IGEA

interactive games & entertainment association

Submission to the Australian Attorney-General's Department

Response to the Privacy Act Review Report

March 2023

We acknowledge the Traditional Custodians of Country throughout Australia and their continuing connection to the land and sea. We pay our respects to all Aboriginal and Torres Strait Islander peoples, their cultures and to their elders past, present and emerging.

Table of Contents

Introduction and overview

Introduction

The Interactive Games & Entertainment Association (IGEA) is pleased to respond to the Attorney-General's Department's (the Department) Privacy Act Review Report of December 2022 (the Report).

IGEA represents and advocates 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 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 has over a hundred members, from local studios to some of the largest technology companies in the world.

Our submission

IGEA has been a highly engaged and long-standing stakeholder of the Australian Government's ongoing review of the *Privacy Act 1988* (the Act). Among our various contributions, we lodged comprehensive submissions in response to the 2019 Issues Paper and the 2021 Discussion Paper.

Noting the significant volume (116) of proposals outlined in the Report and the relatively limited consultation window for comments against a report of this size and complexity, in this response we have limited our response to the proposals of most significance and anticipated impact on our members and our industry. These are outlined below. However, where we have not provided a response to a proposal, it should not necessarily be taken to represent support for that particular idea. Rather, we note the Government's advice that it is intended that many if not most of the proposals that proceed from the present consultation will be subject to further development and discussion before they are finalised and implemented. We look forward to the ability to contribute further to the modernisation of the Act at that stage.

Overarching comments

We thank the Department for the significant work that it has undertaken throughout the review of the Act and in developing the Report. Privacy law is undoubtedly a highly complex policy area with diverse stakeholder views. We also thank the Department for clearly reading and considering IGEA's two previous submission as a part of this review, alongside those of many other stakeholders. We are appreciative that many of the perspectives that we have previously shared with the Department have been considered, captured and specifically cited in the Report.

We overall note that in many parts of the Report, the Department has made thoughtful efforts to provide a balanced approach, considering not only the need to protect personal information but also the realities of our modern society and economy, the primacy of ensuring individuals have the ability to fully and effortless participate online, the practical expectations of these individuals and the regulatory burdens on organisations. We also acknowledge that despite the high volume of proposals, some others that were raised during the review will not be progressed following consultation and analysis. For example, we are relieved that the Overseas Data Flows proposals will not include any data localisation rules. While we do not

agree with all of the proposals in the Report, with some of our key concerns outlined below, we recognise the strong consultation and analysis that has been undertaken.

Finally, subject to our other views set out in this submission, we encourage the Australian Government that in progressing any proposals, interoperability with overseas data protection frameworks such as the European Union's (EU) General Data Protection Regulation (GDPR) be one of the guiding implementation principles to aid in friction-free compliance and enhanced accountability, and to facilitate cross-border expansion for the local Australian games industry.

Response to select proposals

Personal information

Proposal 4.1: Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

Proposal 4.2: Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

Proposal 4.4: 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

While it is clear that the Department has given the arguments around these proposals substantial consideration, we remain concerned that changing the word 'about' in the definition of personal information to 'relates to', with only a non-exhaustive list of information which may be personal information, is too broad and lacks clarity. We are concerned that the idea of providing guidance around what may *not* be personal information, even if there are caveats that it of course would depend on individual circumstances, has been rejected in the Report.

As we outlined in our previous submissions, we are particularly concerned about non-sensitive and non-personal in-game data that is collected on players such as their characters, items that they have collected or progression through a game, being considered personal information. While we do not think that the proposed expansion of the definition of 'personal information' is intended to cover such data, we are worried that there is significant ambiguity around this.

While we also recognise that the Report tries to clarify that personal information relating to an individual means that "the connection needs to be a real, not too tenuous or remote, connection which says something about a specific individual (not any individual)", we believe that there still remains too much subjectivity and we are not confident that the in-game data as provided in the examples above are out-of-scope of the definition of personal information.

We ask that any future reform centred around an expanded definition of 'personal information' such as through proposal 4.1 clarify that its scope would not extend to the kinds of information exemplified by in-game data connected on players such as characters, items that they have collected or progression through a game. Ideally this would be included in any future Act as a part of a list of the kinds of data that would not

normally be considered to be information that 'relates to' a person, but if this is not possible, then in some kind of explanatory commentary such as guidance by the OAIC.

