interactive games & entertainment association

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

Response to Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation

November 2021

Introduction

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 makers of the most popular gaming platforms, consoles, and devices. IGEA also manages 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 further organises the annual Games Connect Asia Pacific (GCAP) conference for Australian game developers, and the Australian Game Developer Awards (AGDAs) that celebrate the best Australian-made games each year. IGEA's full list of members is available on our website.

We thank the Department for the opportunity to respond to the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 ('the draft determination') and are particularly appreciative of the extended window for submissions. Our submission is set out in two parts. The **first part** provides our specific suggested amendments to the provisions of the draft determination and the rationale for our recommendations. The **second part** provides further suggestions of some additional matters that we believe the draft determination should also address or include. Finally, the views expressed in this submission are subject to the views of any other submission that IGEA co-sponsors with other industry stakeholders.

Background

Video game play in Australia

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 in a positive way. Especially during the past 18 months of COVID disruptions and necessary lockdown measures, video games have provided a vital outlet for encouraging and helping Australians to self-isolate by keeping them positive, occupied, and connected to their family and friends as they play together.

Our Digital Australia research has also found that parents are not only highly engaged in how their children play games, but the parent/child gaming relationship is getting even closer. Most parents and carers play games in the same room as their children, while over half even play games with them online. Most parents that we surveyed as part of our research told us that they 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 established rules around how their children play.

Our industry's approach 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 effective technologies and design features aimed at supporting online safety as the video games sector.

Key technologies and processes implemented by our members to enable children and their parents and carers to prevent access to non-age appropriate content include:

1. Strict compliance with the National Classification Scheme to ensure that video games available to Australians are appropriate classified.
2. Development and rollout of the International Age Ratings Coalition (IARC) classification tool (now co-governed by the Australian Government) leading to the classification of millions of mobile and online games and non-game apps.
3. Omnipresent parental and family controls, which may include parental locks, restricted child accounts (eg. where access to MA15+ or R18+ content can be blocked), custom content restrictions, tools for monitoring and limiting child screen activity, internet filters, and companion apps for parents.
4. 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.
5. Highly limited overall player-to-player chat functionality, controlled via the blocking of unsolicited communications, the deployment of automatic text filters, and muting, blocking, and reporting tools.
6. Privacy and anonymity features including customisable visibility settings, anonymised or pseudonymised accounts, and the ability to create restricted or closed game lobbies, clans, and levels for private monitored play between family members and friends.
7. Community standards and terms of services, as well as disciplinary action to enforce them.

To support these measures, our sector takes a proactive approach to raising awareness and undertaking education around parental controls and responsible game play. All major gaming platforms publish easy-to-find information on how parents and carers can access these tools. IGEA's website has a parental resources hub that provides information on family controls and online safety features, 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 together in both a fun and safe way. We also research how Australian players and their parents and carers engage in online safety to help inform our own and our members' activities.

Our sector is continually innovating to improve on the ways to enable children and their parents and carers to better control the content they access online, such as through the creation of new security technologies or investment in advanced data-driven AI. Our industry is also working together to achieve these goals. For example, in December last year, Nintendo, Sony, and Microsoft announced the following set of Shared Online Safety Principles:

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

Recommended text amendments to the draft declaration

At the outset, we would like to acknowledge that it is the view of ourselves and our members that the current text of the draft declaration provides a useful initial foundation for an instrument. In this part, we have only included the sections of the draft declaration that we are recommending be changed. Existing text that we are recommending be removed or replaced is ~~struck-through and highlighted~~. Our suggested replacement text is written in **bold red**. Our commentary explaining the rationale for our suggested changes are in blue and bordered.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument.	~~The day after this instrument is registered.~~ **The day following a period of six months from the day this instrument is registered.**	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

Rather than the instrument taking effect on the day that it is registered, we suggest providing industry with a period of at least six months to enable businesses (and especially start-up businesses) to consider the instrument's various provisions, which may require the development of new or redesigned features, IT solutions, or provision of information within apps or services. For example, we note that the *Online Safety Act 2021* was passed with a delayed commencement of six months for exactly this reason. While we appreciate the transparency provided by the early release of a draft declaration, amendments may be made to the final version that industry will not have visibility of until the instrument is registered.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

4 Definitions

In this instrument:

Act means the *Online Safety Act 2021*.

