Arpita Verma, Gino Dal Pont** and Jane Nielsen****

PERSONAL INFORMATION COLLECTION VIA VIDEO GAMES: AUSTRALIAN PRIVACY LAW IMPLICATIONS

Abstract

Video game companies collect vast amounts of personal information about gamers, including — but not limited to — age, gender, facial scans, credit card details, licence numbers and location data. There is a significant gap in research regarding the true scope of this information collection and associated privacy law implications. This is particularly evident from the Australian standpoint, with no existing studies addressing this issue. This article endeavours to fill this gap by pursuing two research aims: (1) using thematic analysis to explore the extent of personal information collected by video game companies; and (2) investigating how such collection is regulated under the *Privacy Act 1988* (Cth), and the extent to which those companies comply with that Act when collecting personal information.

The analysis reveals that the gaming industry collects the personal information of Australian gamers in a way that has the potential to negatively affect gamers. It also evinces a lack of adherence to certain requirements of Australian privacy law with respect to such collection.

I Introduction

The video game industry is one of the fastest-growing industries in the world, with over 3.4 billion users ('gamers') and USD187.7 billion in revenue earned in 2024.[1] Video game companies ('gaming companies') use personal information to develop and improve games; it represents a commercially valuable asset offering a unique opportunity to obtain detailed, timely and multifaceted insights

* Adjunct Researcher, Faculty of Law, University of Tasmania, Hobart, Australia.

** Professor and Interim Dean and Head of Law, Faculty of Law, University of Tasmania, Hobart, Australia.

*** Professor, Centre for Law and Genetics, Faculty of Law, University of Tasmania, Hobart, Australia.

1 Newzoo, *Global Games Market* (Report, August 2024) 4. See also Michiel Buijsman, 'The Global Games Market Will Generate $187.7 Billion in 2024', *Newzoo* (Web Page, 13 August 2024).

into gamer behaviour and opinions.[2] In turn, this provides a source of business intelligence and guides decision-making concerning games, including the opportunity to launch new updates and adjustments to game design based on gamers' needs, preferences, likes and dislikes.[3]

Personal information collected by gaming companies includes seemingly innocuous information actively provided by gamers,[4] such as age group and the average time gamers play a game. It extends to other more 'sensitive' personal information, such as government issued identifications (including driver's licence numbers)[5] and biometric information (for instance, facial scans,[6] and information about gamer's voice and background sounds when playing).[7] Much of this information can be classified as 'personal information' under relevant privacy laws and its unmitigated collection can encroach into gamers' private lives. In Australia, the collection of personal information is regulated by the *Privacy Act 1988* (Cth) ('*Federal Privacy Act*').

There is limited scholarship examining the actual extent of the personal information collected by gaming companies,[8] despite extensive literature on how to collect,

2 Magy Seif El-Nasr, Anders Drachen and Alessandro Canossa, *Game Analytics: Maximizing the Value of Player Data* (Springer-Verlag, 2013) 63, 153.

3 Rowan Tulloch and Craig Johnson, 'Games and Data Capture Culture: Play in the Era of Accelerated Neoliberalism' (2022) 44(5) *Media, Culture and Society* 922, 923.

4 See, e.g., 'Privacy Policy', *Rockstar Games* (Web Page, November 2024) <https://www.rockstargames.com/privacy>.

5 'Online Privacy Policy', *Blizzard Entertainment* (Web Page, 27 June 2025) <https://www.blizzard.com/en-gb/legal/a4380ee5-5c8d-4e3b-83b7-ea26d01a9918/blizzard-entertainment-online-privacy-policy> [1] ('Blizzard Entertainment Privacy Policy').

6 'Roblox Facial Animation Privacy Notice', *Roblox Support* (Web Page, 12 July 2023) <https://en.help.roblox.com/hc/en-us/articles/8064749848980-Roblox-Facial-Animation-Privacy-Notice>.

7 'Microsoft Privacy Statement', *Microsoft* (Web Page, May 2025) <https://www.microsoft.com/en-gb/privacyoobe/oobeprivacystatementwhite#mainlocationservicesmotionsensingmodule>. Microsoft collects '[y]our voice data, sometimes referred to as "voice clips", such as search queries, commands, or dictation you speak, which may include background sounds'.

8 Some seminal works in this regard include: Jacob Leon Kröger et al, 'Surveilling the Gamers: Privacy Impacts of the Video Game Industry' (2023) 44 *Entertainment Computing* 1; Joe Newman, Joseph Jerome and Christopher Hazard, 'Press Start to Track Privacy and the New Questions Posed by Modern Video Game Technology' (2014) 42 *American Intellectual Property Law Association Quarterly Journal* 527 1; N Cameron Russell, Joel R Reidenberg and Sumyung Moon, 'Privacy in Gaming' (2019) 29(1) *Fordham Intellectual Property, Media and Entertainment Law Journal* 61.

use and analyse gamer data in game development.[9] There is accordingly a notable gap in research addressing the privacy issues arising from gaming companies' data-gathering practices.[10] That this issue has received little, if any, attention from researchers in Australia justifies an analysis of these information-gathering practices, and their privacy law implications, from an Australian legal perspective.

The article is structured as follows. It begins in Part II by outlining the definition of 'personal information' under the *Federal Privacy Act* and briefly examines the prospective changes to the current definition of personal information arising from the Attorney-General's Review of the *Federal Privacy Act*. Part III presents the methodology employed to examine the personal information collected by gaming companies (the thematic analysis method). The results of this analysis, presented in Part IV, reveal a diverse array of personal information collected by gaming companies. Part V considers how gaming companies combine the information they collect, and its privacy implications. This demonstrates that the full extent of personal information collected by gaming companies goes beyond what is apparent from privacy policies, in turn suggesting that gamers are unlikely to understand the full gamut of information collected. Building upon these findings, Part VI evaluates the privacy concerns arising from the personal information being collected and examines whether the information collection aligns with the standards established by the *Federal Privacy Act*. The article concludes with further analysis of the privacy implications derived from the article's key findings and presents ideas for future work.

II Personal Information Under Australian Privacy Law

Informational privacy in Australia is protected by a combination of Commonwealth (the *Federal Privacy Act*),[11] state[12] and territory acts.[13] The organisations bound

9 See generally Yanhui Su, Per Backlund and Henrik Engström, 'Comprehensive Review and Classification of Game Analytics' (2021) 15(2) *Service Oriented Computing and Applications* 141.

10 See, e.g.: Jennifer R Whitson and Bart Simon, 'Game Studies Meets Surveillance Studies at the Edge of Digital Culture: An Introduction to a Special Issue on Surveillance, Games and Play' (2014) 12(3) *Surveillance and Society* 309; Elena Petrovskaya and David Zendle, 'Predatory Monetisation? A Categorisation of Unfair, Misleading and Aggressive Monetisation Techniques in Digital Games from the Player Perspective' (2022) 181(4) *Journal of Business Ethics* 1065.

11 *Privacy Act 1988* (Cth) ('*Federal Privacy Act*').

12 See, e.g.: *Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW); *Information Privacy Act 2009* (Qld); *Privacy and Data Protection Act 2014* (Vic); *Privacy and Responsible Information Sharing Act 2024* (WA); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT). Cf South Australia does not have a dedicated privacy act, but instead relies on a Cabinet Administrative Instruction: Department of the Premier and Cabinet (SA), *Information Privacy Principles Instructions* (PC012, 4 May 2020).

13 *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT).

by the *Federal Privacy Act* comprise government agencies at the Commonwealth level,[14] the Australian Capital Territory ('ACT') Government,[15] as well as organisations including trusts, body corporates or partnerships with an annual turnover exceeding AUD3 million.[16] This includes most video game companies, many of which earn more than AUD3 million and otherwise do not fall under any exclusions listed in the Act.[17] The state and territory laws regulate information privacy in respective state or territory public sector bodies.

