to section 106 above concerning the need for the Government to progress its reform of the classification categories also apply here in relation to R18+. The NCS currently treats video game content harsher than film content due to out-of-date misconceptions around games in the 1990s when the scheme was created. One example that we have provided in our submission on

	classification reform (link above) is the fact that all interactive drug use in games must be R18+ as a minimum. This means that a game like *Beyond: Two Souls* which uses interactivity thoughtfully to explore peer pressure and show the harms of drug use inevitably ends up with a higher classification than a film like *Pineapple Express*, a stoner film named literally after a strain of marijuana.

Section 108 – Restricted access system

(1) The Commissioner may, by legislative instrument, declare that a specified access-control system is a ***restricted access system*** in relation to material for the purposes of this Act. Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*. (2) An instrument under subsection (1) may make different provision with respect to different kinds of material. (3) Subsection (2) does not limit subsection 33(3A) of the *Acts Interpretation Act 1901*. (4) In making an instrument under subsection (1), the Commissioner must have regard to: (a) the objective of protecting children from exposure to material that is unsuitable for children; and (b) the extent to which the instrument would be likely to result in a financial or administrative burden on providers of the following services: (i) social media services; (ii) relevant electronic services; (iii) designated internet services; and (c) such other matters (if any) as the Commissioner considers relevant. (5) The Commissioner must ensure that an instrument under subsection (1) is in force at all times after the commencement of this section.	It is not clear to us why it is necessary or beneficial to have separate definitions of an 'access-control system' and a 'restricted access system'. By its very definition, an 'access-control system' is already a system that restricts access, and we believe it is sufficient and suitable that this definition alone be adopted throughout the bill. Another reason why we consider that the definition of 'access-control system' be used is that we are also concerned that the definition of 'restricted access system' is not contained in the primary legislation but is solely to be determined by the Commissioner, with the only check or balance being the very limited provisions of subsection (4). The problems of this approach are that there is an absence of Parliamentary scrutiny and, more importantly, a lack of clarity and predictability for industry. Particularly in the absence of Parliamentary scrutiny, we are also concerned that the specifications for a 'restricted access system' could be set at too prescriptive a level for one or more providers to reasonably comply with them, or for the parameters of such specifications to be set in a way that is inconsistent with what is practically achievable. For the sake of argument, under the current approach, it would be possible for the Commissioner to declare that the only access-control systems that are restricted access systems are ones that use age-verification technology, which is not technology that currently exists in a reliable way or in a way that does not

	also carry significant privacy risks (so much so that the UK Government abandoned its plans to impose an age-verification requirement for online adult content). While subsection (4) creates a requirement for the Commissioner to consider the risk of "financial or administrative burden", it is not a requirement with weight and enables any such considerations to be ignored. If separate definitions are kept, we suggest that this section be amended by providing a non-exhaustive list of access-control systems that should be considered restricted access systems, such as parental controls, alongside the power of the Commissioner to supplement this list through a legislative instrument under subsection (1). This would provide at least a baseline of predictability for industry. We also recommend the inclusion of an additional requirement for the Commissioner to both consult publicly as well as to consider stakeholder views before making a legislative instrument

Section 109 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

(2) So far as is reasonably practicable, the material must be identified in the removal notice in a way that is sufficient to enable the provider of the service to comply with the notice.	We suggest removing "So far as is reasonably practicable" from subsection (2) as we do not consider that this qualification is appropriate in this context. Rather, the material *must* be identified in the removal notice in a way that is sufficient to enable the provider to comply with the notice. By definition, anything less means that the provider will not have the information it needs to comply.

Section 110 – Removal notice given to a hosting service provider

	We recommend making it a requirement that this power under section 110 must not be exercised until a reasonable attempt has been made to first request the relevant provider of a social media service, relevant electronic service or designated internet service (ie. the primary provider of the material) to remove the material under section 109.

(2) So far as is reasonably practicable, the material must be identified in the removal notice in a way that is sufficient to enable the hosting service provider to comply with the notice.	Please see our comment in relation to section 109 above, which also applies here.