Harmful material **means the following:**

(a) cyber-bullying material targeted at an Australian child; or
(b) cyber abuse material targeted at an Australian adult; or
(c) material that depicts abhorrent violent conduct; or
(d) non-consensual intimate images of a person; or
(e) class 2 material.

as defined in the Act.

The term 'harmful' is used in the draft instrument but is not defined. Further, 'harmful' is not used in *the Online Safety Act 2021*, while 'harm' is not defined. 'Harmful' is a vague and subjective term and without a definition in the draft declaration, some of the BOSE requirements that rely on that term have unclear thresholds and it may be difficult for some service providers to fully understand how to comply with them. Without a tight definition, the use of the term 'harmful' may also extend to a range of activities or materials that has nothing to do with online safety, going well beyond the scope of the legislation. For clarity, we propose that the term 'harmful' be defined, with our proposed definition outlined above (ie. material that is subject to the Commissioner's takedown powers under the legislation).

5 Purpose of this Part

For the purposes of subsections 45(1), (2) and (3) of the Act, this Part specifies the basic online safety expectations for the following:

(a) a social media service;

(b) a relevant electronic service of any kind;

(c) a designated internet service of any kind.

Note 1: Subsections 6(1) and 7(1), section 11, subsection 12(1) and sections 13, 15 and 20 of this instrument are made in accordance with subsection 46(1) of the Act (core expectations).

Note 2: This instrument is not intended to cover online material that has been classified under the National Classification Scheme.

The intended purpose of our proposed additional Note 2 is to avoid the regulatory overlap that currently exists between the operation of the BOSE (and other regulation stemming from the *Online Safety Act 2021*) and the National Classification System, which may cause duplication of requirements and lead to confusion for industry.

There is already precedent for such action. Please note that the eSafety Commissioner has already indicated that the Online Safety Industry Codes created under the same legislation will not apply to classified video game content (see footnote 25 on page 33 of its position paper).

6 Expectations—provider will take reasonable steps to ensure safe use

Core expectation

(1) The provider of the service will take reasonable steps to ensure that end-users are able to use the service in a safe manner.

Additional expectation

(2) The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is or may be ~~unlawful or~~ harmful **material**.

It was undoubtedly not Parliament's intention for the Basic Online Safety Expectations to cover online activities such as copyright infringement, fraud, 'pump and dump' tactics, or false advertising. However, these are examples of the many kinds of 'unlawful or harmful' material that would be covered by subsection 6(2) under the proposed wording, despite these materials having nothing to do with online safety. We have suggested alternative wording,

based on a clear definition of 'harmful material' that we have suggested above. Please note that this change should be repeated elsewhere in the BOSE where 'unlawful or harmful' is used.

Reasonable steps that could be taken

(3) Without limiting subsection (1) or (2), reasonable steps for the purposes of this section could include the following:

(a) developing and implementing processes to detect, **mitigate,** moderate, report, **provide feedback on or** ~~and~~ remove (as applicable) material ~~or activity~~ on the service**, or likely to be place on the service,** that is or may be ~~unlawful or~~ harmful **material**;

Different kinds of 'unlawful or harmful' material or activity on a service will require different responses (and degrees of responses) depending on the circumstances. We believe our suggested amendments better reflect the diverse and flexible range of action that may be considered an appropriate response to such material and clarifies that service providers should not be expected to undertake *all* the listed actions if it is not necessary or proportionate to do so. Adding in "or likely to be placed on the service" also makes it clear that reasonable measures taken by a service provider could include measures taken *before* content is placed on a service.

(b) if a service or a component of a service ~~(such as an online app or game)~~ is targeted at, or ~~being used by~~ **marketed for use by**, children (the ***children's service***)—ensuring that the default privacy and safety settings of the children's service are robust and set to ~~the most~~ **an appropriately** restrictive level;

This paragraph is the only part of the draft declaration that provides a specific example of what a 'service' means, which we consider unnecessary and redundant. There is already no doubt that 'an online app or game' will be considered a 'service'.

