IGEA

interactive games & entertainment association

Submission to the Attorney-General's Department

Review of the Privacy Act 1988

November 2020

Linked table of contents

Executive Summary

Who is IGEA?

IGEA is the industry association representing and advocating for the video games industry in Australia, including the developers, publishers and distributors of video games. We 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 is also known for organising the Game Connect Asia Pacific (GCAP) conference for Australian game developers, and the Australian Game Developer Awards (AGDAs) celebrating the best Australian games of the year.

You can find a list of IGEA's members on our website: https://igea.net/about/members.

Introduction

IGEA welcomes the opportunity to provide a first response to the Attorney-General's Department's (AGD) two-step consultation on a review of the Privacy Act 1988 (the Act). As the Issue Paper notes, the digital economy has brought immense economic growth and prosperity to Australia and our region, including faster and better products and services. This has been fuelled by increased engagement and interaction between businesses and consumers. These benefits notwithstanding, it is appropriate that the Act, like all laws, remain fit-for-purpose for individuals and the businesses they apply to.

Outline of submission

The video games industry is unlikely to be one that Government has front-of-mind as it embarks on this review. As a digital industry, however, our sector is an important stakeholder and it is critical that our members not only have clarity around their privacy obligations, but also confidence that the regulatory environment functions efficiently. This submission seeks to share an understanding of how video game companies use and protect data and to provide our initial views on the key topics outlined in the Issues Paper.

The first part of this submission provides background on the video games industry and the precise (and often specific and limited) ways that game companies may collect and use the personal information of their customers. The variety of practices and technologies employed to ensure individuals' privacy are also outlined. We then provide an overarching statement on our sector's perspective on what the Act, if the Government decides to reform it, should look like. In a sentence, we favour flexible and balanced data regulation that supports, rather than impedes, our industry's longstanding commitment to responsible data management that allows game companies to use data in innovative ways to make better games and experiences for players while prioritising privacy.

The second part of this submission provides more detailed responses to select questions asked by the Issues paper. Consistent with our overarching themes, our specific responses generally articulate the importance of, and provide direction for, a pragmatic and flexible approach to data regulation. Due to the short timeframe for this consultation, we have not been able to address each of the 68 questions in the Issues Paper. However, we have tried to respond to the key questions of most immediate relevance to our sector.

We hope this submission is useful to AGD for its initial policy development process. We would invite further opportunities to discuss matters raised in this submission and look forward to providing a more detailed submission in response to the Discussion Paper.

Background and key issues

Snapshot of the video games industry

Video games are enjoyed by over a third of the world's population, including two-thirds of all Australians. Estimated to be worth around $250 billion this year, we are one of the largest and most popular creative and entertainment industries in the world. Video games have become even more critical in 2020, as globally it has remained a resilient sector of many countries' economies and labour forces despite the broader disruptions caused by COVID. Most important, video games have unexpectedly become a vital tool in encouraging and helping people to self-isolate, while keeping them positive, occupied and connected to their family and friends via games' network features.

There is, of course, an industry that creates video games and all the various devices and platforms on which they are played. While most of the video games industry is based overseas, Australia is home to an exciting and increasingly-important game development sector. Despite receiving no federal support, unlike every other creative sector, Australian video game developers generated $143 million in income in 2018-19 and employed 1,275 fulltime workers. 83% of this income was generated in export markets, and some Australia-made video games, such as *Fruit Ninja, Crossy Road*, *Hollow Knight* and *Untitled Goose Game* are among Australia's most successful cultural export of the past decade, the equal to if not greater than any Australian film, show, music or book.

How the video games industry uses data

Video games are a highly digital industry, with the majority of video game sales in Australia now delivered digitally rather than via discs purchased in stores. Digital industries are global by nature, and video game businesses are no exception to that.

Video games are a form of artistic expression and entertainment that is driven by data. Quite simply, video games today could not exist without data, including data generated by players as they interact with games. This data is crucial for the development of games and the continuous creation of new game content that our players demand. It is also crucial in ensuring our players experience a positive, frictionless and – most importantly - safe gameplay experience for players, particularly younger children. We believe that not only is data generated by players in video games overwhelmingly used by game developers to make their games better and to make better games in the future, but the use of this data for these purposes has also rapidly become a primary and default expectation of players.

Important ways in which aggregated or individual customer data is collected or used by video game companies include:

- Supporting parents and carers to ensure children play age-appropriate games, such as by asking for a player's age in a game
- Providing a suitable online environment for young children by monitoring (and collecting or storing) language in chatrooms and between players
- Addressing harassment or other unacceptable behaviour by taking appropriate action against toxic players such as muting, suspensions and bans, which may require data to be kept in order to enforce disciplinary measures

