FAO: Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)

ISGA Response to the Statutory Review of the Online Safety Act 2021

Introduction

The International Social Games Association respectfully provides this submission for your consideration as part of the statutory review of the Online Safety Act 2021. The statutory review of the Online Safety Act presents an opportunity to establish a flexible and proportionate regulatory framework that aligns with international best practices. This framework is essential to ensure safe online experiences for Australian gamers in a rapidly evolving digital landscape.

About the International Social Games Association

The International Social Games Association[1] (ISGA) is a global non-profit industry association established in 2013 to develop and communicate global best practices in social games, i.e. games played on mobile devices. Around 55% of video games played by Australians are played on mobile devices. The mobile games market is a vibrant, but complex, global consumer market. Our organisation therefore has a material interest in ensuring effective public policymaking in this area in all major jurisdictions, including Australia.

ISGA members include Playtika, Playstudios, Pixel United, Huuuge Games, SciPlay, and Zynga. We are strongly committed to proactive measures that protect Australians online through robust industry-led protections. In addition, we believe in the importance of education, as shown by media literacy initiatives such as the Smart Mobile Gamers website (www.smartmobilegamers.org), which has been developed with leading digital safety organisations, clinical psychologists and games researchers.

ISGA has developed and documented a set of 'Best Practice Principles' which have been regularly updated for over a decade, are global industry guidelines to provide players with the safest and most secure games experience. They are based on the core values of online safety, accountability and transparency. As such, they play an integral role in the mobile games industry's strong commitment to self-regulation, which Dr Aaron Drummond from the School of Psychological Sciences at the University of Tasmania has stated is the most effective form of regulation in the global games industry. ISGA is proud to be taking the lead in responsible standards for the sector and we are pleased that our Principles have been endorsed by an Australian Parliamentary Committee:

'The International Social Games Association (ISGA), the global industry body for social games companies (including simulated gambling games) specifically discourages its members from promoting simulated gambling products to users under the age of 18 years. The ISGA also provides an online resource called 'Smart Mobile Gamers' to give guidance, tips and advice on

---

[1] www.i-sga.org

topics such as parental controls and managing in-game spending. It has partnered with digital safety organisations and experts to create this website.'

Since we were established in 2013, ISGA has consistently engaged with regulators worldwide in navigating emerging issues in the regulation of online games, such as online safety, consumer protection and privacy by design. This includes the eSafety Commissioner's consultation on the Draft Online Safety (Relevant Electronic Services – Class 1 Material) Industry Standard, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) amendment to the Online Safety (Basic Online Safety Expectations) Determination 2022, and reforms to the Classification Scheme.

Table of Contents

Executive Summary

ISGA supports commitments to a fit-for-purpose online safety framework and welcomes the DITRDCA's review of the Online Safety Act 2021 to examine the effectiveness of the Act's regulatory approach. ISGA acknowledges that online safety is a shared responsibility, and the digital environment must be built with the safety of all users, in particular children, in mind. We believe that industry-led protections provide holistic solutions that protect all users and that equipping users, especially children, with digital literacy skills is crucial to empower them to navigate the online ecosystem safely and responsibly. Therefore, collaboration among industry and regulators, across jurisdictions is essential to avoid regulatory fragmentation that can lead to unintended consequences for the protection of all Australians.

Likewise, obligations for services in scope of the Online Safety Act must be 1) evidence-based, and 2) proportionate to the actual risk of harm present on a service. However, the current Draft Online Safety (Relevant Electronic Services – Class 1 Material) Industry Standard defines games with communications functionality as pre-assessed, meaning that the majority of online games will be disproportionately subject to minimum compliance measures akin to the

highest risk services, regardless of their size and risk. As such, the assessment of risk must include consideration of the mitigation measures that are already in place.

Further, Australia must ensure that its online safety framework does not result in regulatory fragmentation. Several jurisdictions have introduced or proposed new online safety frameworks and while they diverge in terms of scope, specificity and the obligations imposed on digital platforms, broadly, they share the same objectives. Nonetheless, Australia's OSA takes a novel approach (by international standards) to the classification of user-generated content (UGC) by classifying such content in a way which corresponds to the manner in which films and games are classified under the Scheme. This approach creates uncertainty about the scope of each instrument that will have an impact on the desired effect of these instruments. There must be a clear separation between content that is classified by the online safety regime (user-generated content) and classifiable content under the National Classification Scheme. It is imperative R18+ rated games are not treated by the Australian government in the same manner as harmful content, notably pornography and terrorism-related violence.