We also do not believe a 'children's service' should include services that are simply being used by children. We believe literally every service available in Australia, including those with very little appeal to children, or where there were reasonable steps taken to restrict its use, is likely to have some users who are under 18, even if the number is very low. This would mean that there would be very few services that would not be captured by the proposed definition of 'children's service'. We suggest that a slightly more specific and much more practical threshold of 'marketed for use by' should be used instead.

Finally, we believe that having a rule that the default privacy and safety setting of a children's service should be set at the 'most' restrictive level is arbitrary and not particularly helpful. It is a relative term informed only by the range of options made available, and not grounded in the appropriateness of those options. For example, if a service only has a single level of restrictiveness, it could arguably meet the threshold of this paragraph even if the setting is not objectively restrictive. However, another service may have several restrictiveness levels, include more than one which are appropriate for children, but only one of those levels would satisfy this paragraph. We suggest that a more nuanced threshold be used – one tied to the suitability of those options - as that will likely lead to better online safety outcomes. It is also important to recognise that the appropriate settings for a five year old will be different to the appropriate settings for a fifteen year old.

(c) ensuring that **relevant** persons who are engaged in ~~providing~~ **developing or moderating** the service, such as the provider's employees or contractors, are trained in, and are expected to implement ~~and promote,~~ online safety **policies**;

(d) continually improving technology and practices relating to the safety of end-users;

(e) ensuring that assessments of safety risks and impacts are undertaken, and safety review processes are implemented, ~~throughout~~ **during** the design, development, deployment and post-deployment stages for the service.

We have suggested some minor textual changes to improve the specificity and clarity of the provisions and to avoid unnecessary impacts. For example, we have suggested including 'relevant' and removing 'promote' because, realistically, not everyone involved in development have roles that are relevant to promoting online safety (eg. graphic designers and audio engineers in our sector). We also prefer 'during' to 'throughout' as safety risk assessments are iterative and necessarily carried out periodically, and are not single continuous processes.

7 Expectations—provider will consult with Commissioner and refer to Commissioner's guidance in determining reasonable steps to ensure safe use

Core expectation

(1) In determining what are reasonable steps for the purposes of subsection 6(1), the provider of the service will consult the Commissioner.

~~*Additional expectation*~~

~~(2) In addition, in determining what are reasonable steps for the purposes of subsection 6(1), the provider of the service will have regard to any relevant guidance material made available by the Commissioner.~~

Consulting the Commissioner

(2) The requirement to consult the Commissioner as required under subsection 7(1) may be satisfied by:

(a) the provider of the service having regard to any relevant guidance material made available by the Commissioner; or

(b) the provider of the service being a member of an industry association that has an active dialogue with its members and the eSafety Commissioner regarding reasonable steps to implement online safety.

While we recognise that subsection 7(1) must be included in the instrument as it is a core expectation outlined in the legislation, it is, when reflected in the real world, an impractical and unrealistic expectation that essentially turns the Commissioner into a product design officer. Every year there are literally millions of social media services, relevant electronic services, and designated internet services developed around the world that will have Australian users. Clearly it would be impossible for all of these service providers to consult individually with the Commissioner, who would also need to have thousands (if not tens of thousands) of staff just for this purpose. Yet that is exactly the expectation that is being created in subsection 7(1).

Aside from these obvious impracticalities, we also have concerns with subsection 7(1) from a general policy perspective. Whether intentional or not, the current drafting leads to an end result that the only way a service provider can 'comply' with the BOSE is to follow whatever

instructions it receives from the Commissioner via a private bilateral meeting. Notwithstanding the fact that the BOSE is non-enforceable, there is nothing stopping the eSafety Commissioner from giving instructions to service providers that are unreasonable, and then using its powers to 'name and shame' services that are, for one reason or another, unable to or choose not to follow those instructions. The subsection 7(1) requirement therefore creates a very unusual (and generally-discouraged) approach to regulation, with different service providers inevitably being given inconsistent and non-transparent requirements based on conversations with the Commissioner who, in the BOSE context, is unencumbered by any legislative guidance, operational oversight, or regulatory impact process. This approach also leaves the Australian Government open to criticism or even legal action if the Commissioner provides inconsistent advice to competing services, leading to some services being placed at an advantage or disadvantage.

