IGEA

interactive games & entertainment association

Submission to the Attorney-General's Department

Response to the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 Exposure Draft

December 2021

Introduction and 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 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.

Video game industry data practices

The industry that we represent provides the means for Australians to play games by themselves and with communities at home and abroad. Australian gamers are overwhelmingly adults, with around four out of five game players being over the age of 18. While our industry is a significant and increasingly digital industry, video game companies differ significantly from many other popular digital services – including social media services – in two significant ways. First, games and gaming content continue to revolve overwhelming around a traditional business model of the purchase of goods and services. Only a small proportion of the video games industry's total revenues comes from advertising or other data-driven practices. As a result, many video game companies primarily use player data for legal reasons, to support the operation of their games and related services, and to improve player experience.

Game companies collect consumer data responsibly, practice data minimalisation, and keep end-user personal information secure. Our industry is committed to upholding all Australian privacy and data management laws, providing multiple and clearly-worded privacy notices to give transparency to players, adopting best practice account security measures, and, for many platforms, offering privacy settings to give players choice around how their data is used.

Not only is data used largely by game developers to make their games better for players, but the use of personal data for this goal is a core expectation of players. Most importantly, player data, when it is collected, helps to ensure that games run well and players can have the best gaming experience possible. Developers use data to find bugs, identify areas of improvement, promote positive in-game behaviour, detect cheating, and to learn how to make even more enjoyable games. Games and gaming services may further use limited personal information such as email addresses to strengthen account security, or to help parents and carers to better monitor what their children play. The video games industry treats its responsibility to protect the data of its players as among its highest priorities, including by leading the digital industry in the pseudonymisation of their players through the widespread use of 'gamer tags'.

Inconsistency between purpose and impact of reform

It is clear from a reading of the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the draft Bill), as well as the Department's explanatory paper, the draft Regulatory Impact Statement (the draft RIS), and the Government's rhetoric around

the proposed reform, that its purpose is to strengthen regulation around businesses that collect and use personal information as a fundamental component of their business model, whether through targeted advertising or other data use. Despite this, as our submission articulates, the way that the draft Bill has been designed is not targeted and in practice also impacts on sectors and businesses that collect and process minimal personal information.

We support data regulation that is targeted, evidence-based, fit-for-purpose, and refined enough to not only differentiate between different kinds of digital services but also to impose different standards on them as may be appropriate and proportionate. We are therefore concerned with the impact that the proposed reforms may have on our members, despite the fact that no questions, let alone any data or evidence, have been raised in the Department's explanatory paper or the draft RIS of any concerns with how video game businesses collect and use personal information. Generally speaking, the data-driven advertising business model that the draft Bill is seeking to target is simply not typical of the video games industry. Despite this, video game businesses have not been explicitly excluded from the scope of the draft Bill.

We believe that regulation that is overly broad and indiscriminately imposes burdens on unrelated businesses that have a completely different risk profile to the intended targets of the regulation, should be avoided. Rather, regulation should take a flexible principles-based approach that is appropriately scoped and encourages good privacy practices, while avoiding overly prescriptive rules that will become out of date, stymie innovation, impose unreasonable red tape, or even have unintended negative impacts on privacy outcomes for end-users.

More information on our key policy positions, including on privacy and related topics, can be found on our website here.

Response to the draft Online Privacy Bill

We thank the Department for the opportunity to provide our views and feedback on the draft Bill. In our response, we have chosen to focus on six key threshold issues that we have identified with the draft Bill and the draft RIS, that we will address in turn.

Social media services

Draft text

Section 9 of Schedule 1 of the draft Bill proposes the following definition of "organisations providing social media services" to be inserted into the *Privacy Act 1988* as new subsections 6W(1) and 6W(2):

Organisations providing social media services

(1) An organisation is an ***OP organisation*** if the organisation:

(a) provides an electronic service that satisfies each of the following conditions:

(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users, including online interaction that enables end-users to share material for social purposes;

(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;

(iii) the service allows end-users to post material on the service;

(iv) such other conditions (if any) as are specified in a legislative instrument made under subsection (7); and

(b) Is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7).