We also ask that the preparation of the non-exhaustive list of information which may be personal information as outlined in proposal 4.2, as well as any non-exhaustive list of information which may *not* be personal information, and the non-exhaustive list of circumstances to which organisations should be expected to have regard in their assessment of 'reasonably identifiable' under proposal 4.4, be subject to stakeholder consultation.

Proposal 4.6: Extend the following protections of the Privacy Act to de-identified information:

(a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information:

(a) from misuse, interference and loss; and

(b) from unauthorised re-identification, access, modification or disclosure.

(b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.

Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.

Proposal 4.7: Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.

We share the concerns raised by many of our fellow stakeholders about the proposed expansion of parts of the Act to de-identified information, which we believe to be unnecessarily broad and without evidence that there is a policy gap that needs to be addressed through such a significant change. For example, it is not clear to us why the loss of information that is de-identified and is not re-identifiable (acknowledging of course it should generally be avoided as a matter of principle) should be covered by the Act in the same way as personal information. **We ask that proposal 4.6 not proceed until further analysis and stakeholder consultation has been undertaken.**

We also highlight our concerns regarding proposal 4.7 to introduce a criminal offence for malicious re-identification, which we believe presents a disproportionate response and one that not likely to effectively address issues with poor de-identification practices by organisations. **While we note that proposal 4.7 is only for the Australian Government to consult on the idea of a criminal office at this stage, we will take the present opportunity to state our opposition to such a change.**

Small business exemption

Proposal 6.1: Remove the small business exemption, but only after:

(a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act

(b) appropriate support is developed in consultation with small business

(c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and

(d) small businesses are in a position to comply with these obligations.

In our previous submissions, we highlighted our concerns with the removal of the small business exemption and we continue to hold this view. We are encouraged at least that the proposed removal of the exemption will be subject to a range of important steps to determine the costs for small business and a practical pathway to compliance for small businesses. With respect to proposal 6.1(a), we particularly highlight the significant new risks and regulatory uncertainty created for small businesses from the removal of the small business exemption in combination with the proposed new right of action.

We remain concerned about the risks of proposal 6.1 but agree with the steps that the Government proposes to undertake first prior to a final decision. We also recommend that the impact analysis outlined at (a) and assessment at (d) be transparently undertaken and subject to consultation with small business, similar to the steps for (b) and (c).

Privacy policies and collection notices

Proposal 10.3: Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

While we are supportive of the proposed plan to standardise templates and layouts for privacy policies and collection notices, we repeat our position from our previous submissions that any such templates be voluntary. While we acknowledge the aim of creating consistency across the economy, we note that there are circumstances where it may be more sensible to adopt bespoke policies and notices that are similar to but not necessarily identical to any particular standardised forms.

With video games, there may be specific games-related concepts, symbols or terminology that might be more clear to players than those used in standardised templates or layouts. Further, there may be circumstances where it is impossible to provide a specific Australian policy or notice – such as on a website, app, service or platform that is global in nature. In circumstances such as these, we believe policies and notices should be considered to comply with standardised templates and layouts as long as they are substantially similar in form.

We recommend that any standardised templates and layouts that are developed under proposal 10.3 be voluntary or be subject to a rule that compliance is achieved if a privacy policy or collection notice is substantially similar in nature to the standardised form.

11. Consent and privacy default settings

Proposal 11.2: The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons

could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

We are grateful that the Department has heard (and summarised in the report) our concerns that any general requirement that the strictest privacy settings be enabled by default would not be workable and may have adverse consequences for end-users. We warmly appreciate the Department's thoughtful consideration and look forward to continuing to work with our members to implement the best possible consent and privacy setting standards.

We are also supportive of the development of guidance on how online services should design consent requests. However, the development of such guidance should be subject to consultation and if any standardise consents are developed in the future, it is necessary that there be some flexibility in their usage.

The development of guidance as proposed at 11.2 should be subject to consultation, while any standardised consents should be voluntary or subject to a rule that compliance is achieved if the consent is substantially similar in nature to the standard developed.

12. Fair and reasonable personal information handling

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances

(b) the kind, sensitivity and amount of personal information being collected, used or disclosed

(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency

(d) the risk of unjustified adverse impact or harm

(e) whether the impact on privacy is proportionate to the benefit

(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and

(g) the objects of the Act.

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

(a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent

(b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and

(c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.