The *Federal Privacy Act* is the primary legislative instrument regulating the protection of the collection, use and disclosure (together 'handling') of individuals' personal information in Australia.[18] The 13 Australian Privacy Principles (APPs), which form the main regulatory mechanism under the Act, prescribe requirements as to how organisations may collect, use, disclose and store 'personal' and 'sensitive' information (concepts that are explored below).[19] The APPs can broadly be divided into transparency obligations — APP 1 and APP 5 — and consent requirements — APP 3 (solicited collection), APP 4 (un-solicited collection), APP 6 (use and disclosure) and APP 7 (direct marketing). In this article, we are concerned only with the kinds of personal information collected by gaming companies. The focus is accordingly on APP 3, which governs how information can be 'solicited' by an organisation.

A *Personal Information*

The definition of 'personal information' is central to the *Federal Privacy Act* as it determines whether an entity handling personal information is subject to the various obligations set forth by the Act.[20]

---

14 *Federal Privacy Act* (n 11) ss 7, 7A, 8.

15 *Information Privacy Act 2014* (ACT) (n 13) s 23; Government of the Australian Capital Territory, 'Privacy', *Chief Minister, Treasury and Economic Development Directorate* (Web Page, 9 November 2020) <https://www.cmtedd.act.gov.au/legal/privacy>. Note that ACT's Information Privacy Act 2014 fully adoptes the commonwealth privacy principles.

16 *Federal Privacy Act* (n 11) ss 6, 6C, 6D.

17 The definition of organisation under the *Federal Privacy Act* is listed in s 6C and excludes organisations that are 'a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory'.

18 *Federal Privacy Act* (n 11) s 2A; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (No 108, 30 May 2008) 162 [2.3] ('*For Your Information*').

19 *Federal Privacy Act* (n 11) sch 1.

20 Ibid s 6(1) (definition of 'personal information'); *For your Information* (n 18) 293 [6.2].

The *Federal Privacy Act* provides the following definition:

> ***Personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.[21]

Information is 'about' an individual when there is a link between the person and that information.[22] The Office of the Australian Information Commissioner ('OAIC') gives two examples of when this is possible:

(1) where an individual is the sole or joint subject matter of information; or (2) where information conveys something about an individual. [23]

Not every single piece of information collected and processed by an organisation will necessarily be 'about' an identified, or a reasonably identifiable, individual. Instead, it might only be about the identified or reasonably identified individual when linked or combined with other information.[24]

In this regard, the OAIC suggests that contextual factors should be used to determine whether information is about an identified, or reasonably identifiable individual, including: (1) the nature and amount of information collected by an entity; (2) the context of release (that is, who will have access to the information); and (3) other information that is available to the entity.[25]

In practice, this makes it necessary to consider the totality of information collected by gaming companies to determine the true extent of personal information collected.[26] This includes personal information collected by drawing inferences about individuals, thus creating new factual personal information about an individual's past or present life.[27] For instance, in the *7-Eleven* determination,[28] it was held that a face-print — an encrypted algorithmic representation of an individual's

[21] *Federal Privacy Act* (n 11) s 6(1) (definition of 'personal information').

[22] Office of the Australian Information Commissioner, *What is Personal Information?* (Report 5 May 2017) 6 ('*What is Personal Information?*').

[23] Ibid 6–7.

[24] Office of the Australian Information Commissioner, *Publication of MBS/PBS Data — Commissioner Initiated Investigation Report* (Report, 23 March 2018) 4.

[25] *What is Personal Information?* (n 22).

[26] *Privacy Commissioner v Telstra Corporation Ltd* [2017] 249 FCR 24, 35–6 [61]–[63].

[27] Office of the Australian Information Commissioner, *Guide to Data Analytics and the Australian Privacy Principles* (Report, 21 March 2018) 9 [1.5].

[28] *Commissioner Initiated Investigation into 7-Eleven Stores Pty Ltd (Privacy)* [2021] AICmr 50 ('*7-Eleven*').

face, from which the age and gender of customers could be inferred[29] — is personal information.[30]

Notably, the definition of 'personal information' is intentionally broad, so as to address shifts in information-handling practices over time.[31] It also has breadth in being applicable across different contexts, sectors, activities and technologies.[32] Hence, a wide variety of information can fall under the umbrella of 'personal information', creating potential ambiguity over precisely what constitutes 'personal information' in a given context.

The scope for ambiguity intensified following the important decision in *Telstra Corporation Ltd v Privacy Commissioner*,[33] in which the issue was whether an Internet Protocol address ('IP address') is personal information. The plaintiff (Mr Grubb) desired access to certain telecommunications metadata, including his IP address, claiming that it was his personal information.[34]

The Administrative Appeals Tribunal ('AAT') found that the IP address was not personal information about Mr Grubb but information about how Telstra provided a service to him.[35] An appeal to the Full Court of the Federal Court failed.[36] While the Federal Court did not examine whether there are any circumstances in which an IP address could be personal information, the Court wrote that the facts, context and circumstances of the case must be considered in deciding whether the information is personal.[37] The lack of substantial analysis in definitely determining what is personal information has led to further uncertainty over whether technical information (such as IP addresses, location information and device identifiers) can be considered to be personal information.[38]

To assuage uncertainty, the OAIC has issued guidance that organisations can refer to in order to understand if information is personal information. The OAIC guidance does this by including examples of information that can be considered personal

---

29 Ibid [6].

30 Ibid [1].

31 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53 ('Explanatory Memorandum to Privacy Bill').

32 Ibid.

33 *Telstra Corporation Ltd v Privacy Commissioner* (2015) 254 IR 83.

34 Ibid 98 [39]–[40].

35 Ibid 121 [113].

36 *Privacy Commissioner v Telstra Corporation Ltd* (n 26).

37 Ibid 36 [63].

38 Normann Witzleb and Julian Wagner, 'When is Personal Data About or Relating to an Individual a Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws' (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 293, 325.

information, such as name, address, date of birth, phone number, location information, IP address, facial recognition biometrics and medical records.[39]

Recently, a need to amend the definition of 'personal information' has been noted by government agencies, arguably because the current iteration under the *Federal Privacy Act* fails to adequately protect individuals' personal information in the digital age.[40] The *Privacy Act Review Report 2022* ('*PAR Report 2022'*) published by the Australian Attorney-General's Department recommended an amendment to the definition of 'personal information', suggesting that the definition be modified to replace the term 'about' with the phrase 'related to'.[41] This would address some of the uncertainty regarding the scope of personal information in two key ways.

First, it would widen the scope of personal information to include technical information (such as IP addresses, location information and device identifiers), which currently may fall outside the definition of information 'about' an individual.[42] This is important because technical information can raise privacy concerns as it 'uniquely identifies' a user, a device or a set of behaviours recorded on the device.[43] Thus, technical information becomes a proxy identifier for the individual who uses the device.[44] This, in turn, facilitates gaming companies singling out individuals by distinguishing them from others; monitoring them across various services, devices and databases to create an individual profile of their interests and preferences.[45] This significantly increases the chance of an individual being reasonably identifiable.[46] The Privacy Commissioner, in the determinations of *7-Eleven*[47] and

39 'Office of the Australian Information Commissioner, 'Chapter B: Key Concepts' (Web Page, 24 March 2023) 9 [B.31] <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts> ('*Chapter B: Key Concepts*').

40 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, 26 July 2019) 461 ('DPI Report').

41 Attorney-General's Department (Cth), *Privacy Act Review Report 2022* (Final Report, 16 February 2023) 25–7 [4.2], recommendation 4.1 ('*PAR Report 2022*').

42 Ibid 25 [4.2.1].

43 Office of the Victorian Information Commissioner, 'Biometrics and Privacy' (Report, July 2019) <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/> 11; Christopher Parsons, 'Privacy Tech-Know Blog: Uniquely You: The Identifiers on Our Phones That Are Used to Track Us', *Office of the Privacy Commissioner of Canada* (Blog, 8 December 2016) <https://www.priv.gc.ca/en/blog/20161208/>.