(2) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard each of the following purposes:

(a) the provision of advertising material on the service;

(b) the generation of revenue from the provision of advertising material on the service.

While subsections (1) and (2) do not mention video games, table 1 of the Department's explanatory paper states that "examples of social media services" include:

Gaming platforms that operate in a model which enables end-users to interact with other end users, such as multiplayer online games with chat functionalities.

Our response

We do not support, for both technical and policy reasons, the position outlined in the Department's explanatory paper that a game or gaming platform may potentially be considered a social media service if it enables end-user interaction.

First, we question why it is at all relevant to the draft Bill whether or not a game or gaming platform has a chat functionality. As we explain below, end-users do not come to video games with chat features in order to use them like social media services. In-game chat, where it is

available at all, fulfils a specific role of facilitating game play. In the same way, we are not aware of the use of in-game communication for advertising or other data-driven business models.

Second, we strongly doubt whether a multiplayer online game with chat functionality would even satisfy the criteria of the proposed sub-section 6W(1). As discussed, we do not believe that the "sole or primary purpose" of online gaming is to enable online social interaction, as is required under sub-paragraph 6W(1)(a)(i). The primary purpose of video games is to facilitate gaming for its players, whether these games are played individually or with other people. To call gaming with a chat functionality an activity that exists "solely or primarily to facilitate social interaction" would be like calling a media outlet where readers can discuss and leave comments on articles (eg. *The Australian*) a social media service, or an e-commerce website where buyers can exchange product reviews (eg. *Harvey Norman*).

Any traditional social interaction that occurs in video gaming, where it is even technically possible, is minimal and always directly related to the gameplay experience. For example, even where there may be a limited or rudimentary text-based (or sometimes voice-based) chat functionality in a game or on a gaming platform, such as chat within a specific game or between the users of a gaming device, it is overwhelmingly or fully used only to facilitate gameplay, such as to organise teams, share gameplay knowledge, or to establish a strategy (and even then, most players choose to use third party platforms like Discord). End-user communications in games serve no broader social role. In fact, we would argue that games with chat functionality fall clearly within the scope of the comment in table 1 of the explanatory paper that the definition of social media services is "not intended to capture organisations that enable online communication / interactions / content sharing as an additional feature".

Other examples of services like video games that have an ancillary communication element but are clearly not social media services include the above examples of *The Australian* and the *Harvey Norman* websites, as well as exercise and mindfulness apps where end-users can 'thumbs-up' one another. Social interactions may make the experience of all of these services more enjoyable or meaningful, but they are not the sole or primary purpose of the activity.

Games and gaming services are clearly different to social media services, both in terms of their general and well-understood characteristics, as well as in matters relevant to privacy regulation. To treat a game, where a player may momentarily chat via text with a handful of other players about that game, as equivalent to a social media service where a person is expected to post text, images, videos, and other content to their hundreds, thousands, or even millions of friends or followers, clearly demonstrates false equivalency. We have provided the table below to further articulate the real and practical gulf between games and gaming platforms with a chat functionality on one hand, and social media services on the other:

Characteristic	**Social media services**	**Games / gaming platforms**
What is the purpose of the service?	To facilitate social interaction.	To facilitate game play.
What is their revenue model?	Most popular services are primarily advertising-driven.	Primarily through the direct purchases of games and gaming services.
Are they free to consumers?	Practically all popular social media services are free.	Practically all popular games are purchased. Even 'freemium' games typically generate their