A much more functional and achievable approach would be to combine the core expectation and the proposed additional expectation in a way that will give greater flexibility for the Commissioner to outline its expectations and guidance to industry - and to do so far more efficiently and consistently. We have also proposed an additional, practical way of complying with the consultation requirement by enabling the Commissioner to give industry-specific guidance to industry bodies who can then efficiently share them with all their members.

[ideally remove section 8 in its entirety, but if it is kept – amend as follows]:

8 Additional expectation—provider will take reasonable steps regarding encrypted services

If the service uses encryption, the provider of the service will take reasonable steps**, to the extent possible,** develop and implement processes to detect and address **harmful** material **that is unlawful** ~~**or activity**~~ on the service ~~**that is or may be unlawful or harmful**~~.

Note: This additional expectation does not create an expectation for the provider of the service to monitor the communications and activities of end users.

There is a very apparent and growing tension between this additional expectation and domestic and international privacy and security regulations. Among other impacts, there is the potential for section 8 to erode the level of trust that the community places in encrypted services for entirely legitimate reasons such as sharing sensitive information or data. Our preference would be to consider removing section 8 entirely, and instead discuss any concerns by Government with the use of encrypted services in a dedicated and more focused approach. At the very least, the bar should be set very high and only cover unlawful material or activity.

The suggested additional note is important, and has been adapted from the Department's 'Frequently Asked Questions' document. Alternatively, it could be addressed in an explanatory statement (if there will be one).

9 Additional expectation—provider will take reasonable steps regarding anonymous accounts

Additional expectation

(1) If the service permits the use of anonymous accounts, the provider of the service will take reasonable steps**, subject to Australian and international privacy requirements,** to prevent those accounts being used to deal with **harmful** material~~**, or for activity, that is or may be unlawful or harmful material**~~.

Reasonable steps that could be taken

(2) Without limiting subsection (1), reasonable steps for the purposes of that subsection could include the following:

(a) having **reasonable** processes that**, where practical and without impacting the lawful use of the service, aim to** prevent the same person from repeatedly using anonymous accounts to post **harmful** material~~, or to engage in activity, that is unlawful or harmful~~;

~~(b) having processes that require verification of identity or ownership of accounts.~~

(b) providing information to end-users during account creation processes confirming that anonymous accounts undertaking illegal or harmful behaviour will be removed.

We believe subsection 9(2) as currently proposed is inconsistent with Australian privacy law, not to mention certain international privacy laws and global best practice. Australian Privacy Principle 2 (APP 2) in the *Privacy Act 1998*, titled 'Anonymity and pseudonymity', requires private sector organisations "to give individuals the option of not identifying themselves, or of using a pseudonym".

We do not believe paragraph 9(2)(a) of the BOSE as currently drafted would be possible to achieve in any reasonably practical sense without contravening APP 2, as to do so will often necessarily require the collection of an identifier of some kind. We have suggested some amendments that may allow the paragraph to still be included in the draft instrument, while not placing service providers in a difficult and conflicted position caught between two laws.

Further, it is important for us to advise that it is often impossible for any service to completely prevent the kind of behaviour that paragraph 9(2)(a) is targeting. End-users may be able to circumvent service bans by using new hardware or creating a new account. Further, if companies attempted to prevent access based on hardware or IP addresses, for instance, very often there are unintended consequences for other legitimate users that are using the same hardware or IP address.

Paragraph 9(2)(b) of the BOSE outright contravenes APP2 because to impose an identity or account-ownership verification process will simply mean that the account-owner is not anonymous. As written, the paragraph requires service providers to have the ability to identify people behind anonymous accounts, which is, by definition, not possible if the account is genuinely anonymous. In practice, complying with this expectation would prevent the creation of any anonymous account, despite the premise of the section being "if the service permits anonymous accounts". This is a confusing circular argument.