Section 111 – Compliance with removal notice

A person must comply with a requirement under a removal notice given under section 109 or 110 to the extent that the person is capable of doing so.	We consider that it would be appropriate to include a "reasonableness" component here, which would not reduce the effectiveness of compliance but would help make the requirement fairer and more practicable for providers to comply (ie. changing the section so that it reads "… to the extent that the person is **reasonably** capable of doing so").

Comments regarding sections 114 – 135

- Our comment above relating to section 109, suggesting the removal of the phrase "so far as is reasonably practicable" also applies to the following sections:
    - Section 114 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service
    - Section 119 – Remedial notice given to the provider of a social media service, relevant electronic service or designated internet service
    - Section 124 – Link deletion notice
    - Section 128 – App removal notice
- Our comment above relating to section 110, recommending that a notice only be given to a hosting service provider after a reasonable attempt has been made to first send a notice to the relevant social media service, relevant electronic service or designated internet service, also applies to the following sections:
    - Section 115 – Removal notice given to a hosting service provider
    - Section 120 – Remedial notice given to a hosting service provider
- Our comment above relating to section 111, recommending the inclusion of a 'reasonableness' component, also applies to the following sections:
    - Section 116 – Compliance with removal notice
    - Section 121 – Compliance with remedial notice
    - Section 125 – Compliance with link deletion notice
    - Section 129 – Compliance with app removal notice

Section 124 – Link deletion notice

(4) The Commissioner must not give the link deletion notice unless: (a) the Commissioner is satisfied that there were 2 or more times during the previous 12 months when end-users in Australia could access class 1 material using a link provided by the service; and (b) during the previous 12 months: (i) the Commissioner gave one or more removal notices under section 109 or 110 in relation to class 1 material that could be accessed using a link provided by the service; and (ii) those removal notices were not complied with.	The power to delete links under section 124 is extremely powerful. While we know this action is limited to Class 1 material and can only be used when certain conditions are met, including that a removal notice has not been complied with, we are concerned that the threshold for using section 124 is not as high as the impact of this power should require it to be (ie. it is too easily triggered). Among other things, it potentially imposes a heavy regulatory burden by co-opting search engines to act as sheriffs against content owners they otherwise have no relationship with. If this power is kept, we recommend tightening the circumstances under which it can be used, such as by making it a requirement that before a link deletion notice can be given, that the Commissioner has first taken all other available steps to compel the specific provider of the Class 1 material to remove it. There should also be a condition that a notice can only be provided where "**the Commissioner is satisfied that the availability of a link is likely to cause significant harm to the Australian community**" (see the wording of section 95).

Section 128 – App removal notice

(4) The Commissioner must not give the app removal notice unless: (a) the Commissioner is satisfied that there were 2 or more times during the previous 12 months when end-users in Australia could use the service to download an app that facilitates the posting of class 1 material; and (b) during the previous 12 months: (i) the Commissioner gave one or more removal notices under section 109 or 110 in relation to class 1 material, the posting of which is facilitated by the app; and (ii) those removal notices were not complied with.	We strongly urge the Department to remove section 128 from the draft bill. The power to require an app distribution service to remove an app under section 128 is even more powerful than the power to delete a link, not only because of the consequences for the provider of the material, but because it also potentially exposes the app distribution services to serious legal, financial and reputational risks given that there will likely be a contractual arrangement between the parties for hosting an app. Further, while Class 1 material will often be illegal or harmful material, where the use of such a power could be justified, it is not exclusively so. Due to the highly out-of-date reality of the Classification Code, there is much content that is current RC, including video games, that

	is no longer inconsistent with community standards, and that a reasonable person would not regard as harmful. If this power is kept, we believe it must be tightened so that before it can be used, the Commissioner must have first taken all other steps to compel the specific provider of the Class 1 material to remove it. There should also be a condition that a notice can only be provided where "**the Commissioner is satisfied that the availability of the app is likely to cause significant harm to the Australian community**" (see the wording of section 95). We also believe it should be subject to review and/or sunsetting so that its regulatory impact can be considered and re-assessed in future.