		revenues through in-game purchases of gaming content.
Do end-users message or post material in their own names?	Accounts and posts are commonly linked to identifiable persons, often via their names.	There is widespread use of pseudonyms, 'gamer tags' and avatars in games.
Do end-users have profile photos or post photos of themselves?	Use of profile photos are common.	Profile photos are not a common feature and are often technically impossible.
Can you easily search for particular end-users?	Many social media services easily allow for people to find or discover other people.	Real name search functionality is generally not possible. To search for real world people, the end-user would need to know that person's pseudonymous user-name, such as their gamer tag.
What communication functionality exists?	Both text and audio-visual, including the sharing of images and video.	Generally text only, if at all, with limited voice chat also available on some platforms. Many players typically also prefer to communicate via third party platforms like Discord.
Is 'individual-to-many' communication possible? (eg. public posts, posts to friends, forum comments)	Commonly, yes.	The majority of communications on gaming platforms are private messages between friends or via in-game chat lobbies. Mass-messaging is rare, if not non-existent.
Would the service still exist if no communication were allowed?	Most if not all social media services would cease to exist.	Gaming would continue as normal (text or voice chat is not essential for gaming). Many players typically also prefer to communicate via third party platforms like Discord.
If there was no interaction between users at all, would people still use the service?	Without any social interaction, social media services would most likely not exist.	Yes – single player games or game modes, without any interaction with other players, remain highly popular.

We therefore strongly disagree with the inclusion of gaming in the list of examples of social media services in the explanatory paper. As gaming is not a social media service and shares no similarities with social media service, it is perplexing and confusing that it has been included in the explanatory paper. Further, gaming is not considered to be a social media service under the *Online Safety Act 2021* and should not be considered so under the draft Bill either.

Our recommendations

First, we recommend that the concept of "online social interaction" in sub-paragraph 6W(1)(a)(i) be reviewed and clarified, either in the legislation itself or in the future Explanatory Memorandum to the bill that will need to be drafted, to ensure that it does not cover activities such as online gaming that Parliament did not intend to be covered.

OP organisations could relevantly be defined as large social media services where the sole or primary purpose of the service is to enable social interaction between two or more end users, allows end-users to post material on the service (etc.), consistent with the definition of social media services in the *Online Safety Act 2021*. For clarity, we suggest that the definition or Explanatory Memorandum could even specifically exclude services principally for online gaming where chat or other social interaction between players or observers of player is an ancillary feature of the service.

On a related note, the example of 'gaming platform' included in table 1 of the explanatory paper should not be included in the Explanatory Memorandum to the bill unless, as suggested above, it is to be included in a statement outlining the kinds of services that are *not* intended to be captured under the definition of social media service. As mentioned earlier, we note that table 1 of the explanatory paper states that the definition of social media service is "not intended to capture organisations that enable online communication / interactions / content sharing as an additional feature". If such commentary is included in the Explanatory Memorandum to the bill, this should specifically cover games and gaming platforms.

Finally, a statement in the Explanatory Memorandum providing examples of services that are not intended to be treated as social media services should, in addition to games and gaming platforms, also list platforms that provide comments or chat box functionality, where such functionality is secondary to the primarily purpose of the service. These may include news or video sites where readers/viewers may write a comment to the content provider or other readers/viewers.

Large online platforms

Draft text

Section 9 of Schedule 1 of the draft Bill proposes the following definition of "large online platforms" to be inserted into the *Privacy Act 1988* as new subsections 6W(4) and 6W(5):

Large online platforms

(4) An organisation is also an OP organisation at a particular time in a year if the organisation:

(a) either:

(i) for an organisation that carried on business in the previous year—had, in the previous year, at least 2,500,000 end-users in Australia;

(ii) for an organisation that did not carry on business in the previous year—has in the current year at least 2,500,000 end-users in Australia; and

(b) collects personal information about an individual in the course of or in connection with providing access to information, goods or services (other than a data brokerage service) by the use of an electronic service (other than an electronic service covered by subsection (1)); and

(c) is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7).

(5) However, an organisation is not an OP organisation for the purposes of subsection (4) to the extent that the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme.