In our view, the proposed addition of a 'fair and reasonable' test under proposal 12.1 for the collect, use and disclosure of personal information is an unnecessary and significant change to the current privacy framework and we are concerned that there has not been sufficient analysis undertaken. In particular, we are concerned that there is so much ambiguity surrounding the meaning and interpretation of this wording for individuals, organisations and the OAIC, that the test is likely to be difficult or impossible to use from a practical perspective and may be counterproductive for advancing the Government's privacy objectives.

We are also concerned by proposal 12.3 that the new 'fair and reasonable' test would still be applied even where consent has been obtained. We believe that this is an unreasonable and onerous requirement that degrades the utility of consent - essentially the test would effectively override, rather than work in tandem with, any personal consent even when it meets the high proposed standard of being voluntary, informed, current, specific and unambiguous. We believe this proposed reform is therefore likely to introduce significant unnecessary regulatory risk and uncertainty for organisations without lifting privacy protections.

We also note that the report has not recommended the introduction of a 'legitimate interest' standard, despite the significant volume of submissions that called for its introduction and its effective application in other territories. From the submissions received and the analysis in the report, we know that the arguments for 'legitimate interest' are well understood by the Department so we will not repeat them here, but we urge the Department to re-consider them. In particular, the proposed right to object for individuals in global privacy frameworks like the GDPR benefits from being counterbalanced against an organisation's legitimate interests in processing personal information.

We do not think it would be unreasonable that if a 'fair and reasonable' test is progressed, that it is at least balanced by a 'legitimate interests' consideration. We note that the Canadian Government's Digital Charter Implementation Act, 2022 (Bill C-27) includes a 'legitimate interest' component by allowing organisations to process personal information, even without the consent or knowledge of individuals, if that processing is for a business activity in which the organisation has a legitimate interest that outweighs the potential adverse effect.

Further, from a practical perspective, it is not clear to us how organisations will be required to demonstrate and provide documentation to prove that it has applied a 'fair and reasonable' test each time it has collected, used or disclosed personal information (eg. the interaction between this proposal and the proposed organisational accountability requirements at chapter 15 of the Report).

Finally, the regulatory uncertainty on organisations resulting from the above issues would be significantly increased if an individual right to action were introduced alongside the 'fair and reasonable' test. At a minimum, if the Government introduces this broad and flexible requirement into the Act, this aspect of the Act should be enforced only by the OAIC to ensure

the coherent development of privacy jurisprudence in Australia and to avoid unpredictable or unintended outcomes.

We recommend that if a fair and reasonable test is introduced, that 'legitimate interests' for the collection, use and disclosure of the personal information be added to the matters to be taken into account and the relevant considerations for determining proportionality as outlined under proposal 12.2 when applying the test.

We also recommend that the nature of any consent given by an individual also be added to the same matters and considerations. We further recommend that if a 'fair and reasonable' test is introduced, that it be enforced only by the regulator and not through any proposed direct actions from individuals.

Finally, we ask the OAIC to publish comprehensive and regularly-updated guidance to clarify the specific record-keeping expectations of organisations for compliance with these proposals.

16. Children

Proposal 16.5: Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.

Overall, we appreciate the thoughtful and balanced analysis that the Department has undertaken in developing the proposals under this chapter. For example, we note the due consideration that was given to the question as to whether consent should generally be required by a parent or guardian on behalf of children under the age of 16 or whether there should be any specific exclusions to the use of children's data – but finding in both instances that the risks outweighed the benefits. We also support the report's conclusion that questions around default privacy settings and age assurance standards for children are complex and cannot be immediately answered.

We note the proposed introduction of a Children's Online Privacy Code under proposal 16.5. We acknowledge the importance of protecting children's data and the example set by the development of the Age Appropriate Design Code (AADC) by the Information Commissioner's Office (ICO) in the UK. While we do not necessarily disagree with the idea of a Children's Online Privacy Code in principle, we consider that there is a timely opportunity to monitor the implementation of the AADC, as well as assess other approaches undertaken in other jurisdiction, to determine the best approach for addressing the specific challenges of processing children's data.

However, should the proposal for a Code be progressed, we recommend that it not exceed the scope of the UK's AADC which, while not considered perfect by all stakeholders, is

generally regarded as balanced and flexible in how it approaches the need for protecting children's data as well as ensuring that children can continue to participate online.

Consideration also should be given to the fact that the UK AADC is a specific implementation of the GDPR by the UK and is administered by the UK's ICO. The AADC is not a legislative enactment. Should a Code be pursued here, we also recommend that the Government consider aligning code-making processes to the regulator-led process followed in the UK, together with comprehensive stakeholder consultation.