Furthermore, paragraph 9(2)(b)'s impact of removing the possibility of an anonymous online account is inconsistent with reasonable practice or public expectation. We note that not even the Department has any way (nor desire) to verify the identity of the end-users of its own 'Have your Say' online facility for making submissions to this consultation. The same can also be said of the Commissioner's submissions lodgement facility. Both of these facilities would fall within the definition of 'designated internet service'.

Finally, we have suggested an additional, practical reasonable step that an end-user could implement to comply with subsection 9(1).

12 Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

Core expectation

(1) The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

Reasonable steps that could be taken

(2) Without limiting subsection (1) of this section, reasonable steps for the purposes of that subsection could include the following:

(a) implementing age assurance mechanisms;

(b) conducting child safety risk assessments;

(c) offering parental controls and locks;

(d) requiring a credit card to make purchases.

In our industry's experience, parental controls and locks are among the most powerful and effective technological tools to prevent access by children to class 2 material and should be included in the list of reasonable steps at subsection 12(2). Further, a requirement for the use of a credit card, while not appropriate in every situation, often proxies in an incidental way as an effective age assurance mechanism where it is already being utilised as a payment method.

13 Core expectation—provider will ensure mechanisms to report and make complaints about certain material

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 **(as applicable)**:

It is important to make it clear that providers that, for example, have no functional capacity to host cyber-bullying material should not be required to have a complaints mechanism for that category of material.

(a) cyber-bullying material targeted at an Australian child;

(b) cyber-abuse material targeted at an Australian adult;

(c) a non-consensual intimate image of a person;

(d) class 1 material;

(e) class 2 material;

(f) material that promotes abhorrent violent conduct;

(g) material that incites abhorrent violent conduct;

(h) material that instructs in abhorrent violent conduct;

(i) material that depicts abhorrent violent conduct.

Note: The reference to class 2 material at paragraph (e) does not apply to any lawful class 2 material that is permitted on the service.

A range of services, including many of the most popular video streaming services and gaming platforms, validly and lawfully make available R18+ content such as commercial films and games. It would be nonsensical for such services to be required to implement reporting

mechanisms with respect to such material (eg. a streaming service that offers a library of R18+ films that also has a button for making complaints about the availability of R18+ films).

14 Additional expectation—provider will ensure service has terms of use, certain policies etc.

The provider of the service will ensure that the service has:

(a) terms of use; and

(b) policies and procedures in relation to the safety of end-users; and

(c) policies and procedures for dealing with reports and complaints mentioned in section 13 or 15; and

(d) standards of conduct for end-users (including in relation to material that may be posted using the service by end-users, if applicable), and policies and procedures in relation to the moderation of conduct and enforcement of those standards.

Note ~~1~~: See section 17 in relation to making this information accessible to end-users.

~~Note 2: For paragraph (b), the policies and procedures might deal with the protection, use and selling (if applicable) of end users' personal information.~~

We believe the specific activities included in Note 2 have more to do with privacy and data management and little to do with online safety. As a result, we believe they are strictly outside of the scope of the BOSE and should be removed. Privacy matters are being addressed by the Government through the forthcoming Online Privacy Code and Review of the *Privacy Act 1988.*

16 Additional expectation—provider will make accessible information on how to complain to Commissioner

If reasonably appropriate and practicable to do so, t~~T~~he provider of the service will ensure that information and guidance on how to make a complaint to the Commissioner, in accordance with the Act, about any of the material mentioned in section 13 provided on the service, is readily accessible to end-users.

It is proportionate and practicable to require each service to provide readily accessible safety and reporting information relevant to that specific service. However, the same cannot be said for the expectation to provide eSafety-specific information. While this may seem to be a relatively achievable expectation on the surface, a requirement for a service provider to provide specific information on the Australian regulatory environment only for their Australian users may be very difficult to achieve in any practical sense. Many services do not currently have the ability to provide different information to their users in different geographical regions and to do so would impose a significant cost. Further, services that are currently unable to, or choose not to, track the location of their end-users, such as to maintain their privacy, should not be required to start monitoring geo-location data purely to follow the guidance set by section 16.