Section 135 – Sections of the online industry

(1) For the purposes of this Division, ***sections of the online industry*** are to be ascertained in accordance with this section. (2) For the purposes of this Division, each of the following groups is a ***section of the online industry***: (a) the group consisting of providers of social media services, so far as those services are provided to end-users in Australia; (b) the group consisting of providers of relevant electronic services, so far as those services are provided to end-users in Australia; (c) the group consisting of providers of designated internet services, so far as those services are provided to end-users in Australia; (d) the group consisting of providers of internet search engine services, so far as those services are provided to end-users in Australia; (e) the group consisting of providers of app distribution services, so far as those services are provided to end-users in Australia; (f) the group consisting of providers of hosting services, so far as those services host material in Australia; (g) the group consisting of providers of internet carriage services, so far as those services are provided to customers in Australia; (h) the group consisting of persons who manufacture, supply, maintain or install any of the following equipment: (i) equipment that is for use by end-users in Australia of a social media service in connection with the service; (ii) equipment that is for use by end-users in Australia of a relevant electronic service in connection with the service; (iii) equipment that is for use by end-users in Australia of a designated internet service in connection with the service; (iv) equipment that is for use by end-users in Australia of an internet carriage service in connection with the service.	We understand that it is the Government's intention that the definition of 'sections of the online industry' as outlined in this section is not meant to be rigid, strict or exclusive, but rather is flexible and can accommodate other groups or sub-groups of providers as may be reasonably identified or self-determined. However, this intention is not clear in the current draft bill. There are many ways to fix this, but one option is to change the phrase "… the group consisting of …" in each of paragraphs (a)–(h) of this section (and as needed elsewhere in this Part) to "… the group **or an appropriate sub-group** consisting of …". An example of why this change is needed is because it could currently be read in the draft bill that there will only be a single 'group consisting of providers of relevant electronic services', even though this group is a legislative construct that in reality consists of several very different kinds of online providers for which there is no overarching industry body.

Section 136 – Participants in a section of the online industry

For the purposes of this Division, if a person is a member of a group that constitutes a section of the online industry, the person is a ***participant*** in that section of the online industry.	We recommend that the section be amended to recognise the fact that the sections of the online industry themselves will not always be absolute

	or clear cut, and that some providers may have compelling links to two or more 'groups', an issue that is likely to increase as the online industry continues to evolve and the services of providers become more diversified and blur. One way to address this would be to make it clear in the draft bill that where a person can reasonably be considered to be a member of more than one group: "**a person may choose to be a member of the group that it reasonably considers to be the most appropriate**".

Section 137 – Statement of regulatory policy

(1) The Parliament intends that bodies or associations that the Commissioner is satisfied represent sections of the online industry should develop codes (***industry codes***) that are to apply to participants in the respective sections of the industry in relation to their online activities.	Please see our comments regarding section 135 above, which are also relevant here. References to 'sections' in this Part should be able to accommodate both groups and sub-groups as may be appropriate.
(2) The Parliament intends that the Commissioner should make reasonable efforts to ensure that, for each section of the online industry, either: (a) an industry code is registered under this Division within 6 months after the commencement of this Division; or (b) an industry standard is registered under this Division within 12 months after the commencement of this Division.	Given the complexity and scope that some industry codes would be expected to cover (eg. the non-exhaustive list of matters that a code could cover includes 36 examples) and the fact that in some instances new industry bodies may need to be formed for some sections of the online industry, we recommend that a minimum of 12 months rather than 6 months initially be allowed for industry codes to be developed and registered. For example, we understand that the processes that the Communications Alliance currently undertake to develop and implement codes for the Internet industry generally requires substantially longer than 6 months.