We recommend that the Australian Government first monitor and assess the implementation of the AADC before making a decision on whether to introduce a Children's Online Privacy Code. However, should a proposed Code be progressed, we recommend that it not exceed the UK's AADC.

18. Rights of the Individual

Proposal 18.3: Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.

(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.

In our previous submissions, we raised strong concerns around any proposed 'right to erasure'. We highlighted that 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. We further highlighted that in the video games environment, a broad 'right to erasure' could potentially 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.

We continue to raise these concerns in light of the Report, and they are even more acute given the proposed expansion of the definition of personal information. On the other hand, we acknowledge that the concerns we have raised around countervailing public interest considerations, such as law enforcement, have been heard and have shaped both the general exceptions as well as the option for the quarantine of certain information subject to an erasure request.

Should the Government continue to progress a proposed right to erasure following this consultation, there are changes that we would suggest. While many aspects of a proposed right to erasure are similar in design and scope to the precedent set by the GDPR, which will support the ability of global organisations to implement it expediently, there is one notable exception. What is missing from the proposed model for a right to erasure is greater specificity of the circumstances under which an organisation should action an erasure request, such as those set out under Article 17(1) of the GDPR. In particular, we note that the right to erasure of

the processing of data for direct marketing purposes under the GDPR through Article 21(1) is counterbalanced by a 'legitimate interest' consideration under Article 17(1)(c).

We also note that the Report provides very limited discourse on the practical challenges that have been experienced in jurisdictions overseas with a right to erasure. For example, organisations have faced uncertainties in implementing the GDPR's right to erasure rule, including around data retention periods, deletion timeframes and technical guidelines. Prior to designing any right to erasure, the Australian Government should closely investigate the learnings from other territories and develop guidelines to support practical compliance.

We do not support the proposed right to erasure, but if it is nevertheless progressed, we strongly recommend that the legislative framework include the circumstances and limits of the right such as those set out under Article 17(1) of the GDPR, including one for 'legitimate interests'.

We also recommend that the Government undertake a thorough analysis of the practical requirements of a right to erasure, including consultation, and provide implementation guidance, including around data retention periods, deletion timeframes and technical requirements.

20. Direct marketing, targeting and trading

Proposal 20.1: Amend the Act to introduce definitions for:

(a) Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.

(b) Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).

(c) Trading – capture the disclosure of personal information for a benefit, service or advantage.

Proposal 20.2: Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.

Proposal 20.3: Provide individuals with an unqualified right to opt-out of receiving targeted advertising.

Proposal 20.5: Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.

Proposal 20.6: Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Proposal 20.8: Amend the Act to introduce the following requirements:

(a) Targeting individuals should be fair and reasonable in the circumstances.

(b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.

Proposal 20.9: Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.

We have serious concerns with many the proposals in this section of the report.

First, we strongly object to the definition of 'targeting' which, as proposed under 20.1(b), would extend to capture the practices of "tailoring online services, content, information, advertisements or offers" – which is far wider in scope than advertising, which we would have reasonably expected 'targeting' to be limited to. While it is unclear to us whether this is the intention, in the context of games this expansive definition would arguably capture the use of 'targeting' to support players in each of the following ways:

- Providing recommendations for games that a person may like based on games that they have played in the past
- Providing recommendations about the broad categories of games that a person may be interested in, based on games that they have played in the past
- Providing information about other matters related to a game likely to be of interest to players, such as local events (like festivals) tied to the game or related media (like books based on the game)
- Providing guidance and advice to aid players based on their progression during a game
- Providing suggestions to players for them to change the difficulty level of a game based on their performance
- Suggesting game controls and player settings (including accessibility options) based on the controls and settings that the player has preferred for previous iterations of the game
- Giving localised game information, such as server maintenance periods, based on the location of players.

While we know that the requirement for the targeting of individuals to be "fair and reasonable in the circumstances" under proposal 20.8(a) might capture some of the above examples, we are concerned that this test is too vague and unclear in its meaning. It is also concerning and unproductive to us that some of the examples above may be considered 'targeted advertising' and therefore captured by the proposed unqualified right to opt out under proposal 20.3.

In addition, it is not clear to us what the policy rationale is for extending the meaning of 'targeting' under proposal 20.1(b) to the collection and use of de-identified and aggregated information (ie. related to groups of individuals). We do not consider that harm has been demonstrated that would justify a definition of 'targeting' that regulates information that is incapable of being tied to an identified person and we believe that this is beyond the scope of the purpose of the privacy framework, being to protect personal information.