Our concerns

We do not agree with the approach of defining 'large online platforms' as 'OP organisations' simply on the basis of their size as well as the overly broad and simple requirement that personal information be collected "in the course of or in connection with providing access to information, goods or services".

The first arm of the definition (a requirement for 2,500,000 end-users) appears arbitrary to us, while the second arm (collection of personal information) seems to set a bar so low that the collection of an email address by a platform would appear to be sufficient to meet the requirement. Under the proposed approach, a video game company that collects the barest minimum of personal information in connection to a game, but has 2,600,000 Australian players, would be considered an OP organisation while another digital service that generates advertising revenue via the collection and use of the personal information of its end-users, but has just 2,400,000 Australian users, would fall outside of its scope.

It is also not entirely clear from the drafting whether an organisation that has several unrelated services that cumulatively, but not individually, have 2,500,000 Australian end-users would fall within the scope of the definition of a 'large online platform'. If such organisations are covered, this presents particular challenges for the video games industry that we represent. Perhaps uniquely to our sector, it is possible for even quite small video game development studios, often employing less than ten staff, to have several popular digital products at once. Most will not have a user base anywhere near 2,500,000, but if some achieve modest success, cumulatively they may reach that threshold. Such studios often collect little to no personal information, and the little information they might collect via their different games may not

necessarily be held centrally in a single database, further reducing privacy-related risks. We argue that such organisations are outside of Parliament's intended scope of 'OP organisations'.

Finally, it is not clear why organisations that "collect personal information about an individual in the course of or in connection with providing a customer loyalty scheme" have been excluded from the scope of an OP organisation. No policy reason has been given in the Department's explanatory paper for this exclusion. While we note that the paper states that such schemes will be addressed as a part of the broader privacy review, so will all other online platforms. Given that one of the primary reasons that organisations will administer a customer loyalty schemes (if not the most important reason outright) is to collect data on the browsing and purchasing habits of its customers and to use this data to focus marketing and increase sales, and given that such schemes often have millions of members, it is not clear why they are not considered OP organisations. By contrast, an organisation like a video game company that collects far less personal information and might have few fewer users (but still over 2,500,000) might still be considered an OP organisation.

Our recommendation

To address our concerns raised above, we recommend that subsection 6W(4) be amended to impose a more precise and targeted threshold for 'large online platforms'.

While the Department's explanatory paper states that 'large online platforms' are "intended to capture organisations who collect a high volume of personal information online" such as Apple, Google, and Amazon, as well as (advertising-revenue driven) media sharing platforms like Spotify, the actual current scope of 'large online platforms' in reality also captures smaller services and services that collect minimal information such as many video game companies.

For example, the definition could be amended to also include an additional requirement that 'large online platforms' must solely or primarily derive their revenue from advertising, and/or exclude services that collect only minimal personal information such as the information reasonably necessary for serving its customers and providing its services. We also recommend that organisations should only be considered 'large online platforms' if at least one of its specific products or services has 2,500,000 end-users in Australia.

Finally, we ask the Government to explain the rationale for singling out customer loyalty schemes as being excluded from the definition of 'large online platforms' (and nothing else), and why no opportunity has been provided for other parts of industry to similarly make their case for exclusion prior to the completion of the draft Bill.

Age verification

Draft text

Section 20 of Schedule 1 of the draft Bill proposes an 'age verification' requirement for social media services to be inserted into the *Privacy Act 1988* as new paragraph 26KC(6)(a):

> (6) Without limiting subsection (5), the OP code must require OP organisations of a kind covered by subsection 6W(1) to do the following:
>
> (a) take all reasonable steps to verify the age of individuals to whom the OP organisation provides an electronic service;

Our concerns

We strongly disagree with the proposed requirement, to be captured within the OP code, for social media services to take all reasonable steps to verify the age of individuals who use an electronic service.