- Enabling games and consoles to remember user settings including not only game preferences but broader settings such as customised family controls (eg. content restrictions or time limits for a child's user account)
- Identifying software errors or bugs experienced by players so that they can be as quickly as possible fixed through changes to the game and software patches
- Detecting fraudulent behaviour within the player community so that suspicious accounts can be quarantined, suspended or terminated efficiently
- Strengthening network and account security by utilising customer data to improve authentication measures and to identify unusual activity better
- Detecting cheating behaviour or software so that players are all provided with a fair and competitive gaming experience, which may require data to be collected
- Providing players with a competitive gaming experience by analysing a player's gameplay data and dynamically adjusting the game's difficulty or matching them with other players who are most suitable for their skill and level
- Ensuring that the game performs and runs well by using non-precise location data to match players on the most appropriately-located servers to prevent 'lag'
- Improving a game's design by seeing how people play them, which can help to identify bottlenecks or areas where the game can be improved
- Continual product improvement through regular patches and software updates to games, as well as new content, all of which depends on data
- Enabling ongoing innovations in-game technology, with examples being the use of a device's camera for augmented reality games, or using GPS data for geolocation-based games, which may require new kinds of data to be collected
- Enabling richer social interaction in gaming, given that games are very often a social activity among family and friends, such as letting players know when their friends are playing, and allowing them to stream or share content online
- Rewarding players within a game such as by celebrating high achievements in the game's community scoreboard and giving prizes
- Encouraging players to create and share user-generated game content within the game and externally, and allowing players to 'own' that content
- Enabling game data to be transferred across devices, a critical need given that many players maintain an account or play games across multiple devices
- Allowing game players to re-download a game even if they have lost their device or a physical copy of their game, which requires account-specific data
- Improving the design of future games by helping developers to track what and how their customers play games, identifying parts of the game that they enjoyed or did not seem to enjoy, and using that information to shape their next projects
- Supporting the free-to-play games market by enabling some developers to release free ad-supported games, including games that use tailored advertising

- Providing recommendations to players about other games and content that they may suit their tastes, which may require some 'profiling' of players
- Complying with laws and regulations noting that various laws in Australia and overseas may require that specific data be collected or kept.

How video game companies keep customer data safe

The video games industry is serious about collecting consumer data responsibly, collecting what is needed only, and keeping personal information safe. Video game companies are committed to providing customers with transparency, flexibility and control over their data and how it is used. Our industry understands that as technologies change, including within our own sector which has embraced the online world as quickly as any other, expectations and needs surrounding data and privacy also evolve.

The video games industry upholds privacy and considers the protection of its Australian customers' data as one of its key priorities, including through the following:

- Commitment to upholding Australian privacy regulations, with many game companies investing heavily in privacy expertise and measures, and when in doubt, generally taking an approach of erring on the side of caution
- Effective privacy notices displayed on screens telling players (and their parents or carers) what data is collected and how it is used, often in several places and in interactive ways, and utilising as simple and understandable English as possible
- Accessible and intuitive privacy settings that provide informed choice to players about what data to share and what impact it may have on the gaming experience
- Best practice account security measures such as two-factor authentication and technological protection measures (TPMs) that are robust and protect the integrity of the players' account data
- Widespread use of pseudonyms, 'gamer tags', avatars and device identifiers across the games sector in place of more sensitive personal information such as names and email addresses (in contrast to other digital sectors such as social media and networking platforms)
- Option to delete a player's personal data upon request, which is offered by some game companies, with warnings given around the effect it will have on the game.

IGEA's objectives for a future privacy framework

Video game companies, like other responsible sectors, regard the protection of the personal information of their customers as a critical regulatory and reputational priority. However, our sector is also observing an increasingly complex data regulatory environment in Australia and overseas, with game companies sometimes facing a patchwork of regional privacy frameworks, some of which are not always consistent, that they must comply with to access markets. While privacy laws are crucial, it is just as crucial that any future reforms are evidence-driven, targeted and pragmatic.

As privacy and data policies rise in prominence, there is a risk of a fragmentation of global privacy standards at a time when an increasingly digital global economy can ill afford additional barriers to trade. Like many digital and future-facing industries, video game companies rely on an efficient transfer of data between territories which is indispensable

for competitiveness within our sector. We believe that this can be achieved to enable game companies to operate globally while also providing effective and efficient protection of individuals' data. To support this, we believe that one of the goals of the Australian Government and other advanced economies should be to minimise the fragmentation of privacy regulation across global digital markets by pushing common standards and promoting the sharing of data between trusted countries and regions.

Looking home, we urge that as the Government embarks on this review of the Act, that it takes a principles-based and outcomes-focused approach to determining what aspects of existing regulation are fit-for-purpose and being pragmatic about what reforms are needed. Any future privacy framework should provide legal clarity and use technology-neutral language, while also avoiding a primary risk of privacy and other regulatory frameworks that they become unreasonably burdensome for businesses and counter another of the Government's key priorities of reducing red tape. One way to achieve this is a framework that articulates the Government's expectations and objectives for organisations with respect to data protection while providing them with the flexibility to determine how best to achieve those outcomes based on their unique products, resources and level of risks.

On that last point, we urge the Government to ensure that any future reform accommodates different risk levels in terms of data and uses of data, rather than taking a 'one-size-fits-all' approach to regulation. For example, transparency and consent requirements should vary depending on the sensitivities and risks surrounding the type of personal data collected. In our sector, game players would not expect the same level of notice, if any, surrounding how a game developer uses gameplay data to help improve the game as they would around how financial account information might be used for marketing, for instance. In the same way, the personal information collected by video game companies is in almost all cases a far lower risk than information collected by healthcare providers or mortgage brokers, for example, and we believe any future Act should be able to reflect this. It should also encourage organisations to collect low-risk information, such as gamer tags, rather than more identifiable information such as names and email addresses. Treating all data as the same would defeat any such incentive.