44 Finn Myrstad and Ingvar Tjøstheim, *Out of Control. How Consumers Are Exploited by the Online Advertising Industry* (Final Report, Norwegian Consumer Council, 14 January 2020) 25 ('*Norwegian Consumer Council*').

45 *Commissioner Initiated Investigation into Clearview AI Inc (Privacy)* [2021] AICmr 54, 20 [96] ('*Clearview*').

46 *PAR Report 2022* (n 41) 31.

47 *7-Eleven* (n 28) 6 [28].

Clearview,[48] considered that individuals can be identifiable when they are distinguished from others in the group. It follows that technical information that permits an individual to be distinguished from others can constitute 'personal information'. Therefore, clarifying — that such technical information is 'personal information' for the purposes of privacy legislation will serve to reflect the Privacy Commissioner's practice.

Second, the proposed amendment would make explicit that inferred information (that is, new identifying information gathered by linking or combining other information together) is considered personal information.[49] While personal information is broad enough to include inferred information, given the privacy risk associated with the collection of inferred information, it is crucial for the *Federal Privacy Act* to clearly address its application to such information.

In its response to the *PAR Report 2022*, the Government agreed in principle with the need for this amendment.[50] At the time of writing, though, if and when these reforms will be implemented remains unclear. In the interim, a lack of certainty regarding the true scope of what constitutes 'personal information' remains. This may cause organisations to exercise insufficient caution when collecting personal information, possibly leading to privacy harm.

B *Sensitive Information*

A subset of personal information is 'sensitive' information, which is defined under s 6(1) of the *Federal Privacy Act* by exhaustively listing types of information that comprise sensitive information, including health information, biometric information, and genetic information that is not otherwise health information.[51] Sensitive information is accorded a higher level of privacy protection because of the likely greater harm caused by its misuse.[52] For instance, biometric information, such as facial scans of an individual, [53] can be used to commit identity theft.[54]

48 *Clearview* (n 45) 20 [96].

49 *PAR Report 2022* (n 41) 30.

50 Australian Government, *Government Response to the Privacy Act Review* (Report, 28 September 2023) 5 ('*Government Response*').

51 *Federal Privacy Act* (n 11) s 6(1) (definition of 'sensitive information').

52 Office of the Australian Information Commissioner, 'Chapter B: Key Concepts' (n 39) 29 [B.144].

53 *Clearview* (n 45).

54 Jessica Bahr, 'The "Hi Mum" Scam Cost Australians Millions. Now, It's Had an Upgrade', *SBS News* (online, 14 January 2024) <https://www.sbs.com.au/news/article/the-hi-mum-scam-cost-australians-millions-now-its-had-an-upgrade/53v2hycvi>.

III Methodology

The following Part describes how the gaming companies were selected, what documents were chosen to glean data about gaming companies' collection of personal information, and the use of thematic analysis to analyse data.

A *Game Companies Screening*

Three inclusion criteria were employed to select gaming companies for analysis:

1 *Representative Size*

The largest gaming companies, by revenue, were chosen because the gaming industry is highly oligopolistic, and larger companies earn a major portion of global gaming revenue.[55] Thus, it can be assumed that most gamers will at some point play games produced by these companies. Additionaly, these companies will not fall within the statutory AUD3 million threshold, which forms exception to small business enterprises under the Federal Privacy Act.

2 *Presence in Australia*

Since the focus of the research is Australian law, companies with no presence in Australia or that do not cater to Australian gamers were excluded from the study.

3 *Involvement in the Gaming Business, Including Involvement in the Process of Publishing Games*

Companies that are not involved in the gaming business but earn money incidentally from games were excluded.[56]

After considering this inclusion criteria, a representative sample of major players were chosen for this study — Sony, Microsoft, Nintendo, Activision Blizzard, Electronic Arts, Take-Two Interactive, WarnerMedia, Roblox, Bandai Namco Entertainment and Playtika — all of which exceed the AUD3 million revenue threshold.

B *Data Collection Techniques*

Once the companies were identified, it was necessary to gather data about their information-handling practices. Privacy policies were the main documents analysed

---

55 Frédéric Le Roy, Frank Robert and Rhizlane Hamouti, 'Vertical vs Horizontal Coopetition and the Market Performance of Product Innovation: An Empirical Study of the Video Game Industry' (2022) 112 (April) *Technovation* 1, 9–11; Michiel Buijsman (n 1).

56 This will include, for example, companies like Apple and Google.

for this purpose, given that, under the *Federal Privacy Act*, these are the documents required to notify gamers about the entity's information-gathering practices.[57]

Multiple privacy policies relevant to Australian gamers were identified and examined. Locating the privacy policy of each company was not straightforward. First, companies that have a global presence, many subsidiary companies or develop multiple games raise the prospect of multiple privacy policies within one parent company. Second, while most gaming companies (8 out of 10) have privacy policies listed on their websites, not all do.[58] In some cases (such as Sony and WarnerMedia), only one such policy is listed. However, some of the games that are available to the Australian market have a discrete privacy policy for Australian gamers, such as for differing age groups, types of console or genre of game. For instance, Sony's main PlayStation privacy policy is listed on the PlayStation website. However, Sony Pictures also releases games for mobile devices (such as *My Hero Academia* and *Zombieland*), which are governed under Sony Pictures Ltd and Sony Pictures International Ltd, respectively, not Sony PlayStation. Additionally, Sony has a separate children's privacy policy. Each privacy policy differs but applies to Australian gamers. Third, gaming companies frequently update their privacy policies, making it essential to establish a final cut-off date for their collection for the current study. This cut-off date is set as 13 November 2024.

Table 1, below, details the total number of privacy policies included in this study (36), how they were located.

Table 1: Privacy Policies Relevant to the Study

Company	Number of privacy Policies Studied	How Were Privacy Policies Found?
Activision	4	Company's website
Sony	4	Company's website and by installing, opening, and downloading games
WarnerMedia	2	Received directly from WarnerMedia
Nintendo	5	Company's website and by installing, opening, and downloading games
Microsoft	2	Company's website
Electronic Arts	1	Company's website
Take-Two Interactive	2	Received directly from Take-Two Interactive
Roblox	1	Company's website
Bandai Namco Entertainment	8	Company's website and by installing, opening, and downloading games
Playtika	7	Company's website
Total	**36**	

57 *Federal Privacy Act* (n 11) sch 1 pt 1 cl 1: APP 1.

58 See Table 1.

C *Data Analysis*

Privacy policies contain detailed information on every information-handling activity of an organisation, from collection to use and disclosure of personal information. The authors needed to extract from the policies the kinds of information obtained by the companies and proffer a broad overview, necessarily by virtue of the detail between policies. The main method employed to undertake this reductive exercise was thematic analysis. Thematic analysis is particularly useful in reducing large volumes of text (such as interview transcripts) without undue cost, making it an appropriate method to analyse privacy policies.[59] Thematic analysis is a method of 'identifying and interpreting patterns of meaning across qualitative data'.[60] It can be used to identify and analyse recurring patterns (themes) from the data and to draw valid inferences from those patterns.[61] Thus, beyond reducing the text, it also aids in generating a thematic perspective of the data collected.

The analysis conducted adapted Braun and Clarke's six-step process (see Figure 1).[62]

Figure 1: Braun and Clarke's Six-Step to Thematic Analysis

Step 1: To begin the thematic analysis, all 36 privacy policies were read until sufficient familiarity with the data was obtained. While the policies were initially read with no specific focus, the authors were able to discern some initial themes. For instance, they noticed that, in general, companies collected the name, age and gender of individuals at the very least.

Step 2: The next phase required the generation of codes. Coding helps to systematically break down the data (that is, privacy policies) into meaningful chunks of information related to the research question.[63] Codes were generated manually using open coding; that meant first separating the information about the 'collection' aspect of information-handling activities from other aspects of information-handling

59 Christian Herzog, Christian Handke and Erik Hitters, 'Analyzing Talk and Text II: Thematic Analysis' in Hilde Van den Bulck et al (eds), *The Palgrave Handbook of Methods for Media Policy Research* (Springer, 2019) 385, 385–6.