First, we note the use of the term "age verification" rather than "age assurance." The term age verification (AV) typically refers to the processes determining a person's age with a high level of accuracy by checking against trusted records of data. Online services typically accomplish age verification the by directly collecting and verifying hard identifiers, such a government issued ID, or through the use of a third-party verification service.

As we outlined in a submission that we recently lodged with the eSafety Commissioner with respect to the Online Content Scheme under the *Online Safety Act 2021*, it is generally accepted by governments, the civil sector, and within the digital industry (with the exception of the private AV industry) that although there have been some incremental improvement in AV technology in recent years, there are currently no AV methodologies that are reliable, practical, cost-effective, and also do not carry significant risks to the community. The most obvious example of the impracticability of AV is the decision of the UK Government in 2019, after years of scoping and even after putting the enabling legislation into place, to ultimately abandon its plan for an AV system for online pornography.

Even ignoring questions around the technological viability of various AV methodologies, there is a wide disparity of philosophical views and fierce debate between key stakeholders including the community, industry, policymakers, and consumer and privacy advocates around what role, if any, AV should play in regulating access to online pornography - let alone far-lower-risk forms of online activities such as the use of social media services or online game services. To provide an example of how significant a decision to implement AV should be, the eSafety Commissioner is currently being tasked by the Government to develop a roadmap for the potential use of AV technology to restrict online pornography. This is a highly forensic, long-term scoping process studying whether and how AV could be used for a very specific purpose related to a very specific form of high-risk content. By contrast, the draft Bill is casually proposing to impose AV across all social media services, with little evidence provided of thorough prior policy analysis.

In our commentary on this topic, we would first like to draw the Department's attention to the UK Information Commissioner's opinion on 'Age Assurance for the Children's Code', released in October of this year. The UK Commissioner applies a strict definition of AV and urges general

caution against the use of AV except in necessary and limited circumstances. In fact, the UK Information Commissioner highlights the risks involved in all types of methods of age assurance, including AV, and suggests that because of the inherent risks, the method employed should be proportionate to the potential harms.

For example, on pages 10-11 of the opinion, the UK Information Commissioner outlines a range of risks with age assurance (including AV):

> Age assurance must be used carefully as it carries its own types of risk. For example, it:
>
> - may be disproportionately intrusive. For example, age verification checks often require access to official data or documentation which can include special category data;
> - may introduce risks of bias and inaccuracy. For example, some emerging approaches to age estimation are based on profiling or facial analysis using AI;
> - may result in exclusion or discrimination of already marginalised groups due to bias, inaccuracy or requirements for official documentation. Those in more deprived socio-economic groups are more likely to lack requisite documentation, and more likely to be affected by algorithmic bias. Non-white ethnicities and people with disabilities are over-represented in these groups. Individuals may be unable to use some types of age assurance due to physical or cognitive reasons and risk being excluded from services they are entitled to access;
> - is not fool-proof. Any approach has some risk of incorrectly classifying a child as an adult or as an older child. This could potentially allow them access to inappropriate or harmful services or material. Conversely, an adult may be incorrectly classified as a child, and be denied access to services they are legally entitled to use; and
> - some methods can be circumvented. For example, a child or parent could provide false information in a self-declaration or a child could log into their parent's account to complete account confirmation.

Because AV poses some of the greatest risks, the UK Information Commissioner's opinion explains (at page 35) that AV has to date generally been limited to "sites that provide goods or services that attract criminal or civil penalties for serving underage customers: online retailers who sell age-restricted products, for example alcohol, tobacco products including vape, and knives".