Finally, ISGA supports the need to protect children from harmful content. The decision by the Australian Government to provide resourcing to conduct a trial of age assurance technology is positive. Success will hinge on a range of issues, including data protection, evidence-based proportionality and technical feasibility – there is no one-size-fits-all solution. Still, coupled with work already underway to update the Classification Scheme, this trial has the potential to be very informative if it is executed well. As a result, ISGA is supportive of Australia's new classification regime for mobile games, which takes effect in September 2024. Outlining the Restricted Access System requirement for games rated R18+, hitherto undefined, is a crucial age assurance facet of the Classification Scheme that ISGA can provide subject-matter expertise from a global perspective.

ISGA Recommendations

1. There must be a clear separation between content that is classified by the online safety regime (user-generated content) and classifiable content under the National Classification Scheme.

2. A Restricted Access System requirement for games rated R18+ must be defined to provide certainty for mobile games – ISGA respectfully requests to be formally consulted about this issue.

3. The eSafety Commissioner should democratise access to risk assessments for all services in scope of the industry codes and standards.

4. Such risk assessments must account for evidence of actual harm arising in practice, on a service and the mitigation measures that have been implemented to further reduce the risk of such harms rising.

5. A flexible, evidence-based, proportionate approach should be extended to the classification of industry-regulated sections. For example, relevant electronic services include certain online games, messaging platforms and dating apps – all of which must adhere to the requirements of an ill-fitting single code.

Industry-Led Protections

A holistic approach to online safety should not negate the need for a thorough understanding of specific industries, after all, the online space is not a monolith. ISGA strongly believes that in considering online safety, mobile/video games are an overwhelming force for good, and, in Australia, the industry has a uniquely positive story to tell. Four out of five Australians are gamers, as it is a key form of stress relief and social connection[2]. According to Dr Jeff Brand, Professor at Bond University, '*Australians still play video games for fun, but this isn't the only reason. Games are increasingly appreciated for their diverse applications – people play to educate and upskill themselves, to stay socially and emotionally connected, as a motivator to stay fit, and to reduce stress.*'[3]

Emerging technologies have enabled us to optimise the consumer experience and find innovative solutions to societal issues in a unique and fun way. During the pandemic, mobile games recorded the highest ever download statistics. When creative industries were under threat globally, the games industry remained resilient. Across the anxiety of the pandemic, in solitude, games provided much needed solace, entertainment, social fulfilment and distraction. More recently, the Russia-Ukraine conflict has seen many mobile games companies providing aid to those in need, enabling a safe passage out of the country and facilitating refuge. Notably, one developer created the 'Rebuild Ukraine' mobile game, with 100% of net proceeds from advertising revenue donated to 'on-the-ground' charities.

In parallel, the online games sector continues to be an industry leader in addressing online safety. For instance, many mobile games companies are part of the Fair Play Alliance, a global coalition of gaming professionals and companies that has set out to achieve a gaming environment that is free from disruption and harms in online gaming. One video games company has set out to combat disruptive behaviour with in-game voice chat moderation that uses artificial intelligence to identify in real-time and take action against toxic speech. Another games company has launched a guide designed to help players address 'toxic' behaviours online in addition to launching a system devised with help from the UK police to tackle the most extreme forms of online harassment. These are a handful of examples that contribute to a strong evidence base regarding the positive nature of online games and how the industry strives to keep users safe online. Complementing this are ISGA's Best Practice Principles and ISGA's key game-play educational tool, the Smart Mobile Gamers website.

---

[2] Bond University. (2023, November 23). *Report led by Bond University Professor reveals 'The Power of Games' in Australia*. https://bond.edu.au/news/report-led-by-bond-university-professor-reveals-power-of-games-australia

[3] Ibid.

The National Classification Scheme (the Scheme) serves as a framework to provide parents and carers with advice on the content of video games and the Classification Board applies consumer advice where necessary. Australia is also a participating ratings authority of the International Age Rating Coalition (IARC), an organisation which provides free tools for game developers, including a questionnaire which produces country-specific classification information for mobile and digital games. The Scheme's role in providing important consumer advice that integrates with major game app providers means that users can apply effective content filtering on their/their children's devices. Mobile/video games that are professionally produced and distributed on a commercial basis, and directed at an Australian audience will continue to be effectively regulated by the Scheme. ISGA supports the steps taken by government to update the Scheme. Games companies use these helpful tools in taking tremendous care to mitigate the risk of harm to all users, in particular, children.

