Submission to

Attorney-General's Department

Subject

Mandatory data breach notification

Date

4 March 2016

Table of Contents

1. Introduction

The Interactive Games and Entertainment Association (**IGEA**) welcomes the opportunity to respond to the proposed mandatory data breach notification scheme detailed in the Attorney-General Department's Discussion Paper entitled "Mandatory data breach notification" (the **Discussion Paper**), regarding the exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (the **Draft Bill**).

The Draft Bill follows the February 2015 inquiry of the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014 (the **Previous Draft Bill**) and the recommendations of the Australian Law Reform Commission's (**ALRC**) 2008 Report entitled "For Your Information: Australian Privacy Law and Practice" (the **ALRC Report**).

IGEA has reviewed the Draft Bill, Explanatory Memorandum and Regulatory Impact Statement related to the proposed data breach notification scheme that attempts to protect individual privacy without placing an unreasonable regulatory burden on business. In our submission, we have set out a brief description of IGEA and the interactive games industry in Australia, together with both a general submission on the introduction of the proposed mandatory data breach notification scheme and specific comments with respect to the Draft Bill.

By way of background, IGEA also refers to its earlier submissions:

a. Discussion Paper: Australian Privacy Breach Notification prepared for Commonwealth Attorney-General's Department, Business & Information Law Branch on 29 November 2012; and
b. Submission to the ALRC on Serious Invasions of Privacy on 15 November 2013.

2. Executive Summary

By way of executive summary, IGEA is of the view that:

1. The ongoing growth of the interactive games industry in Australia reinforces the degree to which IGEA's members continue to develop and introduce new and innovative business models to meet the increasing demands of Australian consumers in the digital economy. These new and innovative business models often rely on a number of factors, including the collection and use of user information.
2. The current legal environment with respect to serious data breach notifications through the application of the Australian Privacy Principles and voluntary notifications to the Office of the Australian Information Commissioner **(OAIC)** is sufficient and fit-for-purpose. Indeed, under this scheme, voluntary notifications of serious data breaches have increased by 150 per cent since 2009.
3. There is a need to clearly articulate the scope of the Draft Bill, including through the Commissioner's guidance material, to ensure that all organisations can unmistakably understand their obligations and comply with them.
4. The Draft Bill should include an unequivocal statement that the use of anonymised and aggregated data will not fall within its scope.
5. The mandatory data breach notification requirements should only apply to limited types of personal information that, due to its nature, carries a risk of harm if it were to be compromised.
6. The regime should not be applicable when a person has consented to the disclosure and use of their personal information by third parties.
7. The exceptions under the Draft Bill are insufficient, as they do not encompass situations such as where an organisation simply publishes information that is published by others.
8. There should be a mechanism for the Commissioner or Court to take into account a defence for circumstances where an entity, in the case of a serious data breach, has nevertheless implemented and used reasonable security measures.

3. About IGEA

IGEA is the industry association representing the business and public policy interests of Australian and New Zealand companies in the interactive games industry. IGEA's members publish, market, develop and/or distribute interactive games and entertainment content and related hardware. The following list represents IGEA's current members:

- 18point2
- Activision Blizzard
- All Interactive Distribution
- Big Ant Studios
- Disney Interactive Studios
- Electronic Arts
- Five Star Games
- Fiveight
- Gamewizz Digital Entertainment
- Mindscape Asia Pacific
- Namco Bandai Entertainment
- Google
- Microsoft
- Nintendo
- Sony Computer Entertainment
- Take 2 Interactive
- Total Interactive
- Ubisoft
- VR Distribution
- Well Placed Cactus
- ZeniMax Australia

4. Overview of the interactive games industry

The interactive games industry is the fastest growing entertainment industry globally[1] and is considered to be highly innovative in terms of its creative content and business models, many of which rely on the appropriate collection of user data. In 2014, the industry worldwide was estimated to be worth approximately US$77 billion, forecast to grow to US$96 billion by 2018.[2] Comparatively:[3]

- The film industry (including box office, home entertainment, sell-through, video on demand and rental, but excluding actual advertising and rental) was estimated to be worth US$107 billion (with a 4.4 percent compound annual growth rate)
- The music industry (incorporating physical distribution, digital distribution and live music) is estimated to account for US$52 billion by 2019, with a compound annual growth rate of 0.8 percent.