We believe that the combination of these two proposals will not only have serious economic impacts on organisations, including the developers and publishers of video games, which we have previously highlighted in our prior submissions, but also poorer overall outcomes for

individual. These include fewer (ad-based) free-to-play video games, reduced content and less robust servers in ongoing games that rely on advertising revenue, less support available to existing players and higher levels of random or irrelevant advertising, degrading the user experience of players. The exceptionally broad definition of 'targeting' also carries considerable risk of unforeseeable and unintended consequences.

Finally, we are also concerned with the proposal to prohibit targeting to a child, with the exception for targeting that is in the child's best interests, under proposal 20.6. While such a rule might appear sensible in the abstract, there are serious questions about what a "child's best interests" means on a practical case-by-case basis. For example, even though the report provides an example of a product recommendation for a child as an example of something that would be in a "child's best interests", we do not consider that even that explicit example illustrated by the Department falls clearly within the scope of a plain interpretation of a "child's best interests". Based on this terminology, it is unclear whether even the most basic personalised experience for a child would be permissible.

We urge the Australian Government to carefully re-consider all of the proposals in chapter 20 as they are too far-reaching and impactful, and we do not think sufficient analysis has been undertaken around the risks to both organisations and individuals. We are particularly concerned around the broad definition of 'targeting', which should be restricted to targeted advertising, its unnecessary extension to the use of deidentified and unidentified information, and the problematic proposal to prohibit targeting to a child except where it is in the child's best interests.

Overseas data transfers

Proposal 23.2: Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).

As discussed in our introduction, we are appreciative that the Report recognises that data localisation measures do not necessarily increase data security and has not proposed any localisation mechanisms. We are also encouraged that the Government is open to seeking an adequacy decision between Australia and the EU, as we have recommended in our prior submissions, although we note from the Report that such a decision may not be a first priority. Also as mentioned in our introduction, we consider international interoperability between Australia and the data management frameworks of larger markets abroad as crucial.

We further welcome the Report's consideration of ways to facilitate cross-border data flows, which will be vital to realising the economic benefits of data-sharing while ensuring the security of Australians' personal information. However, we urge the Government to clarify that the existing transfer mechanisms under the Australian Privacy Principles (APPs) will remain available to APP entities to continue to transfer data across borders. We further urge the Government to ensure that any new certification scheme maximises interoperability with existing global standards and continues to allow the use of standard contract terms.

We recommend that the Australian Government continue to work on a path towards an adequacy decision between Australian and the EU.

More immediately, if proposal 23.2 (for a mechanism to prescribe countries as providing substantially similar protection to the APPs) proceeds, we recommend that the EU's GDPR be prescribed as such at the first opportunity.

However, we also recommend that the Government reconsider whether 'substantially similar' is the correct certification threshold for the prescription mechanism and whether 'adequate' or 'similar' may be sufficient to facilitate secure data flows without requiring those overseas privacy laws to mirror the individual aspects of Australia's Act (which might inadvertently have the impact of restricting cross-border data flows).

26. A direct right of action

Proposal 26.1: Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

We disagree with the proposal for a direct right of action, particularly under its proposed broad design framework. The existing and future privacy frameworks provide strong privacy rules and broad powers and mechanisms for the OAIC to enforce these rules and it is not clear to us what additional benefits a direct right of action would practically provide. It would be unlikely to motivate organisations to take any further data protection measures, given the clear rules and significant penalties that already exist. Rather, it would almost certainly simply lead to a significant number of frivolous or vexatious legal actions that will be burdensome on organisations and the Australian legal system. Further, any action that is taken should always be led by the OAIC, which could be aided by a strengthened public reporting and complaints mechanism.

Finally, we urge the Government to consider ways to mitigate the considerable regulatory risk and uncertainty that will be introduced should wide-ranging privacy reforms be implemented at the same time as introducing a private right of action. It is also important to note the disproportionately large impact that a direct right of action is likely to have on any small businesses who are also adjusting to the proposed removal of the small business exemption.

We ask that the Australian Government reconsider its proposal for a direct right of action. However, should it proceed, we ask that work be undertaken to limit the right to certain serious privacy breaches only, rather than being an open-ended right, and consider other mitigations to reduce regulatory risk and ensure that Australia's reformed privacy law develops in an orderly and coherent way.

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

Game Connect Asia Pacific: @GCAPConf

The Australian Game Developer Awards: @The_AGDAs