17 Additional expectation—provider will make information on terms of use, policies and complaints etc. accessible

(1) The provider of the service will ensure that the information specified in subsection (2) is:

(a) readily accessible to end-users; and

(b) in relation to the information mentioned in paragraph (2)(b)—accessible at ~~all~~ **appropriate** points in the end-user experience, ~~including~~ **which may include**, but

should not **be** limited to, point of purchase, registration, account creation, first use and at regular intervals (as applicable); and

We believe it would be an unreasonable and severe interference to both the service provider's ability to effectively design a service as well as the consumer experience of the end-user for the information to be accessible at *all* points in the end-user experience. For example, the inclusion of this information could come at the expense of other important information, including financial and legal information. It would also almost certainly lead to the end-user experiencing counter-productive 'fine print fatigue'. Service providers should have the flexibility to be able to determine the most effective and appropriate points to provide the required information.

(c) regularly reviewed and updated; and

(d) written in plain language.

(2) For the purposes of subsection (1), the information is the following:

(a) the terms of use, policies and procedures and standards of conduct mentioned in section 14, **except where it would not be appropriate to do so**;

(b) information regarding online safety and parental control settings, including**, if reasonably appropriate and practicable to do so,** in relation to the availability of tools and resources published by the Commissioner.

Our proposed addition to paragraph 17(2)(a) is important. We support the intention of the expectation that services generally make online safety policies and procedures accessible to end-users. However, it is important that this be understood not to include sensitive or operational elements of service safety policies that are intentionally not disclosed to the public. Typically, they may not be disclosed in order to retain their operational effectiveness (eg. by preventing the deliberate abuse, manipulation, or 'weaponisation' of those safety measures).

In relation to paragraph 17(2)(b), as per our comment addressing section 16 above, while this may seem to be a relatively achievable expectation on the surface, in reality it is asking for services from around the world to be able to differentiate between their Australian and non-Australian users, and to only provide the information to the former group. Many services do not have the ability to provide different information to their users in different geographical regions and to do so would impose a significant cost, while others are unable to or choose not to track the location of their end-users, and they should not be required to do so.

18 Additional expectation—provider will provide regular reminders of and information about policies, terms and conditions etc.

If reasonably practical and appropriate to do so, Tthe provider of the service will ensure that end-users receive regular reminders of, and updates in relation to changes in, the information specified in subsection 17(2), including through targeted in-service communications.

For the same reasons as discussed in relation to sections 16 and 17 above, it may not be possible or practical for some services to be able to push out Australian eSafety-specific information to Australian end-users through in-service communications.

[ideally remove section 19 in its entirety, but if it is kept – amend as follows]:

19 Additional expectation—provider will keep records regarding certain matters

The provider of the service will keep records of **the number and outcome of** reports and complaints about the material mentioned in section 13 provided on the service for ~~5 years~~ **a reasonable amount of time** after the making of the report or complaint to which the record relates.

Not only do we believe that a requirement to keep the material for 5 years would be an unreasonable burden on service providers, particularly smaller service providers, as well as being inconsistent with Australian and international privacy laws, but most importantly we believe it would not be in the best interests of end-users. In relation to privacy laws, it is a globally accepted best practice, enshrined in legislation in Australia and abroad, that entities should not keep any personal information that is no longer relevant or necessary to keep. It is difficult to understand why a record of an end-user complaining about alleged cyber-bullying, especially where the complaint has been fully resolved or where the parties have moved on, should still be kept by a service provider four and a half years after the report was made. Further, some of our members have advised us that they have purposefully chosen to only keep certain basic data or metadata about the complaints made about certain matters, and only for a short period of time, in order to reduce the risk of sensitive personal information being compromised through a data leak or cyber attack.

20 Core expectations—provider will provide requested information to the Commissioner

(1) 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.

(2) 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, for each removal notice given to the provider during a specified period (not shorter than 6 months), how long it took the provider to comply with the removal notice, the provider will comply with the request within 30 days after the notice of request is given.

(3) If the Commissioner, by written notice given to a provider of the service, requests the provider to give the Commissioner specified information relating to the measures taken by the provider to ensure that end-users are able to use the service in a safe manner, the provider will comply with the request within 30 days after the notice of request is given.

Note 1: For subsections (1), (2) and (3) the Commissioner may only request information relating to complaints made to the provider of the service by Australian end-users.