[1] Entertainment Software Association of Canada, "Levelling Up: Winning Strategies to Support Canada's Dynamic Video Game Industry", March 2014, page 3 (the **ESAC Submission**).
[2] DFC Intelligence, *Worldwide Video Game Forecast*, cited in Makuch, E, "Report: Xbox One and PS4 will sell 100 million units each by 2020" *Gamespot*, 12 February 2014, at http://www.gamespot.com/articles/report-xbox-one-and-ps4-will-sell-100-million-units-each-by-2020/1100-6417687/ (accessed 15 January 2016).
[3] PriceWaterhouseCoopers, *The Australian Entertainment and Media Outlook 2015-2019*, 14th Edition, 2015.

In 2015, Australia's interactive games industry reached AU$2.83 billion in retail sales (excluding revenue generated from interactive games development or exports), a 15 percent increase from its previous year.[4] That figure incorporated traditional retail sales of AU$1.243 billion and AU$1.589 billion in digital sales, increasing by 2 percent and 27 percent respectively. Mobile games, digital downloads and subscriptions also continued to grow significantly in 2015. The growth in digital came primarily from a 24 percent jump year-on-year in mobile game downloads and a 33 percent jump year-on-year in digital downloads. For further Australian market data in 2015, refer to **Appendix A** of this submission.

To demonstrate the levels of engagement with interactive games by the Australian population, IGEA's Digital Australia 2016 Report released on 28 July 2015 relevantly found that:[5]

- 98 percent of Australian homes with children under the age of 18 have a device for playing interactive games
- 68 percent of Australians play interactive games, with 78 percent of the game playing population aged 18 years or older
- Older Australians continue to make up the largest group of new players over the past four years. Australians aged 50 and over now make up 23 percent of the interactive game playing population - increasing their essential digital literacy for the digital economy
- The average age of those engaged in Australian interactive games has increased from 32 to 33 years old since 2013 and nearly half (47 percent) of this population is female
- As part of the normal media usage, the daily average time spent playing interactive games is 88 minutes by Australians
- 27 percent of players have tried making interactive games using software and 9 percent have studied or plan to study interactive games subjects

Interactive games are increasingly identified for their ability to serve other purposes in addition to simply entertainment. Researchers, educators, businesses and journalists have observed the importance of serious and related interactive games. Importantly, 24 percent of Australian adults have used interactive games at work for training purposes and 35 percent of parents say interactive games are embedded in their children's school curriculum. Games can also be beneficial for healthy

[4] Research based on The NPD Group Australia, Time period 2014 and 2015 calendar year, and Telsyte, cited at IGEA, "Australian video game industry strides towards $3 billion", *Media Release*, 2 March 2016, at http://www.igea.net/2016/03/australian-video-game-industry-strides-towards-3-billion/ (accessed 2 March 2016).
[5] IGEA, *Digital Australia Report 2016*, at http://www.igea.net/wp-content/uploads/2015/07/Digital-Australia-2016-DA16-Final.pdf (accessed 15 January 2016) (**DA16**).

ageing, with 89 percent of older Australians saying that playing interactive games improves thinking skills, 76 percent agreeing that interactive games increase mental stimulation, 79 percent finding that interactive games help improve coordination and dexterity, and 61 percent stating that interactive games help fight dementia.

A contemporary analysis of the Australian interactive games industry is provided in the IGEA's Digital Australia 2016 Report.[6] A historical overview of the interactive games industry in Australia can be found in a number of previous reports including Screen Australia's *Playing for Keeps*,[7] the Australian Centre for Moving Images' *History of Games Development in Australia,*[8] and the CCI's *Working in Australia's Digital Game Industry: Consolidation Report.*[9] [10]

5. General submission: mandatory data breach notification scheme

In 2008, the ALRC recommended introducing a mandatory data breach notification scheme that would apply to data breaches creating a 'real risk of serious harm' to affected individuals. A mandatory data breach notification was described as:[11]

> In essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information.