60 Victoria Clarke and Virginia Braun, 'Thematic Analysis' in Alex C Michalos (ed), *Encyclopedia of Quality of Life and Well-Being Research* (Springer, 2014) 6626, 6627.

61 Moira Maguire and Brid Delahunt, 'Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars' (2017) 9(3) *All Ireland Journal of Higher Education* 3351, 3353.

62 Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2006) 3(2) *Qualitative Research In Psychology* 77, 87.

63 Ibid 87.

activities, such as use and disclosure.[64] What followed was the generation of codes using an inductive approach; that is, instead of relying on a pre-existing theory to develop codes, codes were developed from the data itself.[65] Generating codes was an iterative process; the initial codes were developed and adjusted, if necessary. Initially, the process produced close to 100 codes (see Table 2 for an example of how initial codes were developed using a small segment of data).

Steps 3–5: Codes developed were then clustered together into broader themes based on similarities. This helped to identify overarching patterns in the data. Similar to coding, creating themes was an iterative process that continued until all codes were incorporated into themes. All themes were coherent and separate from each other, and further refinement was unnecessary. A total of ten broad themes relative to categories of personal information collected by gaming companies were generated.

Table 2: Thematic Analysis: Example of How Themes Were Extracted

<table>
<tr><th>Extract from the privacy policy of Call of Duty League:</th><th>Extracted code</th><th>Theme</th><th>Description of the theme</th></tr>
<tr><td rowspan="3">‘When you visit or use our Properties we collect, process and/or combine Information about your use of those Properties, such as websites you visited before and after you used a Property, browser type and language, IP address, hardware and software information, third party account information (for example, information associated with your Activision account), purchase histories, and Social Media data.’[66]</td><td>• Websites visited,
• Browser type.
• Browser language.
• IP address.
• Hardware and software information.
• Third-party account information.</td><td>Technical Information</td><td>Technical information encompasses device identifiers, technical device information, and device event information.</td></tr>
<tr><td>• Purchase histories</td><td>Transactional Information</td><td>This refers to the personal information collected from consumers’ online transactions.</td></tr>
<tr><td>• Social Media data</td><td>Social Information</td><td>Social information refers to information about how gamers interact with each other.</td></tr>
</table>

64 Del Siegle, ‘Open, In Vivo, Axial, and Selective Coding’, *University of Connecticut* (Blog Post, 19 June 2023) <https://researchbasics.education.uconn.edu/open-in-vivo-axial-and-selective-coding/>.

65 Virginia Braun and Victoria Clarke, *Thematic Analysis: A Practical Guide* (Sage, 2021).

66 The Call of Duty League, ‘Privacy Policy’, *The Call of Duty League, LLC* (20 December 2022) <https://callofdutyleague.com/en-us/privacy> (emphasis added) (‘Call of Duty League Privacy Policy’).

IV Summary of Findings: Kinds of Personal Information Collected

The 10 broad themes created as a result of thematic analysis were: (1) contact information; (2) demographic information; (3) transactional information; (4) location information; (5) technical information; (6) biometric information; (7) social information; (8) behavioural information; (9) in-game behavioural information; and (10) personal records.

Notably, not all 10 kinds of information noted above were collected by all companies, as revealed in Table 3 below. Indeed, only four of the companies collect all 10 types of personal information.

Table 3: Categories of Personal Information Collected by Gaming Companies

Companies	Contact information	Demographic information	Transactional information	Location information	Technical information	Biometric information	Social information	Behavioural information	In-game behavioural information	Personal records	Number of data types collected
Activision	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**10**
Sony	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**10**
WarnerMedia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	**9**
Nintendo	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	**8**
Microsoft	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	**9**
Electronic Arts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	**9**
Take-Two Interactive	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	**8**
Roblox	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**10**
Bandai Namco	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**10**
Playtika	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	**8**
Total	**10**	**10**	**10**	**10**	**10**	**7**	**10**	**10**	**10**	**4**	

The individual categories of personal information collected by gaming companies as developed using the thematic analysis are explored below.

A *Contact Information*

Contact information refers to personal information used by gaming companies to contact people, whether directly or indirectly, via the gaming context. Each of the gaming companies studied collected contact information, including name, email address, physical address, telephone number, username and gamertag (a unique gamer identifier).

B *Demographic Information*

Gaming companies collect a variety of demographic information, which can include profile information (including profile photos, likes and languages spoken), education, employment, and sensitive demographic information including race and political affiliations.[67]

C *Transactional Information*

Transactional information refers to personal information collected from consumers' online transactions. It is collected whenever gamers purchase games through gaming companies[68] and includes information such as debit/credit card details (including debit card number, security code and expiry date) and payment instrument details (such as PayPal account details).[69] This information is considered to be personal information.[70]

Transactional information can encompass purchase histories,[71] active subscriptions and missed payments.[72] Information of this nature is used to predict a gamer's revenue potential by forecasting how likely they are to buy a particular product if offered.[73] There is limited research on how transactional information gathered through online gaming is used to determine a gamer's creditworthiness in a context outside gaming, for example, where purchase history is analysed to determine a gamer's general creditworthiness. Nevertheless, one notable example is Pokémon Go, a game that allows the game developer, Niantic, to track players' locations and the distance they travel. This information is reportedly shared by Niantic with insurance companies, which in turn offer discounts or incentives to gamers who meet specific travel or movement goals while playing the games — thus implying

---

67 Warner Media, 'Warner Bros. Discovery Privacy Policy', *Warner Bros Discovery* (Web Page, 27 March 2024) <https://www.wbdprivacy.com/policycenter/b2c/en-us/>.

68 This might change, if the purchase is made via third party. See 'Privacy Policy', *King Inc* (Web Page, 14 September 2023) <https://www.king.com/privacyPolicy>: 'When you purchase items in our mobile apps through the App Store, on Facebook or on Google Play, we do not collect or store any payment information from you'.

69 See, e.g., Sony Interactive Entertainment Europe Limited, 'Privacy Policy', *PlayStation* (Web Page, January 2024) <https://www.playstation.com/en-au/legal/privacy-policy/> ('PlayStation').

70 *Flight Centre Travel Group* (Privacy) [2020] AICmr 57 (25 November 2020) [28] (Commissioner Falk): 'credit card details and/or passport information … constituted their personal information.'

71 See, e.g., Rockstar Games (n 4).

72 See, e.g., Warner Media (n 67).

73 See generally Paolo Burelli, 'Predicting Customer Lifetime Value in Free-to-Play Games' in Günter Wallner (ed), *Data Analytics Applications in Gaming and Entertainment* (Auerbach Publications, 2019) 79, 79.

that player is in good health.[74] Should transactional information be used or shared with insurers who then make credit-related decisions about gamers without properly informing those gamers, it would potentially violate the credit reporting provisions of the *Federal Privacy Act*.[75]

D *Location Information*

Location information refers to information about the location of a gaming device. This may be either imprecise or precise. Imprecise information includes: (1) current and recent locations;[76] (2) geolocation data inferred from IP address, and access points near the gaming device;[77] (3) information about nearby cell towers; and (4) city or postcode level information inferred from a gamer account. Precise information includes: (1) geolocation based on mobile device location;[78] and (2) location gathered using the Global Navigation Satellite System ('GNSS'), e.g., Global Positioning System ('GPS').

Location information can also be collected from third parties, such as analytics and advertising partners. It is important to gaming companies, as it allows the matching of players in a particular location to prevent 'lag' (delay) in the operation of a game. Location information is equally significant when it comes to location-based games, such as augmented reality games, which require gamers to carry a GPS-capable device near specific locations to progress in the game and earn rewards. An example is Pokémon Go, which requires gamers to visit locations to capture and train virtual creatures, called Pokémon.