Approach to Online Safety

Obligations for services in scope of the Online Safety Act must be 1) evidence-based, and 2) proportionate to the actual risk of harm present on a service. ISGA is, therefore, encouraged by the outcomes- and risk-based approach to the Draft Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024. Nonetheless, while it is the eSafety Commissioner's position that risk assessments are an important way to reduce the risk of class 1A and 1B material being generated, posted, stored or distributed, 'games with communications functionality' are deemed to be 'pre-assessed' as high-risk services and therefore, they are disqualified from risk assessment requirements. This essentially deems such games to minimum compliance measures akin to the highest risk Tier 1 services.

As currently drafted, the Relevant Electronic Services (RES) standards undermine the policy intention, being that services are given the flexibility to implement effective, proportionate measures based on an accurate assessment of risk. ISGA is concerned that the guidance places a disproportionate emphasis on the risk of potential harm arising on a service, over the evidence of actual harm arising in practice and the mitigation measures that have been implemented to further reduce the risk of such harms arising. As such, the online safety framework should democratise access to a fair and proportionate risk assessment that includes consideration of the mitigation measures already in place. This would also allow for a more consistent and certain approach to online safety, which is in the interests of Australian consumers.

This approach should also be extended to the OSA classification industry-regulated sections. As the OSA salutatory review consultation's Issue Paper acknowledges, these categories reflect the core functionalities of the service. However, there is high variation in risk and service types within each category. For example, relevant electronic services can include communication aspects of gaming apps, messaging platforms and dating apps. This diversity creates challenges for a single industry code, as it fails to take into account the specific risks of each service type.

Content Classification

Australia's OSA is a world-first landmark framework that has most notably been followed in Europe with the Digital Services Act (DSA) and more recently in the United Kingdom (UK) with the Online Safety Act. All follow the same broad aims, to hold online services accountable for the safety of their users. In-scope services must, therefore, build systems and processes that effectively prevent harm at an earlier stage. Moreover, obligations are proportionate, meaning the largest platforms will have greater obligations, as they will have the capacity to address the high volume of user-generated content (UGC) on their services.

Here, global consistency will be an extremely effective tool in enabling in-scope services to operationalise compliance. The work of the eSafety Commissioner in leading the way in sharing best practices and as Chair of the Global Online Safety Regulators Network demonstrates this. Nonetheless, Australia's OSA takes a novel approach (by international standards) to the classification of UGC by classifying such content in a way which corresponds to the manner in which films and games are classified under the Scheme. The eSafety Commissioner, therefore, regulates potentially harmful online material classified or likely to be classified RC, X18+ or R18+ in respect of the Scheme. This approach creates uncertainty about the scope of each instrument, while also diverges from the international perspective.

For example, under the UK's Online Safety Act, scope services include user-to-user services, search engines and pornography content providers. While the rules largely focus on UGC, a section was added to later iterations of the bill; pornography content, which may be professionally produced, has been included to subject providers of such content which has age verification obligations. Pornography content is clearly an exception[4] to the rule that must be addressed in online safety legislation. ISGA also acknowledges the eSafety Commissioner's important role in addressing this. Accordingly, the focus of online safety rules should be limited to UGC, with the exception of porn content, as per the UK, a country with which Australia has signed an Online Safety and Security Memorandum of Understanding.

Regarding harmful content, the UK's OSA splits this into two categories, illegal content and content harmful to children. As set out in the Act, illegal content relates to, among other things, child sexual abuse, sexual exploitation, intimate image abuse, terrorism and fraud. This is broadly in line with Australia's assessment of class 1a and 1b material. There is a divergence when looking at classification of content that is harmful to children. In the UK, this is split into 'Primary Priority Content' (e.g., pornography, content relating to self-harm/eating disorders/suicide) and 'Priority Content' (e.g., bullying, abusive or hateful content, content that encourages serious violence or injury, danger stunts, using harmful substances). It is clear that in the UK, like Australia, protecting children is at the heart of online safety. However, because Australia's online safety framework uses the Scheme, content that is classified by the Scheme, such as films and mobile/video games, may face double regulation when they are clearly not at the heart of the intent of these online safety rules.