Following the February 2015 inquiry of the PJCIS into the Previous Draft Bill, the Australian Government agreed to introduce a mandatory data breach notification scheme and to undertake consultation of the draft legislation.

---

[6] A copy of the report at http://www.igea.net/2015/07/games-are-present-in-almost-all-australian-family-households/ [accessed 15 January 2016).

[7] Screen Australia, *Playing for Keeps: Enhancing Sustainability in Australia's interactive games industry*, 2011, at http://www.screenaustralia.gov.au/about_us/pub_gamesreport.aspx (accessed 15 January 2016) (**Screen Australia Report**).

[8] Knight, S and Brand, J, *History of Game Development in Australia*, ACMI, 2007.

[9] Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI) and Queensland University of Technology in partnership with the Games Developers‟ Association of Australia, *Working in Australia's Game Development Industry, A Consolidated Report,* May 2011, at http://www.cci.edu.au/sites/default/files/shaukka/Working%20in%20Australia%27s%20Digital%20Games%20Industry%20Consolidation%20Report%20May%202011.pdf (accessed 15 January 2016).

[10] Another resource is Department of Communications, Information Technology and the Arts, *From Cottages to Corporations: Building a Global Industry from Australian Creativity – Report on Access to Overseas Markets for Australia's Creative Digital Industry*, 2003.

[11] ALRC Report, paragraph 51.1.

The rationale of the proposed data breach notification scheme is as follows:[12]

> …to allow individuals whose personal information has been compromised in a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identity theft. Examples might include cancelling a credit card, or changing an online password.

IGEA notes that the present legal environment with respect to data breach notifications is as follows:

a. Australian Privacy Principle (**APP**) 11 in the *Privacy Act (Cth)* 1988 (the **Privacy Act**) requires government agencies and businesses that are subject to the Act to take reasonable steps to secure personal information they hold. It does not mandate notification following a data breach. At present, mandatory data breach notification is required only in the event of unauthorised access to eHealth information under the *My Health Records Act (Cth)* 2012; and
b. The OAIC administers a voluntary data breach notification scheme based on the ALRC recommendation (this includes a 'real risk of serious harm' notification threshold). The OAIC publishes guidelines on how entities subject to the Privacy Act should manage data breaches and how to assess the risk of harm to individuals following a data breach.

As stated in the Discussion Paper, pursuant to the latter:[13]

> The OAIC received 110 voluntary data breach notifications in 2014-15, up from 67 notifications in 2013-14 and 61 in 2012-13. The OAIC's enquiries into voluntary data breach notifications focus on the nature of a breach (such as the kind of personal information involved, and how the breach occurred) and the steps taken to contain the breach, mitigate harm to affected individuals, and improve security practices in the future.

In IGEA's view, the current legal environment with respect to data breach notifications is sufficient and fit-for-purpose.

IGEA and its members acknowledge the importance of ensuring the security of user information and the harmful consequences that follow any breach of such security measures, both to the individuals and the businesses involved.

[12] The Discussion Paper, page 2.
[13] Discussion Paper, page 2.

Data is essential to the digital economy and the ability of industry to innovate and create innovative product and/or service offerings that benefit Australia consumers. The growth of the interactive games industry in Australia, as outlined in our submission above, is testimony to the fact that IGEA's members continue to develop and introduce new and innovative business models to meet the emerging demands of Australian consumers in the digital economy. These new and innovative business models often rely on a number of factors, including the collection and use of user information.