During the lifespan of the current Act, the global economy and how it collects and uses information has transformed almost beyond recognition. While it has not been without its challenges, we would argue that most of this change has been for the better. As ways of collecting and using data continue to transform in the future, the Government should consider how a flexible framework can enable organisations to provide privacy controls that can adapt along with the evolution of their goods and services. In our sector, this will enable game companies to tailor their privacy controls to their unique products and to encourage them to identify new and innovative ways to protect consumer privacy. Highly prescriptive requirements will only encourage risk-aversion in this space, which we believe will not provide the best outcomes for individuals.

Specific responses to Issues Paper questions

Objects of the Act

1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

We agree with the principle outlined in the objects of the Act that the protection of privacy of individuals needs to be balanced against the interests of entities when carrying out their functions and activities. It is an essential and necessary overarching principle that few stakeholders would disagree with, and we see no reason why it should not remain in the Act. If we were to suggest one addition to the list of objects, it would be that the Act should provide a flexible framework that recognises that disparate sectors use different kinds of data for different purposes and that data regulation should not treat every collection and use of data at a consistent level of risk.

On the point about balance, we note that the Issues Paper also raises questions around businesses that have arisen (since the Act was drafted) that deal with personal information as their primary business. Specifically, the AGD notes at page 15 that "the requirement to balance the protection of privacy with the interests of businesses can be difficult in the context of businesses whose core activity is acquiring and dealing in personal information". Video game companies are not businesses whose core activities are acquiring and dealing in personal information.

To the extent that there is a need for re-calibration of privacy expectations between individuals and businesses that deal primarily in personal information, this should be targeted and specific to that sector only. If following its consultation processes, the Government considers that the Act requires changes to be more fit-for-purpose with respect to businesses whose core activities are acquiring and dealing in personal information, any such changes should be focused on those businesses and uses of personal information. They should not be automatically be extended to all businesses.

Scope and application of the Privacy Act

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

We agree that there is currently some legal uncertainty around the current definition of 'personal information' in the Act, and especially on whether specific technical data collected from individuals falls inside or outside of the definition of personal information, as well as the precise meaning of 'reasonably identifiable'. We also note the discussion in the Issues Paper around the definition of personal information in the European Union (EU), which includes explicitly technical data where it can be used to indirectly identify an individual when combined with other data.

We do not support an overly-broad definition of personal information and believe that it may have unintended negative consequences. We particularly caution against adopting the EU's definition of personal data under the General Data Protection Regulation (GDPR) as "personal information relating to an identified or identifiable natural individual", which has not been without criticism for being broad, unclear and potentially limitless in its scope.

While we would welcome greater clarity on the kinds of circumstances surrounding technical information that may or may not constitute personal information, we do not support a definition that automatically considers all technical information to be personal information. We do not consider that treating all technical information that is collected and all uses of such technical information as the same is appropriate or necessarily beneficial to consumers. In particular, we urge caution around the ACCC's recommendation in the Digital Platforms Inquiry (DPI) that the definition of personal information in the Act should specifically capture technical data such as IP addresses, device identifiers, location data and any other online identifiers that may be used to identify an individual.

An overly broad definition of 'personal information' that covers a wide scope of technical information could be counter-productive and potentially undermine efforts to protect consumer privacy. For example, it could potentially remove any incentive for businesses to use (and innovate with) pseudonym-based privacy-protective measures, such as using screen names, avatars and device identifiers in the place of higher risk personal information such as real names and email addresses. This approach is often practised by video game companies to avoid collecting more sensitive information, and we do not believe this kind of information should typically be considered 'personal information'.

There are also some kinds of technical data collected by game companies that we believe should not be considered personal information, even where that data is linked to someone from whom personal information is collected. A basic example is all of the background data tracking where a player's character moves and travels within a game. Many game developers collect this kind of data, including to monitor for bugs in a game level. We doubt that it is the kind of data that the Government would expect to be considered personal information. If the Government moves to change the definition of 'personal information' in future to address technical information, we encourage it to be mindful of these kinds of low-risk data and to appropriately exclude them.

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

As outlined in the Issues Paper, APP 2 states that APP entities must give individuals the option of not identifying themselves, or the option to use a pseudonym, unless an exception applies. APP 11.3 also requires APP entities to either destroy or de-identify any personal information they hold when it is no longer required for any purpose, with de-identification meaning that the information will not be 'reasonably identifiable'. We note the point raised in the Issues Paper that some jurisdictions require personal information be anonymised rather than de-identified, which may make re-identification harder theoretically.

As discussed, we believe that any reform of the Act should be pragmatic and evidence-based. In considering whether to require APP entities to anonymise personal information rather than to de-identify it, the Government should consider whether there are genuine and practical reasons to do so, based on problems that it has observed. As the Issues Paper recognises, the anonymisation of personal information may be more difficult for data holders than de-identification, which can be a simple process involving the deletion of masking identifying information. A requirement to anonymise may impose a significant

regulatory burden for businesses, especially to those that already exercise responsible data management, without necessarily improving privacy outcomes for individuals.