---

[4] *Unicef (n.d.). Protection of children from harmful impacts of pornography.* https://www.unicef.org/harmful-content-online

ISGA strongly believes that there should be a clear separation between the Scheme with the eSafety Commissioner's role as the online safety regulator. It is imperative R18+ rated games are not treated by the Australian government in the same manner as harmful content, notably pornography and terrorism-related violence. To ensure both maximum protection for Australian consumers as well as international harmony, there must be clear differentiation between pornographic content and mobile/video game content which is subject to classification. In addition, the difference between UGC and commercially produced content should be clarified to provide certainty for industry (and therefore, higher levels of compliance).

Previously, ISGA lodged a submission to the DITRDCA consultation on 'Modernising Australia's Classification Scheme – Stage 2 Reforms'. In this, ISGA provided information about the mobile games industry's support for the introduction of mandatory minimum classifications for computer games, which updated the classification of social casino games to R18+. Not only does this bring Australian classification in line with international standards, it will also result in the establishment of a Restricted Access System. This is a vital element in ensuring effective age assurance that will significantly impact mobile games – and the system is yet to be defined in digital settings.

Age Assurance

Age assurance is a central topic in relation to children's online safety, often cited as a plausible solution to ensure that users have access to appropriate content. Equally, ISGA firmly believes that age assurance must be considered in parallel to the classification reforms. Social casino games are set to be classified as R18+ from September 2024. However, the Restricted Access System (RAS) requirement remains undefined for the digital world. Given the diversity of the online world, which encompasses the mobile app ecosystem, streaming, PC/console games, etc, it is clear that a one-size-fits-all solution cannot apply. Given the global nature of the mobile games industry, if a RAS is to be effectively implemented in Australia, it is vital that the industry plays a leading role in working closely with government on the testing and development of a RAS. At the outset, to avoid significant, unintended consequences for the protection of Australian consumers, the mobile games industry should be continually consulted about the age assurance trial.

Age assurance presents a complex challenge due to the interplay between legal requirements and the effectiveness of verification methods. Recognising these challenges, we welcome the Australian Government's age assurance trial, which explores age verification and estimation technologies.[5] In this context, ISGA believes that OSA revision would represent an opportunity to evaluate the suitability of this Act as the legislative age assurance regulatory framework, alongside other measures to restrict children's access to harmful online content.

---

[5] eSafety Commissioner (2024). *Statement: announcement of age assurance trial*.https://www.esafety.gov.au/newsroom/media-releases/statement-announcement-of-age-assurance-trial

Despite the efforts to identify an approach to mitigate online risk, there is a general consensus that age assurance technologies are still under development.[6] A report commissioned by the UK's Information Commissioner's Office notes that age assurance 'techniques are, at present, a nebulous concept'.[7] Similarly, the French data protection regulator (CNIL) acknowledges that there is no 'miracle solution' to age verification, as the available technologies are either too intrusive or ineffectual.

Document-based verification, for example, carries significant risks, including data breaches, pervasive online tracking and potentially exacerbating existing inequalities for those unable to complete the verification process. Meanwhile, age estimation mechanisms, which predict user age through interaction patterns or artificial intelligence tools, heavily rely on data collection and profiling practices, raising concerns about data protection and potential bias. Further, age estimation algorithms may not be accurate for users from different ethnic backgrounds, introducing further bias into the system. A report by the US National Institute of Standards and Technology evaluating six age estimation algorithms found no single standout option, with error rates consistently higher for female faces.[8] Highlighting these concerns, the UK's online regulator launched an investigation into OnlyFans, an adult content platform, to determine if their age verification system, likely relying on age estimation, might be allowing underage users access to inappropriate content.[9]

A prescriptive approach to age assurance will fail to address the dynamic nature of the digital world, resulting in unintended consequences and a failure to capture the intent of the measures. Such unintended consequences could be experienced by Australian players of games because mobile games operate in a completely different medium to traditional video/PC games. Where video games played on PCs/consoles are designed for deep immersion and extended play sessions, the majority of mobile games are free-to-play and prioritise casual experiences for on-the-go play or short bursts of downtime. This makes it crucial for developers to provide a smooth and enjoyable experience that allows players to engage with various functionalities. Prescriptive age assurance may introduce friction points that do not serve the desired outcome and instead provide barriers to entry. This is characterised by the EU's General Data Protection Regulation legislation and the spread of 'cookie notices' that have been roundly criticised. In this case, regulations mandate lengthy

---

[6] https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf
[7] https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf
[8] NIST (2024). *NIST Reports First Results From Age Estimation Software Evaluation.* https://www.nist.gov/news-events/news/2024/05/nist-reports-first-results-age-estimation-software-evaluation#:~:text=Software%20algorithms%20that%20estimate%20a,that%20clearly%20outperforms%20the%20others.
[9] The Guardian (May, 2024). *OnlyFans investigated over claim children accessed pornography*. https://www.theguardian.com/technology/2024/may/01/onlyfans-investigated-over-claim-children-accessed-pornography

disclosures aimed at increasing transparency, but these often lead to user fatigue and superficial skimming, resulting in unintended data sharing.