In our earlier submission to the eSafety Commissioner, which remains relevant in this context, we highlighted a range of specific risks to the community associated with AV processes. This perspective on AV is widely held, even among child rights advocates. For instance, the UK-based child safety advocacy group, the 5Rights Foundation, has outlined risks it perceives in both AV and other age assurance approaches in a March 2021 paper titled 'But how do they know it is a child?'. We have summarised the Foundation's analysis of these risks in the following table:

Risks to the community from the use of AV	**Relevant AV technology / process** Please see the full 5Rights Foundation report for an explanation of the AV technologies listed.
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	All

do so to obtain the same access in the physical world), leading to services and information being denied to them	
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

Further, UNICEF this year also published a report titled 'Digital Age Assurance Tools and Children's Rights Online across the Globe' that 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).

Our recommendation

For the reasons that we have outlined below, we recommend that the requirement for social media services to verify the age (even on a 'reasonable steps' basis) of individuals who use an electronic service be removed from the draft Bill.

First, given the wide meaning given to 'social media services' in the draft Bill, an age verification requirement leads to a too-significant risk that digital platforms will implement unproven or dangerous processes or technologies that may cause harms to children and the wider

community and that are not proportionate to the risks to children that may exist in using the online service. As discussed above, there remains significant concern among all relevant stakeholders around the efficacy and harms of most if not all AV processes and technologies.

Second, the technical challenges around AV that we have already covered in this paper are difficult enough when targeted at the age of adulthood (ie. 18 years of age) and become even more dangerous when targeted at the age of 16 as the draft Bill does. At the age of 16, there are even fewer avenues for effective AV (eg. a child of 16 will generally have less access to documentation than an adult of 18), while the risks of harm from AV are even higher because the draft Bill will be requiring children aged 16 and 17 to undergo AV, including potentially disclosing sensitive personal information, before they can legitimately access a range of digital platforms and services.

Further, and perhaps most significantly, assuming AV is even possible, a requirement for AV would likely force many services to collect more data from children than they would otherwise need or want to collect. In other words, a platform that would not otherwise ask a customer for any personal information, such as their name, or require them to link their account with another account tied to their personal information, such as a credit card, may be compelled to do so in order to comply with a future OP code. Depending on the requirements of the code, they may also need to hold this sensitive data for an extended period of time. Obviously, this result is counter-productive, particularly in a proposed new regulatory reform aimed at strengthening privacy outcomes for individuals.

This requirement also imposes, by the Department's own calculations, an extremely high cost on social media services. The Department's draft RIS, at page 23, predicts implementation costs for social media services in the order of over half a billion dollars ($526,203,500) solely in relation to the proposed age and parental consent requirements. This is one of the highest figures we have ever seen in any RIS. Given the broad definition given to social media services, this is a cost that is not only burdened upon the largest and most popular services, but also upon smaller start-up platforms that have achieved popularity but not necessarily any significant revenues.

Bearing in mind all of these concerns and the significance of the implementation cost to industry, we also cannot ignore the reality (not mentioned in the explanatory paper) that even many 'strict' AV mechanisms can easily be bypassed using widely accessible and highly effective VPNs. It is our understanding that the vulnerability of AV to VPNs and related technologies was one (of the many) reasons why the UK Government made the policy decision to abandon its attempt at implementing AV for online pornography.

While our strongest recommendation is that the AV requirement be removed from the draft Bill in its entirety, should it be kept, 'age verification' must be replaced with another term such as 'age assurance'. In common usage, 'age verification' generally demands a certain high level of confidence around a person's age, by checking against trusted, verifiable records of data, which for the reasons covered in this submission may not be technically achievable, nor even proportionate given the increased intrusion into end-users' privacy that will be necessary for compliance.

A term such as 'age assurance' may strike a better balance by enabling social media services to adopt a more reasonable approach to age gating that may be achievable with less intrusive means. We are currently observing in the policy discussions across the EU and the UK a move away from any language around age verification and towards 'age assurance'. On this topic,

we also highlight the importance of the Australian Government moving in alignment with other, larger territories wherever possible, especially on any expectations around age assurance, rather than to necessarily trial a novel or extreme regulatory approach. Supporting a more consistent global approach will enable the industry in Australia and overseas to achieve regulatory compliance more effectively and quickly.