Flexibility of the APPs in regulating and protecting privacy

6. Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

We agree with the Issues Paper that adaptability and clarity should be vital components of any Australian privacy framework. We encourage a principles-based framework that makes compliance straight-forward for sectors that exercise responsible data management practices and is flexible enough to deal with future unanticipated data practices, while still having the regulatory teeth to deal with problematic entities and sectors. As previously outlined, the kinds of data collected by game companies and how they use them are significantly lower risk than other sectors like healthcare and financial service providers. An effective and practical privacy framework should be nuanced enough to set different expectations as may be appropriate from sector to sector.

We are supportive of the current approach of the APPs that enable personal information to be collected, used and disclosed in certain circumstances where it is 'reasonably necessary' or directly related to one or more of the entity's functions or activities. At least in relation to the games sector, in most circumstances it will be reasonably clear when the personal information of game players meets this standard, while also providing flexibility to accommodate inevitable changes in how information is collected and used as digital technologies evolve.

It remains the responsibility of businesses to demonstrate that the way it uses personal information is 'reasonably necessary'. As the Issue Paper identifies, we believe that this approach "allows the APPs to be scalable to entities of various sizes and capabilities, and to be adapted to different acts and practices of those entities". In this way, while we recognise that improving clarity is generally a constructive goal when developing or reforming regulation, it should not come at the cost of creating a framework that is not flexible and adaptable to the increasingly diverse sectors and entities that collect and use personal information.

While the Issues Paper raises concern raised about the efficacy of the current mechanisms in the Act to respond to new challenges, we note that the Act already provides what on paper at least appear to be powerful mechanisms to 'futureproof' the scheme against unanticipated risks. Specifically, there is already a mechanism in the Act to bring currently exempt entities, acts and practices into the scope of the APPs through delegated legislation, as well as a power for the Information Commissioner to develop an APP Code or request that an entity such as an industry organisation (like IGEA) develop one for its sector. The trigger for exercising both powers is a 'public interest' test, which we believe is both an appropriate and reasonable threshold. Any reforms to expand the scope of these mechanisms should be necessary and evidence-driven.

We generally support the current framework of the Act as it is flexible and provides a reasonable regulatory burden for the vast majority of businesses that collect and use personal information while ensuring that additional obligations and responsibilities can

be imposed in a targeted approach to specific organisations and uses as may be appropriate in the circumstances.

Exemptions from the Privacy Act

7. Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?

8. Is the current threshold appropriately pitched or should the definition of small business be amended?

As a matter of principle, we support the overall intention of the small business exemption that seeks to avoid impactful compliance costs for small businesses that are considered to pose little or no privacy risk. If it is kept, we consider that the current definition of a 'small business', which revolves around a $3 million annual turnover cap and excludes higher risk entities such as businesses that trade in personal information, successfully achieves an appropriate balance between small business red tape reduction and protecting the privacy of individuals.

However, we are also supportive of the Government seeking an adequacy decision from the European Commission (EC) that Australia offers a level of data protection that is essentially equivalent to that which exists within the EU. We discuss this further later in this submission. We believe that there would be a significant benefit in such a decision by permitting more effective cross-border data transfers between Australia and the EU.

If it is the view of trade officials that the small business exemption remains a key issue preventing Australia from seeking adequacy with the EU, and that the Government does intend to seek adequacy, we acknowledge that the benefits to Australian small businesses (including Australian game development studios) of adequacy with the EU may outweigh the benefits of a small business exemption. Given that the vast majority of players of Australian-made game are based overseas, the Australian game development sector, including our smaller developers, are almost certainly already implementing data management practices that comply with both overseas privacy frameworks and the APPs.

Should reform be considered, we urge the Government to reduce the small business exemption only as far as is needed to enable adequacy with the EU, such as by analysing whether small businesses need only comply with some but not all of the APPs.

Notice of collection of personal information

20. Does notice help people to understand and manage their personal information?

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

Our industry continues to recognise the importance of ensuring that individuals are aware of what game companies want to do with their information and are equipped to make an informed decision about whether to share that information. We believe that notices are and should remain the most essential and effective tool of any privacy regime. Any future data regulation framework should continue to require regulated entities that collect personal information to take reasonable steps to provide adequate notice.

We support the requirement for 'reasonable' steps to be taken, rather than prescriptive rules, as it enables diverse entities to consider the most effective way in any given circumstance to provide information to their customer. For example, the highly interactive nature of our medium means that game companies should be incentivised to explore different notice formats to maximise engagement. Our preference would therefore be that the notice requirement should not mandate specific formats or procedures, which might be suitable for today's websites and mobile apps but may not be suitable for platforms in the future. Instead, notice requirements should be flexible enough to both enable and encourage creative approaches more appropriate for future generations of video game consoles, VR/AR/MR headsets, screens and other devices.