However, in IGEA's view, as it has stated previously:

a. There are sufficient commercial incentives for organisations, such as reputation, to have high standards of data security and to voluntarily notify any data breach to the OAIC where appropriate; and
b. The voluntary OAIC guidelines outlined above are operating effectively and IGEA understands that more organisations are using them after voluntarily contacting the OAIC.[14]

User trust in an organisation's willingness and ability to keep personal information secure, particularly in the online global marketplace, is a critical and an essential asset for businesses in the digital economy. While a data security breach will obviously have a negative impact on the level of user trust, failing to notify of such a breach would completely undermine any remaining user trust in the organisation, and significantly impair (if not totally prohibit) the continued operation of that organisation. Therefore, the risk of damaging user trust, in addition to the consequent harm to brand and reputation, provides an appropriate market-derived mechanism for a flexible and efficient approach to data breach notification.

The voluntary OAIC guidelines provide an effective standard for organisations to measure and guide their approach to data breach notification. By strictly complying with these guidelines, organisations are able to protect their brand reputation and user trust when dealing with instances of data security breach. Further, under the existing powers of the Australian Information Commissioner (the **Commissioner**) within the Privacy Act, the Commissioner can audit private sector organisations. This possibility creates further incentives for organisations to proactively report data breaches to the Commissioner and to affected individuals.

[14] Regulation Impact Statement for the Draft Bill, pages 2-3.

IGEA is therefore firmly of the opinion that Australia should continue to maintain a voluntary approach to data breach notification in order to ensure responsible and innovative data collection and processing that stimulates new innovative products and services for the benefit of Australian consumers. This view is also in line with the OECD Privacy Guidelines,[15] which recommend Australia's compliance with the Guidelines, but they are not mandatory. Furthermore, the proposed legislation should only be introduced if there is sufficient evidence that substantiates a significant failure of the current voluntary approach to data breach notification. In our view, this is yet to be demonstrated. IGEA again notes that voluntary notifications to the OAIC have indeed increased dramatically over time by 150 per cent from 2009-10 to 2014-15. Furthermore, as the Australian Government's Regulation Impact Statement concedes, there is no real evidence in Australia of the underreporting of significant data breaches to the OAIC.[16]

6. The Draft Bill

The Draft Bill amends the Privacy Act with a new Part IIIC that, in essence:

a. Defines when a "serious data breach" occurs, namely, when it relates to a "real risk of serious harm";
b. Outlines when and in what form notification of a serious data breach to the Commissioner is required.

With regard to the specifics of the Draft Bill, IGEA makes the following comments.

Scope and definitions

Under the Draft Bill a serious data breach will occur if:

- Personal information;
- Credit reporting information;
- Credit eligibility information; or
- Tax file information.

[15] OECD Privacy Framework 2013.
[16] Regulation Impact Statement for the Draft Bill, page 13.

that an entity holds about one or more individuals is subject to unauthorized access or disclosure, or is lost and puts any individual to whom the information relates at "real risk of serious harm". The Draft Bill then sets out a number of "relevant matters" which entities could take into account in determining the "real risk of serious harm" threshold. Harm is defined broadly in section 26WF.

IGEA welcomes the commitment that the Commissioner will issue guidance material regarding the assessment of whether a "serious data breach" has occurred, particularly given the very encompassing definition of "harm", which includes psychological and emotional harm, and also the need for harm to be "real, that is, not remote".[17] However, given that the notification threshold in the Draft Bill varies from analogous schemes in other overseas jurisdictions, there is a need to clearly articulate the Australian requirements for the benefit of those to whom the requirements apply. Furthermore, any variations to the existing OAIC guidelines should be clearly articulated and communicated to entities that are subject to the scheme, otherwise there is the great potential for confusion and misunderstanding.

IGEA also believes that there should be a clear and unequivocal statement that the use of anonymised and aggregated data will not fall within the scope of the Draft Bill. Increasingly, organisations routinely collect anonymised and aggregated data as a business necessity in order to better understand their users and provide more targeted products and services for their benefit. For example, interactive games developers and publishers may collect information on a user's gameplay time, frequency and spending habits. In relation to educational and learning games, this may include users' learning and development milestones, and areas of improvement and proficiency. The use of such information in an anonymised and aggregated manner is intended to further improve and enhance consumers' experiences and levels of engagement.