Section 138 – Examples of matters that may be dealt with by industry codes and industry standards

(3) The examples are as follows: (a) procedures for dealing with class 1 material, or class 2 material, provided on a social media service; (b) procedures for dealing with class 1 material, or class 2 material, provided on a relevant electronic service; (c) procedures for dealing with class 1 material, or class 2 material, provided on a designated internet service; (d) procedures directed towards the achievement of the objective of ensuring that, in the event that a participant in the providers of internet carriage services section of the online industry becomes aware that a hosting service provider is hosting class 1 material, or class 2 material, in Australia, the hosting service provider is told about the material; (e) procedures to be followed in order to inform producers of online content about their legal responsibilities in relation to that content; (f) procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult; (g) procedures directed towards the achievement of the objective of ensuring that customers have the option of subscribing to a filtered internet carriage service; (h) giving end-users information about the availability, use and appropriate application of online content filtering software; (i) providing end-users with access to technological solutions to help them limit access to class 1 material and class 2 material; (j) providing end-users with advice on how to limit access to class 1 material and class 2 material; (k) action to be taken to assist in the development and implementation of online content filtering technologies (including labelling technologies); (l) promoting awareness of the safety issues associated with social media services; (m) promoting awareness of the safety issues associated with relevant electronic services; (n) promoting awareness of the safety issues associated with designated internet services; (o) procedures to be followed in order to deal with safety issues associated with social media services; (p) procedures to be followed in order to deal with safety issues associated with relevant electronic services; (q) procedures to be followed in order to deal with safety issues associated with designated internet services; (r) giving parents and responsible adults information about how to supervise and control children's access to material provided on social media services; (s) giving parents and responsible adults information about how to supervise and control children's access to material provided on relevant electronic services; (t) giving parents and responsible adults information about how to supervise and control children's access to material provided on designated internet services; (u) telling persons about their rights to make complaints; (v) procedures to be followed in order to deal with complaints about class 1 material, or class 2 material, provided on social media services; (w) procedures to be followed in order to deal with complaints about class 1 material, or class 2 material, provided on relevant electronic services; (w) procedures to be followed in order to deal with complaints about class 1 material, or class 2 material, provided on relevant electronic services; (x) procedures to be followed in order to deal with complaints about class 1 material, or class 2 material, provided on designated internet services; (y) procedures to be followed in order to deal with reports about class 1 material, or class 2 material, provided on social media	While we know that industry codes for different sections of the online industry would not be expected to address all of the examples provided in subsection (3), but rather only the most relevant, the list of examples provided at subsection (3) are nevertheless unwieldy and lengthy. There are also so many examples listed that it is impossible for any section of the online industry to know how to approach developing an industry code or to determine the scope of issues it needs to cover. As a minimum, it would be helpful for these examples to be consolidated into fewer, less prescriptive and higher-level principles to aid clarity and predictability for industry. We would also suggest the following specific changes: • The references to Class 2 material, at least in relation to R18+ rated content, should be removed from subsection (3), such as in paragraphs (d), (i), (j), (zc), (zd) and (ze). R18+ content should be clearly differentiated from Class 1 material as it can be legally accessed by adults. • It is not our understanding that paragraph (f) reflects government policy. If not, it should be removed from this list. For example, there are many instances where it is legal, appropriate and in compliance with an app's terms of service for a teenager 13 years or older to have an online account without necessarily having the express consent of a parent or carer. We are also concerned that there are very few, if any, legal limits on the matters that could be forced to be addressed in industry codes, even where they are unnecessary, unreasonable or would impose a heavy regulatory burden on providers that is disproportionate to the risk. To provide clarity and predictability to industry not