To provide a practical example, while it may be appropriate for some games or gaming platforms to display a single comprehensive privacy notice at initial set-up, as is common in other sectors, others may choose to provide 'layered' privacy notices at various points in a game where it may aid transparency (such as where a game has multiple lengthy play modes). There is no single correct way to provide notices, and entities should have the discretion to determine which approach works the best.

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

As the Issues Paper correctly notes, a privacy notice needs to strike a balance between providing an individual with information without overloading them. As individuals increasingly digitalise their lives and choose to participate with multiple apps, services and platforms each day, it could be argued that they are already very close to being overloaded, with statistics included in the Issues Paper suggesting that consumers are already experiencing fatigue with the amount of information already being provided to them. An effective privacy framework is not one that leads entities to provide as much information as possible to individuals but directs them to provide the level of information that will best facilitate transparency and an informed decision.

We support providing clarity to entities of the key matters for which they must take reasonable steps to notify individuals of, including, as currently outlined in the APPs, the identity and contact details of the entity, the facts and circumstances of collection, the purpose for which the personal information is being collected, and other parties to whom the entity normally discloses personal information to. We believe the current level of transparency is appropriate and expanding the scope of notices is likely to contribute further to 'fine-print fatigue'.

We agree with the point made in the Issues Paper that notice will only be effective in assisting an individual in making an informed decision where the notice is presented in a way that is easily understood by an individual. Indeed, many video game companies including some of the most popular games and consoles have taken significant effort and care to make important legal notices, including privacy policies and terms of services, available to players as concisely and in as plain English terms as possible.

However, we caution against imposing explicit and prescriptive rules that mandate a minimum level of simplicity in how information is presented or how a notice should be set out. There should be flexibility afforded in terms of how entities present information to individuals. It is not always easy and sometimes impossible to present information about the collection, use and disclosure of data, especially when businesses are also navigating complex regulatory requirements, in an objectively simple way. Attempting to do so may have negative consequences, including omitting or over-simplifying key information that would help consumers understand how their data is being used.

Finally, we would be supportive of work around a standardised framework of information that could be present in a notice, such as standard words or icons, which we believe may help ease the burden on both individuals and businesses. However, it is important that such a framework be voluntary and provided for guidance only, as standardised terms are unlikely to provide the best approach in every circumstance. Relevant entities must retain flexibility in how they draft their notices. Further, if work is commenced on a standardised framework of notice, we recommend that it be undertaken in consultation with international partners, such as the EC, as a common or globally-consistent framework would be most beneficial. Any work to develop a standardised framework would also benefit from a consultative process with industry.

Consent to collection and use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

We believe that the current privacy framework provides a practical approach for balancing transparency, informed consent and regulatory burden. The Act and the APPs generally provide clear parameters for entities in terms of how they collect and use personal information – ie. that they must only collect personal information that is reasonably necessary for, or directly related to, one or more of their functions or activities.

The current framework also recognises that consent may be express, implied or not always necessary. For example, relevant entities may collect personal information that is not sensitive without consent and may use or disclose that information (as well as sensitive information obtained with consent) without obtaining consent in a range of specific circumstances, including if it is for the primary purpose for which it was collected.

While it is reasonable that some uses of data may require consent, a future privacy framework should continue to recognise that most typical uses of data should not require consent. In particular, it is not controversial to assume that individuals in most circumstance accept that personal information that they provide to an entity should and will be used to support its business functions.

We disagree with the ACCC's view as articulated in recommendation 16(c) of the DPI that consent should be required for all collection, use or disclosure unless it is required contractually or under law or for an overriding public interest reason. We believe such a requirement would impose a heavy and unreasonable regulatory burden on many low risk, uncontroversial and widely accepted uses of data by businesses, and will almost certainly contribute to consent fatigue (discussed below).

In our sector, we would argue that most players not only accept but would have an expectation that the data they provide via their account and gameplay will be used to enhance their playing experience and to improve the game overall. Further requirements for consent beyond what are currently required in the APPs, at least in relation to our sector, may lead to frustration for our players.

Finally, any future privacy framework should provide flexibility in terms of recognising how consent is given. The highly interactive nature of video games means that game companies often use different options for soliciting engagement and obtaining consent from individuals to maximise their transparency and to reduce consent fatigue. For example, some games may ask players to swipe a notice with their finger, press a particular button on a controller, or perform some other interaction to show that they give consent. Game companies must retain discretion in how they obtain consent.

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

30. What requirements should be considered to manage 'consent fatigue' of individuals?

Consistent with our view above, we see little practical benefit in requiring individuals to separately consent to each purpose for which an entity collects, uses and discloses information. On the other hand, there is a risk that a mandatory de-bundling of consent (particularly if there is an increase in the kinds of collections, uses and disclosures for which consent is required) will make the consent process for individuals more onerous to the extent that in reality, it may only lead to more automated clicking and less reading.

As we have outlined in our submission, personal information is used in our sector for a wide range of primary and secondary purposes, with most if not all of these purposes not only uncontroversial but entirely consistent with what game players would expect. As audiences become increasingly mature digitally and expect more uses and features from the platforms they use, we do not believe that an approach that relies upon providing consent for each use is sustainable over the long term. There is unlikely to be a magic bullet for 'consent fatigue'. However, we believe that the current approach of the privacy framework, which recognises that there are many types of collection, use and disclosure of data for which informed consent can be implied or dealt with via notices, works well.

