IGEA

interactive games & entertainment association

Submission to the eSafety Commissioner

Response to the call for submissions on the Restricted Access System

September 2021

Background

About 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 makers 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 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.

IGEA is pleased to make a submission in response to the eSafety Commissioner's consultation on the Restricted Access System. While it has not been necessary for IGEA to make a submission to the Commissioner's parallel consultation on a proposed roadmap for age verification as our industry is not within the regime's scope, the Commissioner is welcome to use any information provided in this submission for the other consultation if considered useful.

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 set rules around how their children play.

Our industry's approach to content controls

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 helping to protect children from age-inappropriate content 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), customed content restrictions, tools for monitoring and limiting child screen activity, internet filters, and companion apps for parents.
4. Automatic, pre-emptive, and customisable text filters for player-to-player communications, often implemented via algorithms that are constantly updated and implemented across multiple languages.

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.

Video games and R18+ material

R18+ level material comprises a miniscule proportion of the video games released in Australia each year. According to the Australian Classification Board's 2019-20 Annual Report, a mere 13 video games received an R18+ rating out of the 316 games classified by the Board – a proportion of barely 4 per cent. Further, the proportion of games classified R18+ by the IARC classification tool was several times lower – a proportion of barely 0.2% of all decisions generated by the tool in 2019-20 (even ignoring the fact that the IARC classification tool tends to over-classify rather than to under-classify games). While similar statistics are not available with respect to video gaming content on user-generated streaming and video-on-demand platforms, the proportion of players recording game play of R18+ games is likely to be similarly miniscule. In addition, the fact that a person streams themselves playing an R18+ game does not automatically make that content R18+. Among other differentiating factors, video game play footage lacks all of the interactivity elements that may have made that game R18+.

The global context

The approach in Australia discussed above is largely replicated in all other territories around the world. For example, the IARC Classification Tool does not just generate Australian ratings for online and mobile games, but also localised ratings for each territory that has implemented IARC, including across all of Europe and North America, as well as Brazil, South Korea, and other regions. Similarly, parent-controlled child accounts that do not allow content to be accessed above a specified ratings category typically work hand-in-hand with each territory's individual classification system. In practically all of these territories, these measures have been implemented via our duty of industry responsibility and proactive self-regulation.

In the vast majority of territories around the world, age ratings for video games, even at the higher (eg. R18+ equivalent) categories, are not enforceable and are primarily intended as guidance for parents and carers, who are considered as having primary responsibility for determining what video game content is appropriate for their children to access. On the topic of content age ratings, UNICEF recently published a report that concluded the importance of a "more flexible system that is sensitive to the individual needs of a child" (see p. 13). The same report also noted that the only country in the world that mandates age assurance tools for accessing certain video games is China (see p. 39). Further, age assurance tools are primarily used in China not for content regulation but to help manage overall screen time for children.

Responses to Discussion Paper Questions

Restricted Access System effectiveness and impacts

***Question 1**: Under the Online Safety Act 2021, the RAS will only apply to Restricted Material that is provided from Australia on a social media service, relevant electronic service or designated internet service, or that is hosted in Australia. What elements should be part of an effective system to limit access to that kind of material?*

The video games industry shares the Australian Government's aim of ensuring measures exist to help prevent children from accessing R18+ content. The best way to achieve this is a RAS framework that enables digital service providers (including the providers of video game content) to approach this aim flexibly by adopting the most appropriate approaches for their platform, as well as to encourage digital service providers to continually innovate with new processes and technologies. The overall flexibility and reasonable steps-based approach of the current Restricted Access System Declaration 2014 (the 2014 RAS Declaration) helps industry to achieve these benefits.

The RAS framework must be reasonable, realistic, and achievable for industry. Conversely, a prescriptive framework that outlines the specific technologies that must be implemented is not appropriate and will fail, especially where those technologies themselves are seen as unproven at best, and dangerously flawed at worst. Basing a framework around the specific technologies or processes that exist in 2021 will also lead to the RAS inevitably going out of date. Specifically, it may lead to the inclusion of approaches that subsequently fall out of favour, as well as the omission of new approaches that should be permitted. A major risk of a system that does not enable service providers to realistically achieve the requirements of a RAS is that it will simply force those services to operate offshore or, far more problematically, push consumers towards alternate overseas-based services that offer no content controls at all.

Finally, while we support an effective system to limit children's access to R18+ material, it is important that the requirements of a RAS are not mistakenly held to the same standard as age verification (AV). AV is a specific kind of activity, and as we noted earlier, no country in the world apart from China legally requires the use of AV for video games. More importantly, the House of Representatives Standing Committee on Social Policy and Legal Affairs in its final report on *Protecting the age of innocence*, focused its recommendation 3 relating to a roadmap for the implementation of an AV regime on online pornography only, excluding R18+ material from its scope. The Australian Government is also not requesting or seeking to pursue the implementation of AV for R18+ content, with the eSafety Commissioner's task of developing an implementation roadmap for an AV regime strictly limited to online pornography.