services, where the reports are made by or on behalf of end-users of those services; (z) procedures to be followed in order to deal with reports about class 1 material, or class 2 material, provided on relevant electronic services, where the reports are made by or on behalf of end-users of those services; (za) procedures to be followed in order to deal with reports about class 1 material, or class 2 material, provided on designated internet services, where the reports are made by or on behalf of end-users of those services; (zb) procedures to be followed in order to deal with complaints about unsolicited electronic messages that promote or advertise one or more: (i) websites; or (ii) distinct parts of websites; or (iii) apps; that enable, or purport to enable, end-users to access class 1 material or class 2 material; (zc) if: (i) class 2 material is provided on a social media service; and (ii) the service is provided from a foreign country; and (iii) the provider of the service has reasonable grounds to believe that the material is hosted in Australia; procedures to be followed to ensure the Commissioner is notified of the material; (zd) if: (i) class 2 material is provided on a relevant electronic service; and (ii) the service is provided from a foreign country; and (iii) the provider of the service has reasonable grounds to believe that the material is hosted in Australia; procedures to be followed to ensure the Commissioner is notified of the material; (ze) if: (i) class 2 material is provided on a designated internet service; and (ii) the service is provided from a foreign country; and (iii) the provider of the service has reasonable grounds to believe that the material is hosted in Australia; procedures to be followed to ensure the Commissioner is notified of the material; (zf) the referral to the Commissioner of complaints about matters, where the complainant is dissatisfied with the way in which the complaint was dealt with under the code or standard; (zg) ensuring that end-users are provided with information, and support services, relating to online safety for Australians; (zh) the making and retention of material directed towards the achievement of the objective of ensuring that, in the event that new social media services are developed that could put at risk the safety of children who are end-users of the services, the Commissioner is informed about those services; (zi) the making and retention of material directed towards the achievement of the objective of ensuring that, in the event that new relevant electronic services are developed that could put at risk the safety of children who are end-users of the services, the Commissioner is informed about those services; (zj) the making and retention of material directed towards the achievement of the objective of ensuring that, in the event that new designated internet services are developed that could put at risk the safety of children who are end-users of the services, the Commissioner is informed about those services.	only around the matters a code may be required to address, but also matters that it would *not* reasonably be expected to deal with, it may also be helpful for this section to include provisions that set reasonable limits or parameters around the scope of industry codes.

Section 140 – Registration of industry codes

(1) This section applies if: (a) the Commissioner is satisfied that a body or association represents a particular section of the online industry; and (b) that body or association develops an industry code that applies to participants in that section of the industry and deals with one or more matters relating to the online activities of those participants; and	Please see our comment regarding sections 135 and 137 above, which are also relevant here.
(d) the Commissioner is satisfied that: (i) to the extent to which the code deals with one or more matters of substantial relevance to the community—the code provides appropriate community safeguards for that matter or those matters; and (ii) to the extent to which the code deals with one or more matters that are not of substantial relevance to the community—the code deals with that matter or those matters in an appropriate manner; and	Paragraph (d) currently provides the Commissioner with sole discretion for determining whether the content of an industry code is or is not appropriate. This discretion is powerful, particularly given that there are few limits on what codes may be expected to deal with, and the Commissioner also has the power to compel a provider to comply with a code. To increase the clarity, predictability and transparency of the regulatory framework to industry and the public, we suggest that this section be amended to include guidance or parameters around when an industry code is to be considered sufficient for registration. As a minimum, this section should be amended to provide a minimum threshold around which the Commissioner *must* accept a code beyond simply a standard of 'appropriateness' that is difficult to dispute on objective grounds. This is the only way to provide industry with the predictability it needs for compliance. It could also be a requirement that in considering whether a code can be registered, the Commissioner is required to consider the profile of the online safety risks relating to that section of the online industry, the number of complaints it has received regarding that section, and the likely impact of the administrative or regulatory burden on providers in that section.

Section 141 – Commissioner may request codes

(2) The period specified in a notice under subsection (1) must run for at least 120 days.	We would recommend a longer period of time (eg. 6 months as a minimum). The drafting, negotiation and industry-wide consultation processes needed to prepare a new code will almost certainly take more than 120 days.

Section 145 – Commissioner may determine an industry standard

(1) The Commissioner may, by legislative instrument, determine a standard that applies to participants in a particular section of the online industry. Note: For variation and revocation, see subsection 33(3) of the *Acts Interpretation Act 1901*. (2) A standard under this section is to be known as an ***industry standard***. (3) The Minister may, by legislative instrument, give the Commissioner a written direction as to the exercise of the Commissioner's powers under this section.	To reflect a cooperative industry-government relationship and a co-regulatory scheme, which we see this part of the draft bill being, we believe that the Commissioner should only be able to determine an industry standard in the absence of a satisfactory code (or the likelihood of one) for a particular section or sub-section of the online industry. Given that the Commissioner must be 'satisfied' with all codes, we see no risk to the Government of this approach. We understand that it is already the intention of the Government that standards fill the gaps where industry codes do not exist, and if this is so, then this should be made clear in the draft bill to prevent standards from being made pre-maturely.