Note 2: For subsections (1), (2) and (3) the Commissioner may only request information relating to complaints about breaches of a service's terms of use if the complaints relate to online safety matters.

Note 3: For subsections (1), (2) and (3) the Commissioner must specify, in the written notice, the particular service to which the request refers.

Note 4: For subsections (1), (2) and (3) the provider may choose to only provide information relating to complaints that were found to be reasonably substantiated.

Regarding our proposed Note 1, it is logical and appropriate that the Commissioner may only request the number of complaints about potential breaches of a service's terms of use that have been made by Australian users (eg. complaints made by Canadian end-users are irrelevant for these purposes).

Regarding our proposed Note 2, it is similarly logical and appropriate that the Commissioner may only request the number of complaints about potential breaches of a service's terms of use if those complaints concern online safety (eg. complaints about copyright-related breaches of a service's terms of use would be irrelevant for this context).

Regarding our proposed Note 3, the Commissioner should be required to provide specific details in the written notice regarding the service to which they refer, to minimise confusion in a situation where the entity receiving the notice offers multiple, possibly unrelated, services.

The purpose of our proposed Note 4 is to enable service providers to ignore complaints that are unsubstantiated, erroneously-made, or frivolous. For example, on platforms where complaints or reports can be easily made, it is not uncommon for such mechanisms to be weaponised against certain high profile celebrities (eg. groups of people lodging false 'offensive content' complaints about a singer because they do not like their new song).

Alternatively, these notes could be addressed in an explanatory statement (if there will be one).

Additional matters

Further provisions

Further to our specific suggested textual amendments above, we recommend that the draft declaration include or address the following:

- The draft declaration should make it clear that not every expectation outlined in the BOSE will necessarily be relevant or will apply to all services, nor are services expected to adopt every reasonable step available. For example, section 15 of the draft declaration (dealing with mechanisms for reporting and making complaints about breaches of terms of use) will be irrelevant for services where terms of use are not needed, and breaches are impossible (eg. games where players can only communicate with one another using pre-determined phrases). While we note that the Department's 'Frequently Asked Questions' document released as a part of the present consultation makes this clear, it should be reflected in the instrument itself.
- The draft declaration should also acknowledge that how a business complies with the BOSE may depend on their specific circumstances, such as their organisational size, the number of end-users of their service, the number of Australians that use their service, and the stage of the services growth. For example, large multinationals running an extensive and mature service will have a much stronger capability to consider, for example, section 10 (dealing with consulting and cooperating with other service providers) than a start-up still launching its first product with a small number of users.
- The draft declaration should make it clear that services will not be expected to meet the requirements of the BOSE if it would not be appropriate to do so, such as if doing so would create an inconsistency with a national or international law. For example, it is possible that some of the existing BOSE requirements may be inconsistent with some privacy or data management laws abroad. While the BOSE are by their very nature secondary to any legislative or regulatory frameworks, it would be helpful for the draft declaration to be clear and explicit about this.
- The draft declaration should include a section that describes the considerations the Commissioner must take into account when assessing whether the efforts reported by a service under an expectation meets the test of 'reasonable steps' in those particular circumstances. This should be drafted in a similar spirit to subsection 49(5) of the *Online Safety Act 2021*, and could look like:
    - *In deciding whether a report provided by a service under subsection (X) complies with the applicable basic online safety expectations during the period specified in the determination, the Commissioner must have regard to the following:*
        - *contextual information regarding the risk of harm posed by the particular service type;*
        - *the relevance of the expectation to the particular service type in question; and*
        - *the size and maturity of the relevant service.*

Further consultations

Finally, we recommend that the Department further consult on a final draft of the declaration before it comes into place. This will give stakeholders visibility over any changes that are made to the draft declaration as a result of this consultation process as well as further internal considerations by the Department or Minister. If the subsequent consultation occurs after 23 January 2022, it may also give the Government greater comfort that the requirement under section 47 the *Online Safety Act 2021*, that the Government must consult on any draft declaration, has been met (ie. given that the current consultation is occurring prior to the commencement of the legislation, it may not strictly meet the requirements of section 47).

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