***Question 2**: Has industry experienced any difficulties complying with the Restricted Access System Declaration 2014?*

We are not aware of any difficulties that our members have experienced in complying with the 2014 RAS Declaration. We are also not aware of any concerns that have ever been raised by regulators regarding the compliance of the video games industry to the 2014 RAS Declaration.

***Question 3**: Has the Restricted Access System Declaration 2014 allowed industry the flexibility to develop access-control systems appropriate to their business models?*

Flexibility for industry is generally one of the strengths of the 2014 RAS Declaration. Specifically, while the 2014 RAS Declaration provides clear expectations for industry, including requirement for an access application, warnings and safety information about R18+ material, and a reasonable steps-based age confirmation step, it provides flexibility for digital service providers in how they can meet those expectations in the most appropriate and expedient way.

There will be no single approach to content restriction that will necessarily work best or most effectively across the vast variety of different apps, services, and platforms that exist or will exist. The approaches that will work best will depend on, among other things, the nature of the service, the kinds of material accessible on it, the platform's audience, how consumers (and children) interact with it, and the overall risk profile of the R18+ content on it. This is why the reasonable steps-based approach of the 2014 RAS Declaration is the correct one.

Question 4*: What is the nature of the impact that has been experienced by:*

(a) industry; and

(b) the Australian public

as a result of the Restricted Access System Declaration 2014? Have financial and administrative burdens been placed on service providers by the 2014 RAS Declaration? Have there been any indirect effects (for example, costs being passed on to customers or suppliers)? Please provide examples.

As a result of the flexible approach that it provides to industry to determine the best implementation pathway, we are not aware of any financial or administrative burdens being placed on our members by the 2014 RAS Declaration, nor of any indirect effects such as costs being passed on to customers. We also fully agree with the objective outlined by the eSafety Commissioner in the discussion paper that "the RAS should meet the policy objective of keeping children and young people safe online, while not placing unnecessary financial or administrative burden on industry".

Age restriction methods

Question 5*: What factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material?*

The following factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material:

- <u>Is the approach realistic?</u> A reasonable approach must be one that is practically possible and achievable. For example, it would not be realistic for the RAS to expect a service to implement facial analysis, for example, a process that all stakeholders would surely agree should play no role in age confirmation for media access. However, it would be realistic to provide online safety information and controls for parents and carers. It is also vital that the Commissioner recognise that 'realistic' in the context of this question must also mean implementable cost-effectively.

- <u>Is the approach effective?</u> The approach adopted should be one that does act to help limit access to age-inappropriate material. Throughout the almost two decades that the previous Online Content Scheme ran for, we are not aware of any complaints raised by the eSafety Commissioner and prior to that the ACMA, or complaints they have received from consumers, of deficiencies or gaps in our members' reasonable steps.

- Is the approach practicable? The approach must be compatible with the consumer. For example, the requirements of a RAS must not be so onerous or impracticable that it unreasonably restricts adults from accessing material they have a right to access. For example, a requirement for an adult to share their sensitive personal information with a third party age verifier simply to watch the R18+ film *Pulp Fiction* on their streaming service would arguably be an unreasonable and censorial interference with their right under the *National Classification Code* to "read, hear, see and play what they want".

- Is it proportional to the material being restricted? In our sector's case, the material in question is typically classified commercial R18+ material - the lowest risk category of content within the scope of the Online Content Scheme. Not only are R18+ games a far lower risk category than online pornography, for instance, but with only 13 games classified R18+ by the Board in 2019-20, there is hardly any of it. 'Reasonable steps' to limit access to thousands of hours of hardcore online pornography on a website will be vastly different to what should be considered reasonable steps to limit access to, say, a handful of classified R18+ games available on an online gaming platform.

- What are the risks of the approach? The basic incontrovertible principle that must underpin the design of the RAS here is that the more intrusive the approach for limiting access to age-inappropriate content, the higher the risks of that approach, such as the risks to privacy. The fact that so many questions still linger around the efficacy of almost all AV mechanisms, as well as the underdeveloped nature of the private AV industry heightens these risks. These are outlined further in our response to Question 6 below.

- What are the costs to industry and consumers? Efficient and effective approaches to content restrictions, such as reasonable on-platform systems like parental controls, are well established and their continued improvement will result in minimal cost to consumers. More intrusive and novel approaches, especially ones that involve third parties or sensitive data storage, will result in significant costs to service providers - costs that will be inevitably passed down to consumers. These approaches also cost consumers in terms of the sensitive personal information they may be required to share.