Section 146 – Compliance with industry standards

If: (a) an industry standard that applies to participants in a particular section of the online industry is registered under this Division; and (b) a person is a participant in that section of the online industry; the person must comply with the industry standard.	We suggest that the draft bill also provide for possible exemptions to industry standards, such as the exemptions from service provider determinations provided under section 152.

Section 160 – Commissioner may obtain advice from the Classification Board

(1) The Commissioner may request the Classification Board to:	We strongly encourage that section 160 be amended so that, at least where it is practicable to do so, the Commissioner "**must**", not "may", request the Classification Board to advise the Commissioner whether the material is Class 1 or Class 2. If the Online Content Scheme is to use the classification categories of the National Classification Scheme as its content standard benchmark, it makes sense that the Australian Government's body that has been solely tasked with maintaining that standard and making classification decisions should be tasked with that role under the Online Content Scheme also. Under the current proposed framework, there will be two separate government bodies tasked with making classification assessments, with the primary proposed decision-maker (the Commissioner) being the far less experienced one. This duplication of functions was a problem

	that the ACMA highlighted in its prior submission to the earlier consultation on these reforms.
(2) The Classification Board may give the advice requested by the Commissioner. (3) Subsection (2) does not, by implication, limit the matters that may be taken into account by the Commissioner in considering:	We recommend amending "may" to "**must**".

Part 11 – Administrative provisions relating to the Commissioner

Section 167 – Appointment of the Commissioner

(2) A person is not eligible for appointment as the Commissioner unless the Minister is satisfied that the person has: (a) substantial experience or knowledge; and (b) significant standing; in at least one of the following fields: (c) the operation of social media services; (d) the operation of the internet industry; (e) public engagement on issues relating to online safety; (f) public policy in relation to the communications sector.	Subsection (2) should be amended so that the list of the fields that the Minister must be satisfied a person has experience or standing in, to be eligible for appointment as the Commissioner, also includes "**the operation of relevant electronic services**".
	Given the constructive findings of the Briggs Review, the significant expansion of the Commissioner's role and powers over a short period of time since the Office was created, as well as the rapidly-evolving nature of the online environment, we suggest including in the legislation a requirement for the Minister to conduct a review of the operation of the Act and other matters within a certain number of years following the passage of the draft bill, similar to the existing section 107 ('Review of this Act etc.') of the *Enhancing Online Safety Act 2015*.

Part 13 – Information-gathering powers

Section 194 – Commissioner may obtain end-user identity information or contact details

(1) This section applies to a person if: (a) the person is the provider of: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the Commissioner believes on reasonable grounds that the person has: (i) information about the identity of an end-user of the service; or (ii) contact details of an end-user of the service; and (c) the Commissioner believes on reasonable grounds that the information is, or the contact details are, relevant to the operation of this Act. *Requirement* (2) The Commissioner may, by written notice given to the person, require the person: (a) if subparagraph (1)(b)(i) applies—to give to the Commissioner, within the period and in the manner and form specified in the notice, any such information; or (b) if subparagraph (1)(b)(ii) applies—to give to the Commissioner, within the period and in the manner and form specified in the notice, any such contact details.	We are concerned with the inclusion of this power in the draft bill. This power is a remarkable and highly intrusive power, not only in relation to the providers that would be subject to it but particularly concerning potential end-users. While we are overall supportive of the Commissioner's use of end-user notices, noting that in many if not most instances (with social media and chat services) the end-user will be easily identifiable or is already known to the complainant, we believe there are significant risks to having a power that would seek to compel providers to provide data about end-users. For reasons including online safety, privacy, and compliance with international data protection laws, anonymity and the minimal collection of personal information is ingrained into the operations of most video game providers. As we noted in our prior submission, this anonymity also means that it will be often very difficult or improper, if not impossible, for a provider to disclose any relevant information about an end-user to the Commissioner or another third party, and even where technically it may be possible to share such data, a requirement to do so may require them to breach data protection laws overseas. If this power is kept, as a minimum we would suggest two changes: First, references to "… an end-user of the service…" in this section should be changed to: "… an end-user of the service **in Australia** …". We do not believe it is appropriate (or in some cases even legal) for providers to be compelled to provide sensitive personal information on non-Australian end-users. Second, a caveat or defence should be added to make it clear that the provider may only provide the requested data where it is reasonably practicable for

	them to do so, and where it would not require them to breach any laws.