Finally, we do support work to develop standardised icons or phrases (as noted in recommendation 16(c) of the DPI report) that entities may voluntarily adopt. While it will not solve the problem of 'consent fatigue' alone, it may provide a useful tool under a future privacy framework, and we would be happy to contribute to this work.

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

While the idea of pro-privacy defaults may sound uncontroversial, in the video games sector, it may be problematic to implement and could have some unintended negative impacts. For example, most if not all game players would expect that in a standard multiplayer game that they as a minimum should be immediately able to play online, pick the best servers based on their location, be visible within the game, find and play with their friends, share content and celebrate their achievements with others. Pro-privacy

defaults could prevent these uncontroversial and expected features from automatically working, leading to needless frustration as players must find and manually change each setting.

The worst-case outcome if pro-privacy defaults are implemented is that some developers may decide to remove offline versions of games or features like 'hidden' mode entirely from their game to make gameplay more functional and friction-less while still being compliant. While we are not saying this is likely to occur, it could be an unintended effect, leaving individuals potentially worse off in terms of privacy outcomes.

Finally, we are concerned that pro-privacy defaults could curtail innovation in business models that are often for the benefit of consumers, which for our sector include the growth of 'free-to-play' games. 'Free-to-play' games, which have played a key role in ensuring video gaming is accessible to diverse socio-economic groups in Australia and abroad, rely on advertising (including targeted advertising) to exist. While some video game companies have chosen to make targeted advertising 'opt-in', we believe that requiring this as a default could disadvantageous Australian developers of 'free-to-play' games, which include some of Australia's most successful game development studios, compared to overseas developers. Given how competitive the global 'free-to-play' market is, the impact on the Australian game development industry could be significant.

33. Should specific requirements be introduced in relation to how entities seek consent from children?

We note the Issue Paper's advice that there is a separate process underway for progressing the DPI report's recommendation for an online privacy code of practice that will consider whether additional requirements for children's interaction with digital platforms are needed. We look forward to being a stakeholder as this work progresses.

A sensible privacy framework, including any future potential online privacy code of practice, should be flexible and scalable in how it addresses parental consent. We support a future framework that is both effective and user-friendly, and in particular, it should be able to accommodate pragmatic, realistic and innovative mechanisms for obtaining both express and implied parental consent. In particular, we support a 'sliding scale' approach that recognises that there are different types of data across varying risks levels and does not impose unreasonable barriers to a child's digital engagement. In this way, any future framework must strike a suitable balance between the privacy of children and not constraining the ability of game companies to create the online entertainment products and services enjoyed and used by Australian families.

In this submission, we have already argued that the definition of 'personal information' must not be impracticably broad. This is particularly important in relation to seeking consent from children because if an overly-broad definition of 'personal information' is adopted, virtually any online or gaming activity of children under 13 could potentially require parental consent, including, for instance, a pseudonymised screen name for an avatar in a children's game. As we have already covered, within the games sector developers and console manufacturers often collect screen and user names in lieu of more personal information such as a child's name or email address. Allowing a child to have an account or user name has other uses apart from gaming, including giving parents

and carers the ability to customise family control settings for that child while allowing them to still have an enriching experience playing games and collecting achievements.

Treating data like screen names and gamer tags as data that requires parental consent before it can be collected removes any privacy-related incentive for their use and may become counter-productive. We highlight the useful approach taken in the US, following a recent FTC amendment to the Children's Online Privacy Protection Act (COPPA) that states that a screen name or user name is a legitimate way to avoid the collection of personal information of children under 13.

Finally, we highlight a key potential risk that would arise with new specific requirements for seeking consent from children as opposed to adults. Specifically, it may lead to entities like video game companies needing to specifically asking the age of their players to ensure compliance, even though that information is not needed and they would otherwise not try to obtain that kind of personal information but for their legal obligations to do so. Such a situation could be counter-productive for any privacy framework.

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

As the Issues Paper notes, the APPs already include a requirement for entities to collect personal information 'by lawful and fair means'. In general terms, we urge caution around the use of subjective and potentially vague concepts like 'fairness' into a legal framework that is relied upon up by both individuals and entities to provide clarity. However, if the Government nevertheless decides to extend the expectation of fairness to the use and disclosure of information, as suggested in the Issues Paper, we recommend that the current framing be kept rather than a more prescriptive and inflexible requirement.

We also urge caution around the designation of 'no-go zones' around specific uses or disclosures of information, as flagged in the Issues Paper, as some uses of personal information that may seem unreasonable for some entities may be reasonable for others. For example, while it might not be fair to use data from a person's performance to adjust the difficulty of a recruiter's online testing platform dynamically, it would be fair to do so in a video game to give a player a more enjoyable and competitive experience.

Also, the public expectation's about reasonable uses of data, as well as ways in which entities may provide protections around these uses, are likely to evolve over time. Blacklisting these in a set of APPs may not only be an unreasonably inflexible approach, but it strips agency from consumers who might otherwise consent to such practices.