Unfortunately, location information allows its collectors to infer more information about individuals, including sensitive information. For example, in the United States, a local newspaper disclosed the sexual orientation of a priest without his consent, after obtaining location information indicating he frequented gay bars.[79] In the PAR Report 2022, the Australian Attorney-General's Department recommended that precise geolocation tracking data (an individual's precise geolocation tracked over time) should be included in the category of sensitive information.[80] The

---

74 Sumitomo Life, 'Sumitomo Life to Become Japan's Very First Financial Institution to Partner with "Pokémon GO"'!', *Sumitomo Life* (News Release, 22 March 2021) <https://www.sumitomolife.co.jp/english/newsrelease/pdf/nr20210322.pdf>.

75 *Federal Privacy Act* (n 11) s 6N defines credit information. It is regulated separately under Part IIIA of the Act.

76 PlayStation (n 69).

77 'Privacy and Cookie Policy', *Electronic Arts Inc* (Web Page, 23 August 2024) <https://www.ea.com/legal/privacy-and-cookie-policy>.

78 'Microsoft Privacy Statement' (n 7).

79 Michelle Boorstein, Marisa Iati and Annys Shin, 'Top US Catholic Church Official Resigns after Cellphone Data Used to Track Him on Grindr and to Gay Bars', *Washington Post* (Web Page, 20 July 2021) <https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/>.

80 *PAR Report 2022* (n 41) 45.

Australian Government has agreed in principle with this recommendation.[81] Thus, despite location information not being explicitly considered personal information under the *Federal Privacy Act*, the Australian Government has already accepted that such information should be protected as sensitive information. This applies in cases where the information collected classifies as personal information. At the time of writing, it is unclear when (or, indeed, whether) this response will be implemented.

E *Technical Information*

Technical information encompasses three key elements — device identifiers, technical device information and device event information — elaborated further in Table 4:

Table 4: Technical Information Collected by Gaming Companies

Device Identifiers
Gaming companies collect many device identifiers in respect of users, including: • International Mobile Equipment Identifiers (IMEI). • Apple Identifiers for Advertising (IDFA), Android Advertising IDs (AAIDs), Media Access Control (MAC) address and IP address.[82]
Technical Device Information
• Here the information concerns the operating systems, software installed or any associated peripherals (that is, virtual reality headsets and controllers).
Device Event Information
• Device event information includes crash reports (e.g., where gamers encounter an error playing games) and detailed information related to software or hardware used, or contents of files opened in error.

There is ambiguity surrounding whether technical information — particularly device identifiers — qualifies as personal information under the *Federal Privacy Act*.[83] This stems from the broad nature of the concept of personal information under the Act, as highlighted in Part II. However, as also noted in Part II, there is a strong possibility that technical information including IP addresses, cookie identifiers, device identifiers, location data, radio identification tags, and other such identifiers may be classified as personal information in the future.[84]

81 G*overnment Response* (n 50) 6.

82 Appcensus, *1,000 Mobile Apps in Australia: A Report for the ACCC* (Interim Report, ACCC, 24 September 2020) 9.

83 *PAR Report 2022* (n 41) 24.

84 *Government Response* (n 50) 5.

F *Biometric Information*

Biometric information is 'information about an individual's unique physiological or behavioural characteristics'.[85] Under the *Federal Privacy Act*, biometric information that is used to automatically verify or identify an individual is considered sensitive information.[86] Automatic verification occurs when an image is matched with another image in a database to verify that a person is who they claim to be.[87] Automatic identification occurs when an image is matched with all other images in the database to identify a potential match.[88]

The term 'biometric' is not further defined under the *Federal Privacy Act*. However, in the *7-Eleven* determination, it was noted that biometric information can include information about physiological features[89] (including any facial features, iris scans, fingerprints, signatures and voices) which can be used to identify an individual and behavioural attributes (such as an individual's gait or keystroke pattern).[90] If biometric information is collected but used for purposes other than identification or verification, it is classified as personal information.[91]

Gaming companies use cameras, microphones and other hardware to collect biometric information, which includes the four following elements:

1. Sensitive information is collected via facial scanning,[92] eye tracking, skin response,[93] and biometric templates, including scans of fingerprints, hands, or face geometry.[94] This information is considered sensitive information and not personal information because it is used to verify the identity of the gamer. The purpose of verification could be to: (1) confirm the age of a gamer;[95] (2) ensure

---

85 Sharon Givoni and Alec Christie, 'Guide to Understanding the Australian Biometric Privacy Law Landscape', *LexisNexis* (Web Page, 9 March 2023) <https://www.lexisnexis.com.au/en/insights-and-analysis/research-and-whitepapers/2023/privacy-law-bulletin-2023-special-issue>.

86 *Federal Privacy Act* (n 11) s 6 (definition of 'sensitive information').

87 'Biometrics and Privacy' (n 43).

88 *Clearview* (n 45) [123].

89 *7-Eleven* (n 28) [47].

90 Ibid.

91 *PAR Report 2022* (n 41) 127.

92 See, e.g., PlayStation (n 69).

93 Russell, Reidenberg and Moon (n 8) 61, 85.

94 See, e.g., Roblox, 'Roblox Biometric Privacy Notice', *Roblox Support* (Web Page, 29 August 2024) <https://en.help.roblox.com/hc/en-us/articles/4412863575316-Roblox-Biometric-Privacy-Notice>.

95 See, e.g., Bandai Namco, 'Privacy Policy', *Bandai Namco Entertainment America Inc.* (Web Page, 31 July 2025) <https://www.bandainamcoent.com/legal/privacy>.

that an access request under APP 12 of the *Federal Privacy Act;*[96] is made by the gamer and not an imposter;[97] or (3) confirm gamer identity in cases involving competitive gaming.[98]

2. Photographs (including profile or account photos containing facial images of a person)[99] and live camera inputs[100] which could be classified as 'personal information'. However, there is a lack of consensus over when photographs *alone* qualify as personal information. In the *7-Eleven* determination, it was noted that 'facial image alone will generally be sufficient to establish a link back to a particular individual', as facial images 'display identifying features unique to that individual''.[101] In *Clearview AI Inc v Australian Information Commissioner*, however, it was noted that a 'photo will render a person reasonably identifiable if it is shown to someone who knows them but not if it is shown to someone who doesn't.[102] Nevertheless, the OAIC considers photographs alone to be personal information.[103]
3. Audio/visual information, such as voice clips or gameplay recordings (video footage of a video game as it is being played, which could include a gamer's voice and face). Here, the biometric information is used to enable gameplay and not for *identification* and so is likely to be classified as personal information, rather than sensitive information, under the *Federal Privacy Act.*
4. Information about physical movements,[104] such as steps taken,[105] skeletal tracking,[106] hand gestures and movements of facial features (e.g., closing eyes and opening mouth).[107] This information is likely to be considered 'weak biometric' information; that is, 'features that are "less unique" or "less stable", e.g. body shape, [and] behavioural patterns'.[108] As this is less likely to uniquely identify an individual, whether it is classified as personal information under Australian privacy law remains unclear. As noted, for a piece of information to

96 *Federal Privacy Act* (n 11) sch 1 pt 5 cl 1: APP 12. Australian Privacy Principle 12 entitles individuals with a right to request access to their personal information held and processed by the APP entity.

97 See, e.g., 'Microsoft Privacy Statement' (n 7).

98 See, e.g., 'Call of Duty League Privacy Policy' (n 66).

99 See, e.g., Playtika, 'Privacy Notice', *Playtika Ltd.* (Web Page, October 2024) <https://www.playtika.com/privacy-notice/> ('Playtika Privacy Notice').

100 Roblox Facial Animation Privacy Notice (n 6).

101 *7-Eleven* (n 28) [33].

102 [2023] AATA 1069 [109].

103 *What is Personal Information?* (n 22).

104 See, e.g., Roblox, 'Roblox Privacy and Cookie Policy', *Roblox Support* (Web Page, 6 November 2024) <https://en.help.roblox.com/hc/en-us/articles/115004630823-Roblox-Privacy-and-Cookie-Policy>. ('Roblox Privacy and Cookie Policy').