The mandatory data breach notification requirements should also only apply to limited types of personal information that, due to its nature, carries a risk of harm if it were to be compromised. If this approach is utilised, the "real risk of serious harm" test in the determination of a serious data breach can then only be applied to a narrower but more appropriate pool of personal information. We would expect the notification requirements would still apply to personal information relating to financials, passwords and the like, since this may cause harm if compromised

IGEA would also like to note that the system does not consider the situation where disclosure of information is necessary to fulfil contractual obligations. This is particularly relevant to third-party

[17] Paragraph 8 of the Explanatory Memorandum, page 3.

subscription management services and gateway payments where there is a need for disclosure of information in order to offer the service or product. While this could be addressed by including a specific exclusion to cover such circumstances, IGEA recommends that the regime simply not be applicable when a person has consented to the disclosure and use of their personal information by third parties (including third-party subscription management and gateway payment services). This would confirm that this type of disclosure would not constitute "unauthorised access or disclosure", and therefore prevent the application of the data breach notification requirements.

Notification requirements

Under the Draft Bill, entities are required to notify the Commissioner and affected individuals if there are reasonable grounds to believe that a serious data breach has occurred. Failure to notify would result in non-compliance with the scheme. An entity has 30 days to assess whether notification is required and, if so, is required to take such steps, as are reasonable in the circumstances, to notify each individual. Where the Commissioner believes that there has been a serious data breach and that the entity has not notified of the breach, the Commissioner can direct the entity to undertake notification.

IGEA is concerned that, given the broad application of the Draft Bill to a large number of entities, including many small businesses, there needs to be further clarification as to what is considered "reasonable" notification.

For example, IGEA is aware of a number of small, innovative games developers in Australia with only two or three employees that have developed unexpectedly popular interactive games and experience a sudden increase in popularity, resulting in their annual turnover increasing above $3 million for that year. Given that these smaller companies may have hundreds of thousands of customers all over the world, the requirement that they individually notify each customer would be resource intensive and onerous. Moreover, while a 30-day turnaround for investigation and notification of serious data breaches may be considered reasonable for larger and more resource capable organisations, this may not be the case for much smaller companies.

Additionally, while we note that Section 26WC states "if it is not practicable for an entity to notify the contents of the statement to each of the individuals to whom the relevant information relates" then they may publish a copy of the statement on their website, we think it would also be helpful if

the Commissioner's guidance material specifically refers to the sorts of circumstances where this is envisaged.

Exceptions

The exceptions to the data breach notification requirements, both under the Scope and Definition and the Exceptions sections, include:

- Entities already exempt from the operation of the Privacy Act (including intelligence agencies and small businesses);
- Law enforcement bodies, where notification would be likely to prejudice law enforcement activities;
- Other entities that are not subject to the operation of the Privacy Act;
- Where compliance with the Privacy Act was inconsistent with other Commonwealth laws, such as under the *My Health Records Act 2012* (Cth);
- Where an entity, if after becoming aware that there are reasonable grounds to believe a serious data breach has occurred, subsequently carries out a reasonable assessment within 30 days and finds that there are in fact not reasonable grounds to believe a serious data breach occurred; and
- Where an entity applies and is granted an exemption if notification would be contrary to the public interest.

In IGEA's view these exceptions are insufficient.

For instance, the exceptions do not encompass the situation where an organisation simply publishes information that is published by others. Section 230 of the *Communications Decency Act* in the United States provides that providers and users of interactive computer services that publish information provided by others are immune from liability. In our view, such an exception would go some way to ensure that the Draft Bill does not inhibit the development or provision of online products or services to Australian consumers, particularly where those products and/or services may enhance the sharing of ideas and information. Therefore, IGEA would support an exception that applies to internet intermediaries and organisations that host material uploaded or otherwise provided by third parties.

Enforcement

Failure to comply with notification obligations falls under the Privacy Act's existing framework for enforcement and civil penalties. In certain circumstances, the Commissioner can apply to the Federal Court to impose a civil penalty.