The Issues Paper suggests the possible use of 'proceed with caution zones' to supplement 'no-go zones'. A better approach may be the use of 'proceed with caution zones' to replace or as an alternative to 'no-go zones'. We consider that this would strike a better balance between providing guidance to businesses about fair and unfair uses of information, while also providing flexibility on a case-by-case basis and over time as community and regulatory expectations shift.

Control and security of personal information

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

We support reasonable and appropriate requirements under any future privacy regime for the protection of an individual's data. Specifically, we support the approach taken by APP 11, which sets out a flexible principles-based requirement for entities to take reasonable and appropriate measures to protect information that they hold. Video game companies treat the security of the information of their customers and players as one of their highest priorities and invest heavily into active and passive measures to prevent identity fraud and unauthorised disclosures of personal information. In particular, Technological Protection Measures (TPMs) such as persistent online authentication, while helping to prevent copyright infringement, also provides a strong layer of security over the player and their information to prevent external intrusion and identity fraud.

We note that the APPs do not currently provide for a strict requirement for entities to delete an individual's personal information when the individual is no longer interacting with the entity, an approach that we recommend should be kept under any future privacy framework. Among other reasons, it is not always easy to tell when an entity and an individual no longer have a relationship. Particularly with games, it is almost impossible to determine when a player ceases its relationship with a games company. For example, some players may also follow only a single game series from a developer, so there can be a strong relationship between a games company and a player even though the player only purchases a game from them every few years.

Further, video game players typically play a diverse range of games, and it is not uncommon for players to revisit a game that they have purchased even after not playing it for years. Reasons for re-connecting with a game include enjoyment or nostalgia, to introduce it to their children, or because new content has since been added. In these circumstances, a player would expect that their previous saved games and all the characters, levels, equipment and achievements that they had previously unlocked remain accessible. A requirement or expectation to delete a player's account data because a game has not been played for a few years would be entirely contrary to the expectations of most if not all game players and lead to significant reputational damage.

45. Should amendments be made to the Act to enhance: a. transparency to individuals about what personal information is being collected and used by entities? b. the ability for personal information to be kept up to date or corrected?

We believe that notice is and remains the primary tool that provides transparency to individuals about what personal information is being collected and how it is being used. There are also already obligations under the APPs for personal information to be kept up-to-date or corrected, and for an individual to have access to their own information.

If amendments are made to the Act, they should include providing clarity as to what information, and level of detail of that information, should be disclosed in response to a transparency request from an individual. Currently, this is not always clear to entities. In the case of video games, this could theoretically include every piece of data that is collected from a player's gameplay, which we consider would be unreasonable and sometimes impossible to provide. A future privacy framework could clarify expectations

around the kinds of data that should reasonably be included in a transparency request, and at the same time, outline the kinds of data that can be excluded.

Another trade-off for enhanced transparency not mentioned in the Issues Paper is the increased risk of identity fraud that may come from an unreasonably broad scope for individuals to access personal information. There is a concern that hackers and identity fraudsters are increasingly able to leverage one piece of information that they have obtained from an individual as verification to obtain more information via transparency obligations on other platforms, essentially allowing them to 'snow-ball' data about their victim. One solution would be for a future privacy framework to clarify that an entity can satisfy its transparency obligations by disclosing categories of information collected, rather than having to provide all the details of an individual's personal information.

Finally, alongside any privacy reforms, we also call for continued strong enforcement and penalties against those who steal or attempt to steal data held by entities.

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

We note that APP 11.3 already provides a requirement that an entity must "take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs". We believe that this is a practical and effective regulatory obligation that is also highly efficient because in practice, it encourages entities to implement systems and processes to destroy or de-identify personal information quickly and in bulk once it identifies that there is no longer need to hold it. Further, we note that APP 12 already provide relevant entities with an obligation to give individuals qualified access to their personal information upon request.

While we recognise that the DPI report has called for a 'right to erasure', we are not supportive of one being introduced in Australia. We believe it would be a significant and unreasonable regulatory burden, would be challenging and unsustainable to implement and provide limited public benefit beyond existing effective obligations that are already in place. In the video games environment, a broad 'right to erasure' could include every interaction that a player has had within a game over many years, none of which could be considered sensitive. If a player who makes a 'right to erasure' request has played multiplayer games, it could be impossible to erase that data without impacting the data of other players who would not want that game information removed.

Furthermore, the Issues Paper recognises that some countervailing public interest considerations have been identified against a 'right to erasure', or at least against a widely-framed right. For example, as AGD notes in the Issues Paper, it would not be in the public interest for personal information in online chat logs containing evidence of the grooming of children to be erased as it could prevent current and future law enforcement from investigating or prosecuting that activity. Even a 'right to erasure' that is subject to a law enforcement public interest exemption is problematic. If an individual exercises this right and there has been no approach from law enforcement, would the onus be on the entity to pre-emptively assess all of the individual's chat logs to identify potential

evidence of grooming? While many video game companies have measures in place to address such illegal behaviour within their communities, given that grooming activity can be subtle and obvious often only in hindsight, we submit that it would not be appropriate or even possible for an entity to bear this responsibility.