105 'Microsoft Privacy Statement' (n 7).

106 Ibid.

107 'Roblox Facial Animation Privacy Notice' (n 6).

108 Christiane Wendehorst and Yannic Duller, *Biometric Recognition and Behavioral Detection* (Study, No PE 696.968, 2021) 13.

be personal information, it must be *about an identified or reasonably identifiable individual*. While biometric information (such as hand gestures) is about an individual, given that it is an action taken by an individual, by itself it cannot reasonably identify an individual. But if attached to other personal information, it can help infer more information. For instance, a person's gait can help determine their gender.[109]

G *Social Information*

Social information refers to information about how gamers interact with each other.[110] It includes their movements across the user community (such as forums and websites),[111] as well as social information relating to gamers themselves (information collected over social media accounts connected to gamers' real-world identities and friend lists, including how often they use social media, such as chat).[112] Social information, such as the content of messages and posts, is likely to be considered personal information under the *Federal Privacy Act*.[113] Thus, gamers disclosing their name, political views, or sexuality in the forum or chat would be voluntarily disclosing sensitive information. Collection also occurs when gamers use their social media account to play a game. The amount of information collected in this way depends on users' privacy settings on the social media platform.[114] In general, the use of social media accounts can facilitate the collection of information that includes real name, profile picture, email address, age, gender, country,[115] birthday, likes, location, advertisements seen and content viewed.[116]

H *Behavioural Information*

Behavioural information refers to information about gamers' behaviour and characteristics. From information collected about the 10 companies studied, behavioural information collected by gaming companies can be divided into three kinds: (1) information regarding gamers' interactions with products (in this case, games); (2) purchasing behaviour (as distinct from transactional information); and

109 Muhammad Azhar et al, 'A Gait-Based Real-Time Gender Classification System Using Whole Body Joints' (2022) 22(23) *Sensors* 9113, 9113.

110 Magy Seif El-Nasr, Anders Drachen and Alessandro Canossa (n 2) 23.

111 See, e.g., 'Privacy Policy', *Take-Two Interactive* (Web Page, 26 April 2023) <https://www.take2games.com/privacy>.

112 See, e.g., 'Privacy Policy', *Activision* (Web Page, 22 December 2022) <https://www.activision.com/au/en/legal/privacy-policy>.

113 See e.g., *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [8]: 'chats' and 'posts' made via their personal Facebook account were considered as personal information. See also *Australian Information Commission v Facebook Inc* (2020) 144 ACSR 88, 97 [46]: where the OIAC submitted that chat and messages are personal information.

114 See, e.g., Activision (n 112).

115 King (n 68).

116 Warner Media (n 67).

(3) information about gamers' interests and likes. Table 5 provides a glimpse of behavioural information revealed by privacy policies to be collected by the gaming companies examined.

Table 5: Behavioural Information Collected by Gaming Companies

Information Regarding Gamers' Interactions with Product (Game) Features
• Content and advertisements downloaded to a gamer's device, content viewed or posted. • Advertisements interacted with. • Information related to browsing behaviour. • Information about gamers' active or inactive subscriptions, licences and other entitlements, promotions trial periods, and rewards.
Purchasing Behaviour
• Products or services considered (added to the 'basket' in-game companies digital stores) or purchased.
Information about Gamers' Interests and Favourites
• Information about certain preferences, such as sports teams, game genre interests, media content interests (such as TV, video, movies, music, textbooks, apps, and games) or the stocks gamers track. In addition, interests and likes can be inferred or derived from other information, such as ratings, reviews, or problem reports submitted to the digital store and the account associated with them.

Behavioural information is valuable not just for gaming companies but also to AdTech companies (advertisers)[117] to which information is often disclosed for 'targeted'[118] or personalised advertising,[119] that is, to better target advertisements to individuals.[120] Advertising companies use tracking technologies, such as cookies and web beacons, to aggressively collect gamers' personal information outside the gaming context (such as shopping websites[121] or social media websites)[122] and combine it with information received from gaming companies. Advertising companies accordingly have access to information about gamers outside the gaming context, meaning that the information collected can potentially be used for unanticipated purposes and so poses a higher risk of privacy harm.

117 AdTech companies include advertising agencies and networks, data brokers, data analytics companies, publishers and buyers.

118 Electronic Arts (n 77).

119 Roblox, *Roblox Privacy and Cookie Policy* (n 104).

120 Sophie C Boerman, Sanne Kruikemeier and Frederik J Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) *Journal of Advertising* 363, 363–4.

121 See, e.g., Nintendo, 'Nintendo Account Privacy Policy', *Nintendo* (Web Page, July 2021) <https://accounts.nintendo.com/term/privacy_policy/AU?lang=en-GB>.

122 See, e.g., King (n 68).

I *In-Game Behavioural Information*

In-game behavioural information targets information about how gamers interact within the game, which includes tracing 'every single choice, action, and footstep'[123] taken within the game. Table 6 below provides examples of in-game behavioural information collected by the subject gaming companies.

Table 6: In-Game Information Collected by Gaming Companies

In-Game Behaviour Information
• Information about the actions gamers take within games (e.g., obstacles jumped over and types of vehicles used in-game). • Items collected, collaborations, and other in-game choices (such as the way gamers interact with certain features or pop-ups). • Any content gamers create or submit in the game or app and other gameplay information.

In-game behavioural information is a type of personal information that is particular to the video game industry. It includes information such as the gamer's progress within the game, which, while generally harmless, can raise privacy concerns when combined with other information to create new inferences about an individual. For instance, in-game behavioural data can help discern personality traits, such as leadership skills, or the fact that gamers are disloyal in real life.[124]

J *Personal Records*

This information is collected on an opt-in basis and includes 'government related identifiers' as defined by the *Federal Privacy Act*.[125] Personal records collected by gaming companies include government-issued identifications, such as an individual's driver's licence number, Medicare number and passport number,[126] presumably to establish or verify the identity of an individual.[127] However, only four of the 10 companies studied collected personal records and then only with gamers' consent.

The thematic analysis accordingly reveals that a substantial amount of gamer information is collected by gaming companies, raising potentially significant privacy concerns. This includes sensitive information, such as biometric information, personal records and transactional information. Some categories of information

123 Alex Wiltshire, 'How Developers Harvest Your Data to Make Their Games Better', *pcgamer* (Web Page, 5 October 2018) <https://www.pcgamer.com/how-developers-harvest-your-data-to-make-their-games-better/>.

124 Dragana Martinovic et al, '"You Are What You Play": Breaching Privacy and Identifying Users in Online Gaming' in *2014 Twelfth Annual International Conference on Privacy, Security and Trust* (2014) 31, 35.

125 *Federal Privacy Act* (n 11) s 6(1) (definition of 'government related identifier').

126 'Blizzard Entertainment Privacy Policy' (n 5).

127 *Federal Privacy Act* (n 11) sch 1 pt 3 cl 9.3: APP 9.3.

collected, such as precise location information and technical information, can be used to identify and track individuals, enabling gaming companies to create a gamer behaviour profile. For instance, companies use information about places gamers have visited, alongside their general interests, likes, and behaviours, to determine their political leaning.[128] Companies can then manipulate users by targeting them with specific content. For instance, gaming companies can discern which users are willing to spend money and then coerce them to spend (more) money[129] — either with offers made exclusively to them (such as rare collectible items or discounts on the next purchase),[130] or by offering items at a differing higher price (but claiming it is an exclusive low price).[131] Thus, gaming companies collect a plethora of personal information, which may be harmful to gamers if exploited.

V Combining Information and Privacy Implications

Privacy concerns go beyond the collection of vast amounts of information. Gaming companies combine the information they collect across different contexts. Some of the information they collect and combine, such as biometric data or political beliefs, is also sensitive information. This information may be seriously prejudicial to the gamer if disclosed.