Finally, the "take all reasonable steps" qualifier in the current language must also be kept as it provides vital flexibility for social media services to undertake age assurance in the most effective and practical manner in the circumstances. Such an approach would enable service providers to incorporate age assurance where it is safe, responsible, proportionate, 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 potentially damaging.

Parental consent verification

Draft text

Section 20 of Schedule 1 of the draft Bill proposes a 'parental consent verification' requirement to be inserted into the *Privacy Act 1988* as new paragraphs 26KC(6)(b)-(d).

> (6) Without limiting subsection (5), the OP code must require OP organisations of a kind covered by subsection 6W(1) to do the following:
>
> > (b) obtain the consent of a parent or guardian of a child who has not reached 16 years before collecting, using or disclosing personal information of the child;
> >
> > (c) if the OP organisation becomes aware after it collects, uses or discloses personal information of an individual that the individual is a child who has not reached 16 years, obtain the consent of a parent or guardian of the child as soon as practicable after becoming so aware;
> >
> > (d) take all reasonable steps to verify the consent obtained for the purposes of paragraph (b) or (c);

Our concerns

Just as age verification sets a very high bar given the expectation of a high degree of confidence around the age of an end-user, a requirement for parental consent verification similarly raises many of the challenges outlined in the previous section.

These challenges include technical capability, the unnecessary collection of personal information, and significant implementation costs to industry. Taking a plain reading of the text, it is also not entirely clear to us what technological methodologies would constitute reasonable steps to 'verify' that consent has been provided short of also requiring age verification of not only the end-user's parent but also verification of their familiar relationship. Both of these steps, assuming they were even feasible, would require significant personal information to be disclosed for this singular purpose - steps which we would consider to be a disproportionate requirement.

We also question why the age of digital consent in the draft Bill has been set at 16 when in most other countries the threshold is set at 13. No evidence or rationale is given in the explanatory paper or the RIS as to why a higher age is necessary, appropriate, or justified.

Finally, we ask whether the Department has considered the social implications of a parental consent requirement for accessing social media services. For example, what impact, if any, a parental consent requirement may have on children currently using, or who may in future use, social media services to obtain health (including mental health) information and advice without, for one reason or another, the express involvement or knowledge of their parents. Given the increasing number of social and community services that now rely on social media platforms to connect with young people, this example is not a far-fetched one.

Our recommendations

Similar to our views regarding age verification, we recommend that 'verification' be removed from this requirement, and that it be replaced with a more flexible approach of

requiring the service provider to simply take all reasonable steps to obtain parental consent for end-users who are children under the age of 13.

We recommend that the reasonable parental consent requirement be limited to children under 13 in order to be in alignment with the age of digital consent set by the majority of countries, including the UK and the US. This will allow service providers to design and implement practical, effective, and appropriate systems for obtaining reasonable assurance that consent has been given and will more appropriately consider the developmental maturity of teens.

One practical method for parental consent, which was recently recognised by the UK Information Commissioner in its recent opinion (highlighted at page 36), is the use of linked or family accounts where only the account-holder's details need to be verified, as is common in the video games industry, as a practical method of ensuring a practical degree of parental control without imposing an unreasonable burden on both families and service providers:

> Many platforms and services offer the option to have linked or family accounts. This means that there is a main account holder but additional profiles are set up for other users, such as children. As part of this, linked or family accounts can be used to confirm the age of an account or profile user with the main account holder. This is a useful way of enabling children access to an age appropriate version of a service, whilst ensuring there is parental control.

Such an approach also encourages parents and carers to adopt genuine accountability and agency with their choices over the apps and services that their children use, rather than a 'box ticking' exercise that parental consent verification inevitably devolves into.