- Is it a reasonable approach? This is the final question, considering all of the above factors discussed above and potentially others, that the RAS framework must be designed around. Until a 'perfect' solution is uncovered - and we do not yet see one in the foreseeable future - it is necessary and sufficient that industry have the flexibility to determine and implement the most appropriate reasonable steps in the circumstances.

Question 6*: What systems, methods and approaches do you consider effective, reasonable and proportionate for verifying the age of users prior to limiting access age-inappropriate material?*

We strongly disagree with the use of the word 'verifying' in this question, and reiterate the point we made above in our response to Question 1 that R18+ material is not within the scope of the Government's proposed roadmap for an AV regime. It would therefore be inappropriate for the RAS to include any mandatory requirement for digital platforms to implement AV.

We also disagree with the point made in the discussion paper that there have been significant technological advancements in methods for determining or assuring the age of online service users. We believe it to be generally accepted that although there have been some technological improvements and innovation in AV over recent years, and despite the advocacy from the private AV industry, there are currently no AV methodologies that are reliable, practical, cost-effective, and do not carry significant risks. Even ignoring the questions around the technological merits of various AV processes, there is a wide disparity of views and fierce debate between key stakeholders including the community, industry, policy-makers, and consumer and privacy advocates around what role, if any, AV should play in regulating access to online pornography - let alone the far lower risk category of content that is R18+ material.

We note that in March 2021, the renowned UK-based child safety advocacy group the 5Rights Foundation published a major paper that, amongst other things, highlighted a range of risks to the community from the use of the most commonly-discussed forms of potential AV. We have summarised the Foundation's excellent analysis of these risks in the following table:

Risks to the community from the use of AV	**Relevant AV technology / process***
Significant tensions between data processing and the community's right to privacy	All
Discriminates against people who do not wish to provide personal information (and would not necessarily need to do so to obtain the same access in the physical world), leading to services and information being denied to them	All
Little transparency to users and a lack of understanding by users around how data necessarily collected for AV is stored, shared, and used	All
AV opens the door to the use of broader user data for restrictions and discrimination (eg. making decisions based on location, demographic, or gender)	All
AV technology is unproven, unverified, opaque, unpopular, and/or lacking in agreed standards	Profiling, Biometric, Capacity-testing, Age tokens
AV technology is inaccurate, leading to children close to 18 being falsely verified or young adults being denied access to services or information	Profiling, Biometric, Capacity-testing
AV only enables soft assurance (eg. a person is *likely to be* a certain age) rather than exact assurance (ie. a person *is exactly* a certain age) – eroding its usefulness	Profiling, Biometric, Capacity-testing
Likely to result in the collection of data beyond that which is needed for age assurance, data which may also be used to build up a person's data profile	Profiling, Hard identifiers, Biometric, Cross-account authentication
Data is commercially valuable and will likely be shared with or sold to third parties, which may result in negative outcomes for users	Profiling, Cross-account authentication, Third-party digital identities
Requires a person to disclose sensitive personal information (eg. name, photos, address, race, gender, financial information, employment, family members etc.)	Hard identifiers, Cross-account authentication, Third party digital identities
The more personal information a company collects, the greater the security risks surrounding the storage and use of that data (including hacking, fraud, and the commercial misuse of that data)	Hard identifiers, Biometric
If a person (and particularly a child) uses another person's ID or falsified document, they may be committing fraud or other crimes	Hard identifiers

Discriminates against people with more limited access to official documentation, such as disadvantaged and culturally and linguistically diverse (CALD) persons	Hard identifiers, Account holder confirmation
Discriminates against persons with different skin tones, physical attributes, and/or craniofacial features	Biometric
Discriminates against persons with a lower aptitude, persons with disabilities, and neurodiverse persons	Profiling, Capacity-testing
AV process may also collect information on emotion, attention, comprehension, and mood, which may be used to affect real world outcomes	Profiling, Biometric, Capacity-testing
Vulnerable to cheating (eg. an adult or older child may complete the AV activity on behalf of a younger child)	Profiling, Capacity-testing
Use of low quality data, datasets, or third-party authentications will result in a low level of assurance	Cross-account authentication, Third-party digital identities, B2B verification, Age tokens
Widespread use of major age assurance providers will entrench their market dominance (including those formed by the online pornography industry)	Cross-account authentication, Third-party digital identities, B2B verification, Age tokens
Involvement of third parties introduces others into the value chain of sensitive personal information, which is undesirable, may lack user consent, and increases risks	Cross-account authentication, Third-party digital identities, B2B verification
Commercial realities means that digital assurance providers will inevitably collect more information (ie. little commercial incentive to only collect age information)	Third-party digital identities, B2B verification, Age tokens
Amassing data sets that hold personal information presents massive security risks from hacking, fraud, and commercial misuse	Cross-account authentication, Third-party digital identities, B2B verification, Age tokens
Discriminates against older children who may wish to access services or information without adult involvement (eg. sexual health services), which can lead to harm	Account holder confirmation

* Please see the full 5Rights Foundation report for an explanation of the individual AV technologies or processes listed.