The collection of information is not limited to the gaming environment. For example, as Electronic Arts ('EA') explains, referring to their tracking technology, 'these technologies can sync or connect behavior across different websites, mobile apps, and devices'.[132] Gaming companies use a plethora of such tracking technologies — such as cookies, web beacons, Application Programming Interface ('API') and Software Development Kit ('SDK') — to collect information about gamers. The information thereby collected includes specifications of the users' device (e.g., type of device, version of Android) and games (e.g., gamers' preferences, location, friends). These

128 James Ball, 'Angry Birds and "Leaky" Phone Apps Targeted by NSA and GCHQ for User Data', *The Guardian* (online, 28 January 2014) <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>; Sam Schechner, Emily Glazer and Patience Haggin, 'Political Campaigns Know Where You've Been. They're Tracking Your Phone', *Wall Street Journal* (online, 10 October 2019) <https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889>.

129 *Norwegian Consumer Council* (n 44) 20–1.

130 Daniel L King et al, 'Unfair Play? Video Games as Exploitative Monetized Services: An Examination of Game Patents from a Consumer Protection Perspective' (2019) 101(December) *Computers in Human Behavior* 131, 138.

131 Daniel L King and Paul H Delfabbro, 'Predatory Monetization Schemes in Video Games (Eg "Loot Boxes") and Internet Gaming Disorder' (2018) 113(1) *Addiction* 1967, 1968; Rafi Mohammed, 'How Retailers Use Personalized Prices to Test What You're Willing to Pay' *Harvard Business Review* (Web Page, 20 October 2017) <https://hbr.org/2017/10/how-retailers-use-personalized-prices-to-test-what-youre-willing-to-pay>.

132 Electronic Arts Inc (n 77).

technologies are also capable of sending personal information, including sensitive financial and health information, to a third party.[133]

Most of these tracking technologies have a unique identifier (such as an Ad ID) that can uniquely identify individuals and distinguish them from a group. This makes it possible to identify users, even if they are neither directly named nor identifiable.[134] In turn, this enables gaming companies to create a granular 360-degree view of gamers and then target them with advertisements and services that align with each gamer's nature.[135]

Another cause for concern is the potential for the combination and linking of information to create new personal information (inferred information).[136] Consider, say, the virtual reality ('VR') game, MetaData, collecting information on gamers as they play an escape game for 25 minutes.[137] This VR game could likely collect information related to height, age, gender, physical fitness and ethnicity.[138]

Inferences are of specific concern because video games are an extension of our physical world; that is, they are a contained environment based on the real world, where gamers' actions and behaviour can be studied.[139] This allows companies to make predictions about the behaviour of individuals in real life.[140] For instance, the choices gamers make in selecting their avatar in a game can help companies infer the gender[141] and personality of a gamer (such as how friendly they are in real

133 Sam Schechner and Mark Secada, 'You Give Apps Sensitive Personal Information. Then They Tell Facebook', *Wall Street Journal* (online, 22 February 2019) <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>.

134 *Commissioner Initiated Investigation into Australian Federal Police (AFP) (Privacy)* [2021] AICmr 74 [54]; *PAR Report 2022* (Australia) (n 41) 31: 'an individual is 'identifiable' where they are 'distinguished from all others in a group''.

135 *Norwegian Consumer Council* (n 44) 20.

136 Kröger et al (n 8) 3–6.

137 Vivek Nair et al, 'Exploring the Privacy Risks of Adversarial VR Game Design' (2023) 23(4) *Proceedings on Privacy Enhancing Technologies* 238, 238.

138 Ibid 241–3.

139 Whitson and Simon (n 10) 313.

140 See, e.g: Yannick Ferreira De Sousa and Alistair Munro, 'Truck, Barter and Exchange versus the Endowment Effect: Virtual Field Experiments in an Online Game Environment' (2012) 33(3) *Journal of Economic Psychology* 482; Zahid Halim et al, 'Profiling Players Using Real-World Datasets: Clustering the Data and Correlating the Results with the Big-Five Personality Traits' (2019) 10(4) *IEEE Transactions on Affective Computing* 568, 568.

141 Daniel Zimmermann, Anna Wehler and Kai Kaspar, 'Self-Representation through Avatars in Digital Environments' (2023) 42(25) *Current Psychology* 21775, 21775.

life).[142] Moreover, some of this information, such as gamer behaviour information (whom gamers play against or how they play),[143] is unique to games and thus not easily available through other digital mediums such as social media.

Inferences drawn can also constitute sensitive information. A gaming app may, for example, allow an inference to be drawn about a gamer's gambling problem.[144] Moreover, the information collected can be used to predict future behaviour not only of the individual whose information is collected, but also of others. For example, information including the age, location, and gameplay style of an individual over time can be analysed to determine how gamers of a similar demographic will play the game in the future.[145] Thus, the personal information collected affects not just the individual subject of the collection but others. The volume of behavioural information collected this way can be enormous, considering that an average Australian plays video games for over 90 minutes each day.[146]

It follows that the collection of information is not limited to collection practices explicitly disclosed by respective privacy policies but can encompass inferences arising from combining existing information collected outside the gaming context via third parties. Unfortunately, the true extent of information gaming companies can extract from third parties depends on preferences or an opt-out setting set by gamers with those third parties.[147] Consequently, gamers may well be unaware of the actual extent of information being collected, meaning that collection likely goes beyond what could be anticipated by gamers. For instance, Bandi Namco collects personal information from third parties about gamers including their 'preferences, characteristics, behaviour, and other information'.[148] Here it is not clear what information is collected. To illustrate, Bandai Namco collects personal information that helps determine gamers' gameplay characteristics such as how long a gamer plays or whether they are an avid player.[149] It also collects information about gamers'

142 Katrina Fong and Raymond A Mar, 'What Does My Avatar Say about Me? Inferring Personality from Avatars' (2015) 41(2) *Personality and Social Psychology Bulletin* 237, 237.

143 See, e.g., Innplay Labs, 'Privacy Notice Animals and Coins', *Innplay Labs* (Web Page, 1 November 2023) <https://www.innplaylabs.com/privacy-notice-animals-and-coins/>.

144 Imdad Ullah et al, 'Protecting Private Attributes in App Based Mobile User Profiling' [2020] *IEEE Access* 143818, 143818.

145 Rainer Mühlhoff, 'Predictive Privacy: Towards an Applied Ethics of Data Analytics' (2021) 23(3) *Ethics and Information Technology* 675, 675.

146 Jeffrey E Brand et al, *Australia Plays 2023* (Interactive Games and Entertainment Association, 2023) 5.

147 Activision, 'Privacy Policy' (n 112): 'You may be able to control how third parties collect and share your Information by changing your preferences or opting out of collection directly with those third parties.'

148 Bandai Namco Entertainment America Inc (n 95).

149 'Wooga Privacy Notice', *Wooga* (Web Page, 4 November 2024) <https://www.wooga.com/legal/en-privacy-policy>.

real-life characteristics, like their monthly spending on games.[150] Gamers would likely expect (and consider acceptable) the collection of the gameplay information, but not their purchasing habits and marriage status.[151]

VI Personal Information Collection: Legal Implications

The *Federal Privacy Act* requires an entity collecting personal information to comply with the Australian Privacy Principles ('APP') embedded in the Act. One such principle, APP 3, sets out the requirements related to the collection of personal information and sensitive information. It prescribes that personal information can only be collected if it is 'reasonably necessary' to carry out the entity's functions or activities.[152] Where possible, collection must be directly from the individual.[153] It must also be done using 'lawful and fair means'.[154] Given the importance of protecting sensitive information, the Act deals with the collection of sensitive information discretely from personal information. While the Act forbids the collection of sensitive information as a starting point, it envisages that such information may be collected if at least one of the exceptions listed in APP 3.3 applies.[155] These exceptions include where consent is obtained before the collection of sensitive information and the collection is reasonably necessary for one or more of the entity's functions or activities,[156] or where the collection is authorised by or under Australian law.[157] The ensuing sections of this paper explore the key requirements under APP 3: the need for personal information to be collected 'directly' from gamers, the use of lawful and fair means, and compliance with the 'reasonably necessary' test.