Section 195 – Compliance with notice

A person must comply with a requirement under section 194 to the extent that the person is capable of doing so.	Consistent with the comments above concerning section 194, there should only be a requirement for compliance where a person "is **reasonably** capable of doing so".

Part 14 – Investigative powers

Section 205 – Non-compliance with requirement to give evidence

(1) A person required to answer a question, to give evidence or to produce documents under this Part must not: (a) when required to take an oath or make an affirmation, refuse or fail to take the oath or make the affirmation; or (b) refuse or fail to answer a question that the person is required to answer; or (c) refuse or fail to produce a document that the person is required to produce. Penalty: Imprisonment for 12 months.	Many aspects of the powers given to the Commissioner in Part 14 resemble those given to federal law enforcement and criminal intelligence agencies. For example, failure to comply with the broad range of powers given to the Commissioner may result in imprisonment for 12 months under this section, which is difficult to reconcile with an agency that outside of its very specific complaint-focused regulatory functions largely has an education and awareness-raising role. Given that all of the other penalties outlined in the draft bill are civil penalties, it is not clear why a criminal penalty is needed in this instance. Notwithstanding the defence provided in subsection (3), we strongly urge that the inclusion of a criminal penalty at subsection (1) be re-considered.
(3) Subsections (1) and (2) do not apply if the person has a reasonable excuse.	Throughout the entire draft bill, the defence of "[provision x] do not apply if the person has a reasonable excuse" has only been included in this section. We recommend including this defence for each other compliance-related obligation outlined in the draft bill.

Part 15 – Disclosure of information

Section 212 – Disclosure to certain authorities

(g) an authority of a foreign country responsible for regulating either or both of the following matters: (i) matters relating to the capacity of individuals to use social media services and electronic services in a safe manner; (ii) matters relating to material that is accessible to, or delivered to, the end-users of social media services and electronic services; (h) an authority of a foreign country responsible for enforcing one or more laws of the foreign country relating to either or both of the following matters: (i) matters relating to the capacity of individuals to use social media services and electronic services in a safe manner; (ii) matters relating to material that is accessible to, or delivered to, the end-users of social media services and electronic services.	We see significant risks with, and question the appropriateness of, enabling the Commissioner to disclose information that it holds to authorities of foreign countries, especially as the disclosure does not need to necessarily be related to online safety purposes. We recommend that paragraphs (g) and (h) be removed entirely. However, if they are kept, as a minimum, the references to "either or both of the following matters" should be amended to "**both of the following matters**" only.

Section 217 – Disclosure of summaries and statistics

The Commissioner may disclose: (a) summaries of de-identified information; and (b) statistics derived from de-identified information.	As a general point, the draft bill significantly increases the Commissioner's powers, without providing for any additional reporting or transparency requirements. As we outlined in our prior submission, the Commissioner currently only provides minimal reporting around its activities, how it resolves complaints and how and how often it uses its powers. In addition to this power to disclosure, we recommend that the draft bill be amended to include some minimum reporting requirements to increase transparency and understanding around the Commissioner's use of its powers, not only to industry but the community. These could include a requirement to report at least annually on, for instance: • the number of complaints it receives and the number of legitimate and non-legitimate (eg. found not to be substantive) complaints • the origin of those complaints (ie. what sectors they relate to) and what those complaints pertain to (eg. type of cyber-bullying) • whether and how those complaints were resolved, and • whether and how its powers have been used.

Any questions?

[redacted]

For more on IGEA and what we do, visit igea.net or follow us on Twitter below:

IGEA: @igea

The Arcade: @TheArcadeMelb

Game Connect Asia Pacific: @GCAPConf

The Australian Game Developer Awards: @The_AGDAs