Another practical example of challenges with a 'right to erasure' is the impact it may have on the ability of game companies to retain and use personal information to address issues such as fraud, copyright infringement, cheating and online toxicity. Notwithstanding a consumer's desire to delete their account after being suspended from a video game for cheating, for instance, the publisher may need to retain some account information, such as IP identifiers, to help prevent that person from re-registering (which would violate the game's terms of service) and to strengthen anti-cheating measures.

Should the Government nevertheless decide to implement a 'right to erasure', we would urge it to follow the 'right to erasure' that exists in the EU provided under the GDPR as closely as possible to reduce the fragmentation of global privacy frameworks and by extension the regulatory burden on companies that operate in both regions.

Overseas data flows

48. What are the benefits and disadvantages of the current accountability approach to crossborder disclosures of personal information? a. Are APP8 and section 16C still appropriately framed?

As the Issues Paper highlights, free and open cross-border flow of information is critical to both Australia and the world's economic growth. It is particularly crucial in the video games industry, where our players' global spread and expectations for frictionless multiplayer gameplay means that their data must flow freely between borders and across servers all around the world. We, therefore, encourage the Government to progress a privacy framework that can preserve individuals' privacy without sacrificing the ability of Australian game developers to efficiently serve and expand their local and global player base, or the ability of game developers based overseas to support the two-thirds of Australians who love games.

For example, we support the existing exception from APP 8 that applies to personal information that is routed through servers outside of Australia. For the same reason, we also believe that any future privacy framework should provide clarity that APP 8 does not apply to entities that provide personal information to secure cloud service providers.

We also support the current broad exception to the application of APP 8 that applies where an entity reasonably believes that the recipient is subject to substantially similar laws to the AP. We support the Government prioritising work, as flagged in the Issues Paper, to publish a list of acceptable jurisdictions outside of Australia. This will provide much-needed clarity to industry. As a part of this work, we urge the Government to identify other opportunities to reduce regulatory duplication with key trading partners. Given that it is becoming increasingly difficult for successful Australian export-based businesses like game developers, as well as global businesses, to treat the personal information of Australians differently to consumers in other markets, efforts to reduce the fragmentation of global privacy standards may aid economic recovery and growth.

Finally, we note that Australia has formally agreed to, in principle, implement the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) framework but

has not yet embarked upon the implementation. We urge the Government to proceed with this implementation to provide businesses with a clearer framework how cross border data flows can lawfully take place.

49. Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?

In the absence of a viable alternative approach, the exception to extraterritorial application of the Act in relation to acts or practices required by applicable foreign law is still needed. The intention of this exception, as the Issues Paper notes, is to ensure that the Act does not compel entities to act in contravention of overseas laws even where those laws are not consistent with the APPs. The best way to address these kinds of privacy risks is through bilateral and multiple efforts between governments to improve consistency and reduce conflicts between regional privacy frameworks.

51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

While we hold no specific view on whether a domestic privacy certification scheme should be developed, we note that the Government has already decided to implement the CBPR system, which is intended to enhance cross-border information flows within the APEC region, so a domestic framework would need to provide further demonstratable benefits and avoid duplication. Should a domestic privacy certification scheme be implemented, we believe a voluntary scheme would be the most practical way forward, mirroring the voluntary nature of the CBPR system.

52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

Major video game companies, like many large organisations in other sectors, operate globally and hold data from customers based all around the world. Under the GDPR, personal data can only be transferred outside the EU to countries or organisations that provide an adequate level of privacy protection, with personal data able to be transferred to countries designated by the EC as having adequate protections, or to other countries on the condition that certain GDPR rights are enforceable.

Given the broad extra-territoriality application of the GDPR, and the fact that Australia has not been whitelisted by the EC, Australian businesses that collect personal information from EU residents or partner with overseas entities subject to the GDPR face a higher regulatory burden than many of their competitors. In our industry, this includes Australian game developers who almost certainly will have many players from the EU or have businesses relationships with publishers or other partners based in the EU.

Generally speaking, and subject to our specific views articulated in this submission, we believe that the best approach for achieving free, open and safe cross-border information flows is to ensure that any necessary and appropriate changes to Australian privacy laws are as consistent as possible to those of larger markets, such as the EU. This will help to harmonise the complex rules that both Australian exporters and overseas companies that collect data in Australia must comply with, and to avoid duplicative and inconsistent privacy obligations as they inevitably navigate multiple territories.

We are also generally supportive of the Government taking concrete steps towards obtaining EU adequacy. We urge the Government to investigate in more detail what changes would be needed to Australian privacy laws to achieve this and to consult on potential options in the subsequent Discussion Paper. While we acknowledge and do not disagree with the point made in the Issues Paper that overall less trade is undertaken with the EU than within the APEC region, when we talk about digital industries like video games, geography is less important, and trade markets are likely to be more diverse.

Finally, we note the argument made in the Issues Paper *against* seeking EU adequacy that requiring businesses to comply with different information-handling requirements under the Act, CBPR and GDPR could result in an overly-complex regulatory landscape. However, we contend that it is rather an argument *for* seeking EU adequacy. Further, we expect that the GDPR will become increasingly influential over the coming years and would not be surprised if more countries shift their own privacy standards towards it. While it is not perfect, the GDPR remains the most significant modern privacy framework.

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