IGEA welcomes the graduated approach to sanctions such as less severe penalties encompassing personal apologies. However, IGEA notes that the scheme does not specifically take into account instances of cyber-crime, which is an inevitable risk in the online environment. No security measures are 100 per cent effective, despite an organisation's best intentions and attempts to protect their users' privacy. Therefore, IGEA suggests that there should be a mechanism for the Commissioner or Court to take into account a defence for circumstances where an entity has implemented and used reasonable security measures.

7. Conclusion

In conclusion, IGEA and its members do not support the Draft Bill. In our view, the current voluntary regime applicable to serious data breach notifications is flexible, sufficient and appropriate to support both innovation in the digital economy and the protection of individuals from such breaches.

APPENDIX A – AUSTRALIAN MARKET DATA

The IGEA's commissioned research from NPD Group Australia showed that, in 2015:[18]

- Video games industry growth has been led by the console sector, with current generation (Microsoft Xbox One, Nintendo Wii U and Sony PlayStation 4) consoles increasing in sales volume compared to 2014 by 9 per cent
- Console software was the best performing category, experiencing 13 per cent growth in revenue over last year
- Strong platform sales had a flow on effect to other areas, as the console accessories market grew in value by 12.2 per cent over 2014 data
- Over half (59 per cent) of game units sold were classified as G, PG or M

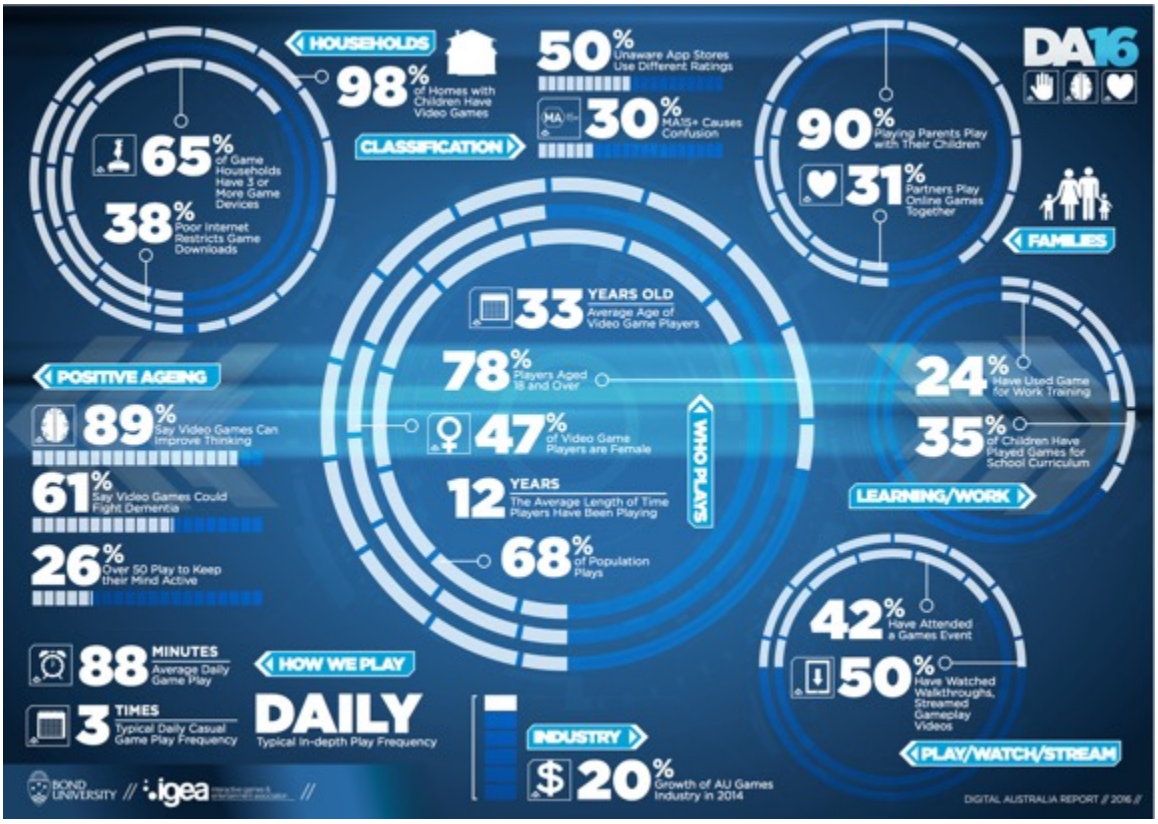
Further industry key highlights by independent research firm Telsyte evidenced:[19]