Taking these considerations into account, ISGA advocates for a flexible and proportionate age assurance regulatory approach which also evaluates the risks associated with the particular online activity. Research commissioned by the UK's Information Commissioner's Office (ICO) and Ofcom to explore parents and children's attitudes towards potential age assurance methods shows that there is parental and child support for the principle of age assurance. However, parents expressed their preference for flexibility and therefore, rigid age restrictions often did not always feel appropriate. They tended to demand more robust measurements for activities that represent a higher risk, such as pornography or buying age-restricted goods, but less restrictive tools for gaming. [10] This preference stems from the perceived ease of circumventing methods like self-declaration, along with a desire for more control and flexibility.

It is important that age assurance measures are effective and proportionate and respect all children's rights. The United Nations Convention on the Rights of the Child (UNCRC)[11] emphasises the importance of children's leisure and recreational activities. In today's digital age, online games platforms can be significant spaces for children to foster imagination, problem-solving skills and teamwork.[12] However, strict age verification methods could potentially conflict with these developmental benefits. Therefore, regulatory frameworks need to strike a balance between creating a safer online environment for children and avoiding solutions that might result in unintended consequences, including for players of games in Australia.

Involving children, parents and stakeholders in the design and development of age verification methods is crucial as they can provide valuable insights based on their experiences, expectations, and concerns. Children's experiences also vary depending on their circumstances and developmental stages, meaning what is accessible and understandable to some may not be to others. In this context, it is important to view age verification not as the sole solution for online child safety but as one of several protective measures. This approach is acknowledged in the European Audio-Visual Media Services Directive,[13] which lists age verification alongside other methods, such as age ratings, parental controls and education campaigns, that allow users to make informed decisions. In this regard, ISGA welcomes the

---

[10] ICO & OFCOM (2021). *Families' attitudes towards age assurance.* https://assets.publishing.service.gov.uk/media/6343dd3f8fa8f52a5803e669/Ofcom_ICO_joint_research_-_age_assurance_report.pdf

[11] Unicef (n.d). *Convention on the Rights of the Child.* https://www.unicef.org/child-rights-convention

[12] Granic et. al (2014). *The Benefits of Playing Video Games.* https://www.apa.org/pubs/journals/releases/amp- a0034857.pdf

[13] *Directive - 2010/13 - EN - EUR-Lex.* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32010L0013

announcement by the Albanese government to invest $1.0 million between 2024 and 2025 to fund education and awareness of the Government's new mandatory classifications for gambling-like content in computer games.[14]

Competition Threats

While finding the most effective regulatory approach for age verification is paramount, another critical issue is the role of app stores and their verification systems in this process. This is especially important to consider for mobile games, which operate in this ecosystem and are subject to platform policies. As the eSafety Commissioner has pointed out, this issue presents competition concerns. If the responsibility of age verification falls solely on a handful of companies, such as app stores or operating system developers, it could significantly strengthen their dominance, with detrimental effects for both service providers and users.

The Australian Competition and Consumer Commission (ACCC) has identified similar concerns within the app distribution ecosystem. Markets prone to 'tipping,' where one or two firms hold a dominant position, often lead to anti-competitive fee structures.[15] These structures could become a major barrier for smaller developers struggling to comply with age verification requirements. Furthermore, larger companies with a significant interest in their own verification tools might be incentivised to hinder the adoption of independent safety providers. This raises data privacy concerns, as user information could become concentrated within a limited number of companies.

This situation emphasises the need for a regulatory framework that promotes a broad spectrum of technology-agnostic solutions to address age assurance. A prescriptive approach, especially in markets susceptible to tipping, could stifle innovation and competition within the industry.

Conclusion

ISGA appreciates the opportunity to contribute to this important consultation and we would be pleased to provide further information to the department on request.

---

[14] Ministers for the Department of Infrastructure (2024). *Boosting connectivity and safety for Australians*. https://minister.infrastructure.gov.au/rowland/media-release/boosting-connectivity-and-safety-australians

[15] Australian Competition and Consumer Commission (2022). *September 2022 interim report.* https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/september-2022-interim-report