UNICEF's recent report on digital age assurance tools likewise identified some major obstacles to the implementation and acceptance of AV technologies and processes, including:

- the intrusive use of personal data
- the uncomfortable requirement for adults to provide potentially sensitive data
- the exclusion of people without official ID
- the implications of tracking and surveillance
- the risk of potentially catastrophic data breaches of personal data
- the margins of error that many newer AV technologies still experience
- the unproven, opaque, and problematic algorithms (especially when used on people whose datasets do not feature in the training data used)
- the inherently invasive and potentially unlawful use of behaviour for AV
- the difficulties in using behavioural analytics in determining age across countries and contexts

- the inevitable creation of data trails
- the highly contested nature of some technologies such as blockchain, and
- the fact that there are gaping deficiencies with third party data holders (the report cites evidence that around 30 per cent of the data that one of the largest data brokers in the world held was incorrect).

For these reasons, the RAS must not impose any requirement for any general or specific form of AV. Rather, at least with respect to commercial, classified R18+ content, which is the lowest impact category of Class 2 material, the RAS should focus on a more general requirement for service providers to take reasonable steps to limit children's exposure to age-inappropriate material. Such an approach would enable service providers to incorporate AV where it is safe, responsible, and appropriate for them to do so, either now or in the future, without forcing them to prematurely adopt AV technologies that are unproven, problematic, unnecessary, and damaging.

Question 7*: Should the new RAS be prescriptive about the measures used to limit children's exposure to age inappropriate material, or should it allow for industry to determine the most effective methods?*

The new RAS must not be prescriptive about the measures used to limit children's exposure to age-inappropriate material, but should rather allow for industry to determine the most effective methods of doing so. Different methods will of course be more appropriate for some services and less appropriate for others. For example, a parent may choose to use a mobile phone's facial recognition or swipe pattern security feature to prevent their child from accessing an app on their phone, a feature that may not be available on a PC or console, where an ordinary PIN code lock would instead be a better option. Allowing industry to determine the most effective method of limiting children's exposure to age-inappropriate material at the R18+ level will also ensure that the RAS will be flexible enough to both accommodate and encourage the experimentation and adoption of new technologies, systems, methodologies, and processes.

Additional information

Question 8*: Is there any additional information eSafety should consider in drafting a new Restricted Access System declaration?*

Notwithstanding that we share the Government's expectation that service providers should take reasonable steps to limit the access of children to age-inappropriate material, it is also important to acknowledge that if a parent has purchased an R18+ game, it is perfectly legal in many if not most states and territories for their child to play that game at home with parental permission. In fact, in order to remove any doubt, many state and territory classification enforcement laws have specific provisions permitting parents to let their children access R18+ games (see, for example, paragraph 39(2)(b) of the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (VIC) and paragraph 43(3)(a) of the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (ACT)).

This is also consistent with the reality that parents and carers overwhelmingly feel like they have a role and primary agency for determining what their children should and should not play. For example, research conducted by the Australian Government in 2016 found that over four out of every five Australian parents or carers believed that it was ultimately up to them to decide what is best for their children to watch or play. The research similarly showed that around seven in ten Australian parents or carers used classification categories only as a guide, rather than something that they follow strictly. While these views may not have been quite so pronounced in decades past when Australia's classification and online content schemes were first designed, we believe these views are reflective of a more modern community today that has a far greater familiarity and comfort around media and how to navigate children's media use.

To illustrate this, a parent may be happy for their child to engage in supervised play around a part of their R18+ game that they know does not contain age-inappropriate material, such as a discrete fishing mini-game or forest exploration level within a larger adventure game. While our industry does not encourage parents allowing their children to play R18+ games generally, we recognise that it can occur and also that it will often place the child at no risk. This is one of the ways in which attitudes around R18+ material differ most significantly from attitudes around X18+ and RC level material. This is also consistent with the general consensus of policymakers and communities globally, where content age ratings are overwhelmingly considered guidance for families only and legally-restricted categories are very rare.

We raise these points not to argue against the basis for a RAS, but rather to highlight the necessity for the design and implementation of a RAS that is flexible enough to allow industry to place greater agency with parents and carers on how to limit their child from accessing age-inappropriate material. Doing so will help the RAS to reflect more accurately the greater maturity and shift in societal expectations around the relationship between the community and the media that has occurred since the previous Online Content Scheme was first introduced into Schedules 5 and 7 of the Broadcasting Services Act almost two decades ago.

Any questions?

For more information on any issues raised in this submission, please contact IGEA's Director of Policy & Government Affairs, Ben Au, at ben@igea.net

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