- Digital is now greater than half of the total games market, accounting for 56 per cent of sales
- Digital extras, which include season passes, map packs and game expansions, boomed with 53 per cent growth in 2015
- Games publishers are increasingly adopting the in-game purchase business model which is greatly contributing to the growth of digital extras market
- Physical products in the games market remain important with consumers indicating a preference for physical copies when purchasing as a gift or as a collectable or where there might be technical limitations such as download speeds or data caps

[18] Research based on The NPD Group Australia, Time period 2014 and 2015 calendar year, and Telsyte, cited at IGEA, "Australian video game industry strides towards $3 billion", *Media Release*, 2 March 2016, at http://www.igea.net/2016/03/australian-video-game-industry-strides-towards-3-billion/ (accessed 2 March 2016).
[19] Ibid.


igea
interactive games & entertainment association
AUSTRALIA
TOTAL INDUSTRY VALUE
UP 15%
$2.832 BILLION
TRADITIONAL RETAIL
NPD DATA*
UP 2%
$1.243 BILLION
DIGITAL SALES
TELSYTE DIGITAL MARKET MONITOR**
UP 27%
$1.589 BILLION
CONSOLE SOFTWARE
UP 13%
$579 MILLION
CURRENT GEN HARDWARE
UP 9% UNITS
CONSOLE ACCESSORIES
UP 12%
$166 MILLION
MOBILE
UP 24%
$870 MILLION
DIGITAL DOWNLOADS
UP 33%
$603 MILLION
XBOX LIVE
PlayStation. Plus
Nintendo eShop
SUBSCRIPTIONS
UP 29%
$116 MILLION
npd
Telsyte
IGEA commissioned research from:
*The NPD Group Australia
Time period January 5 2015 – January 6 2016
**Telsyte – IGEA Digital Market Monitor, Q1 – Q4 2015

Key Findings: Digital Australia 2016



// Key Findings //

Games Households
98% of homes with children have computer games.
65% of game households have three or more game devices.
38% choose not to download games due to data limits.

Who Plays
68% of Australians play video games.
47% of video game players are female.
33 years old is the average age of video game players.
78% of players are aged 18 years or older.
39% of those aged 65 and over play video games.
12 years is the average length of time adult players have been playing.

How We Play
88 Minutes is the average daily total of all game play.
10 Minutes, three times a day is typical for casual game play.
1 Hour, daily is typical for in-depth game play.

Why We Play
To keep the mind active is the main reason older adults play.
To have fun is the primary reason PC and console players play.
To pass time is the main reason mobile players play.

Families and Play
90% of playing parents play with their children.
31% play online games with partners.
57% of adults are "Always present" for purchase of games for children.
66% are familiar with parental controls on game systems.

Classification and Media Concerns
30% indicate MA 15+ causes most confusion.
28% indicate M causes most confusion.
50% are unaware that app stores have different rating systems.
41% say ratings have "a lot of influence" on games purchased for children.

Game Play Culture
50% have watched walkthroughs or streamed gameplay videos.
42% have attended a games event.

Games and Benefits
89% say video games can improve thinking skills - health.
79% say video games can improve coordination and dexterity - health.
76% say video games increase mental stimulation - positive ageing.
61% say video games could figth dementia - positive ageing.

Learning and Work
24% have used video games at work for training.
35% say their children have used video games for school curriculum.

Game Business
20% is the amount of growth in the Australian game industry in 2014.

Methodology
Digital Australia 2016 (DA16) is a study of 1274 Australian households and 3398 individuals of all ages in those households. Participants were drawn randomly from the Nielsen Your Voice Panel in May 2015; research was designed and conducted at Bond University. The margin of error is ±2.7%.