Regulatory Impact Statement

While we appreciate that the draft RIS recognises many of the burdens that will be imposed upon industry by the draft Bill, unfortunately it is our view that there remain some significant deficiencies in the draft RIS. Before the draft Bill progresses any further, much further analysis must be undertaken to assess, determine, and explain why such reforms are not only necessary, but necessary to be completed prior to the implementation of the broader privacy review.

First, we do not believe that the draft RIS (or the explanatory paper) presents a sufficiently compelling or evidence-based case as to why such far-reaching and impactful regulatory action is required. The only specific example of a deficiency that has been raised in the draft RIS is of Cambridge Analytica in the background section, an example that only concerns one platform, that occurred many years ago, that was already the subject of OAIC action, and that we understand has since been rectified. In fact, we believe that particular example demonstrates the effectiveness of the current privacy framework and provides no evidence as to why a new and costly regulation burden must now be imposed on over 500 companies.

No other specific concerns with non-compliance with Australian privacy regulations have been identified in the rest of the draft RIS, and while the Department does outline areas where regulation can be improved, we believe most will already be captured as a part of the separate privacy review. In particular, no specific evidence has been offered as to why age and parental consent verification is necessary for social media services, despite how impactful such requirements will be on both businesses and end-users.

The need for scrutiny over the policy justification for the draft Bill is necessary given the significant economic costs that it imposes. By its own calculations, the Department estimates that there will be a one-off code development and implementation cost of over half a billion dollars ($530,153,678.75) as well as ongoing regulatory costs of $7,943,457 per year. First, we believe this figure to be an underestimation of the actual likely cost to businesses. For example, we think the OP code will impact more than just 500 organisations and will require far greater than 60 hours of staff time per organisation (as the RIS estimates). 60 hours of staff time per organisation is only a week and a half of time for a single staff member, which we consider to be considerably less than what we believe organisations will actually need to dedicate in order to implement the OP code, considering its wide scope and requirement for ongoing action. Not mentioned also in the cost calculations in the RIS is any consideration of research and development of measures needed to comply with the OP code or any initial or ongoing costs to third party age assurance service providers, both of which may be massive cost drivers.

Nevertheless, even the Department's own estimates of the regulatory costs of the draft Bill are staggering. The figures also indicate that the overwhelming majority of this cost to industry is driven by the age and parental consent verification requirements, at $526,203,500. In other words, over 99% of the half-billion-dollar implementation cost of the draft Bill is tied to the age and parental consent requirements alone, requirements that we believe that no case has been adequately presented as to why they are necessary to be implemented. We also note that the draft RIS estimates that the cost to OP code developers, being industry associations, will likely be $882,078.75. This is an extremely high figure which will have an impact on industry associations that we do not believe the draft RIS fully appreciates. The magnitude of such an implementation cost would likely crush many associations if imposed upon them.

Similarly, we do not believe that a sufficiently robust cost-benefit analysis has been undertaken in drafting the RIS. Despite identifying a half-billion-dollar initial implementation cost and significant ongoing costs to businesses, the draft RIS only includes a short half-page summary of the benefits (to individuals) of the proposed reforms on page 22. Further, the benefits discussed only cover what we would argue are relatively administrative matters such as increased confidence in the OAIC, higher clearance rates for the OAIC's complaint clearance process, greater conciliation and remediation processes, increased penalties, and the fact that it will help Government to "send a message" about privacy. It is difficult to see how these benefits clearly outweigh the regulatory impact of the proposed reform, despite the draft RIS taking such a position.

We also note that none of the benefits listed here relate directly to the new age and parental consent verification requirements being imposed – requirements that constitute over 99 per cent of the regulatory costs under the Department's analysis. This demonstrates to us that much more work is needed for the Government's cost-benefit analysis. We further note that no costs to individuals have been identified in the RIS, such as the cost to the public if certain platforms decide to withdraw their services from Australia or start to charge a cost for the use of their services that had previously been free.

We recommend that the draft Bill not proceed until a more detailed RIS process is undertaken.

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