A *Directly Collected*

An analysis of the privacy policies reveals that gaming companies collect information about gamers in three ways: (1) actively from gamers; (2) passively from gamers;

[150] Rafet Sifa et al, 'Predicting Purchase Decisions in Mobile Free-to-Play Games' 11(1) (2015) *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment* 79, 79.

[151] Amel Bourdoucen, Leysan Nurgalieva and Janne Lindqvist, 'Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games' (2023) 7 (CHI PLAY) *Proceedings of the ACM on Human-Computer Interaction* 1136, 1148. Surveyed gamers considered personal information as acceptable only to the extent that it does not relate to them in the real world.

[152] *Federal Privacy Act* (n 11) sch 1 pt 2 cls 3.1–3.2: APPs 3.1, 3.2.

[153] Ibid sch 1 APP 3.6.

[154] Ibid sch 1 APP 3.5.

[155] Ibid sch 1 APP 3.3(a).

[156] Ibid sch 1 APP 3.3(a)(ii).

[157] Ibid sch 1 pt 1 cl 2: APP 2.2.

and (3) by inference from other sources.[158] Personal information can be actively collected by requesting gamers to provide it. This includes scenarios where gamers register accounts with the company[159] or engage in multiple social and community channels created by gaming companies to foster community building.[160]

Secondly, personal information is collected automatically, simply by gamers playing the game,[161] downloading, installing, or accessing games or gaming client software,[162] or using game services.[163] This avenue for collection might go unnoticed by gamers as there is no additional action required. The passively collected information can help track individuals over time across various websites and services,[164] positioning companies to infer more information about gamers.

Thirdly, gaming companies collect personal information by drawing inferences about individuals using additional personal information obtained from other third-party sources.[165] The sources include vendors, affiliates, advertisers, other gaming companies, and even other gamers.[166]

Thus, gaming companies collect personal information both directly from gamers and indirectly from third parties. The *Federal Privacy Act* requires that an organisation collect personal information directly from individuals unless it is 'unreasonable or impracticable' to do so.[167] The terms 'unreasonable' or 'impracticable' are not defined, nor have they been interpreted in any privacy determinations. The OAIC guidelines observe that whether direct collection of personal information is unreasonable or impracticable depends on the facts and circumstances of the case.[168]

158 Scholars have proffered varying classifications of different types of collection. See, e.g., Simone Van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34(2) *Wisconsin International Law Journal* 409, 412–3, which notes three classification of data collection: data volunteered, observed data and inferred data.

159 See, e.g., Nintendo Account Privacy Policy (n 121).

160 See, e.g., King (n 68).

161 See, e.g., Take-Two Interactive Software Inc (n 111).

162 See, e.g., Microsoft, 'Data Sharing with Games and Apps', *Xbox.com* (Web Page) <https://www.xbox.com/en-AU/legal/ThirdPartyDataSharing>: 'If you want to stop sharing game or app data with a publisher, remove all its games or apps from all devices where you have them installed'.

163 Electronic Arts Inc (n 77): 'Your use of EA online services through these third parties indicates your agreement for the transfer of this information'.

164 *PAR Report 2022* (n 41) 31.

165 *DPI Report* (n 40) 479.

166 See, e.g., 'Privacy Policy', *Sony Pictures Entertainment* (Web Page, 28 June 2024) <https://www.sonypictures.com/corp/privacy.html>.

167 *Federal Privacy Act* (n 11) sch 1 pt 2 cl 6: APP 3.6(b).

168 Office of the Australian Information Commissioner, 'Chapter 3: APP 3 Collection of Solicited Personal Information', *Office of the Australian Information Commissioner* (Web Page, 22 July 2019) [3.65] <https://www.oaic.gov.au/privacy/australian-privacy-

As per those guidelines, considerations that might be relevant to this assessment are elaborated below.[169]

1 *Sensitivity of the Information Concerned*

The greater the sensitivity of the information being collected, the higher the expectation that its collection will occur directly. Most gaming companies collect sensitive information such as biometric information and credit card details from third-party sources.[170] Thus, there is a higher expectation for personal information to be gathered directly.

2 *Whether Individuals Would Reasonably Expect Their Information to be Collected Either Directly From Them or Indirectly by Other Organisations*

In most indirect collections, gamers receive pre-collection notices from companies that information about them is being indirectly collected. For instance, in its privacy notice, Rockstar Games states that it collects information about gamers from 'third parties, such as advertising networks, business partners, third party information providers, and other players'.[171] Therefore, a gamer whose personal information is collected must be considered as having been 'notified' under APP 5 of the information being directly or indirectly collected.[172] Thus, they have a reasonable expectation of the direct or indirect collection.

However, gaming companies only disclose that personal information is collected directly or indirectly and not the source of collection for *each piece of information* (for instance, age) or even *each category* of personal information (for instance, transaction information) collected. In other words, the companies do not inform gamers about what categories of personal information are collected directly as opposed to indirectly.

principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information> ('Chapter 3: APP 3 Collection of Solicited Personal Information').

169 Ibid [3.66].

170 See, e.g., Playtika Privacy Notice (n 99); Roblox, *Roblox Privacy and Cookie Policy* (n 104).

171 Rockstar Games (n 4).

172 APP 5 under the *Federal Privacy Act* (n 11) proffers individuals with a right to receive a notice of collection from the data collecting entity. This collection notice must inform individuals about entities information-gathering and handling activities. This includes, inter alia, the kind of information being collected, details about the entity collecting it, why it is being collected, and the consequences of the collection. Collection notices differ from privacy policies as they perform different functions and have distinct goals. However, gaming companies conflate both by providing notices of collection via their privacy policies.

Thus, while it may be clear to gamers that information is being collected indirectly, it is unclear whether they understand the full gamut of actual information being indirectly collected. This raises the question of whether gamers could be 'reasonably expected' to be informed about what information is collected about them indirectly and thus consider such collection as reasonable. For example, gaming companies like Activision Blizzard often create cosmetic banners that gamers can use to customise their characters in the game. This cosmetic banner includes a label supporting a community or cause such as the LGBTQ+ community.[173] A person using a banner might have a reasonable expectation that gaming companies will deduce that they support the LGBTQ+ community. That is, they can rightfully assume that gaming companies collect data about their sexuality by inferring it using 'banners.' However, they will likely not agree to the indirect collection by gaming companies of their sexual orientation from third parties like the gay dating app Grindr.[174]

Surprisingly, some companies like Playtika in their information disclosure to Californian residences do mention what information is directly or indirectly collected.[175] Thus, while it is presumably not onerous for companies to disclose this information, they nonetheless choose not to disclose this information without some compulsion.

3 *Whether Direct Collection Would Compromise the Intended Purpose of Collection*

The *Federal Privacy Act* aims to balance industry interests with consumer rights.[176] Therefore, when collecting personal information, it is essential to also consider whether the direct collection would hinder the organisation from performing intended functions. For example, gaming companies indirectly collect software information from gamers to ensure that they are not violating their code of conduct by cheating.

---

173 Blizzard Entertainment, 'Coming Together to Celebrate Pride', *Overwatch Blizzard Entertainment* (Web Page, 30 May 2024) <https://overwatch.blizzard.com/news/24102826/coming-together-to-celebrate-pride/>.

174 Bobby Allyn, 'Study: Tinder, Grindr And Other Apps Share Sensitive Personal Data With Advertisers', *NPR* (Web Page, 14 January 2020) <https://www.npr.org/2020/01/14/796427696/study-grindr-tindr-and-other-apps-share-sensitive-personal-data-with-advertisers>; Emily Moschet, Brandon Liu, and Neha Aletty, 'Growth for Gaming: How Embracing a Player-Centric Approach Drives Success', *Braze* (Web Page, 11 March 2022) <https://www.braze.com/resources/articles/growth-for-gaming>. Grindr routinely shares information about their users including their sexual orientation with analytics companies like Braze. Braze, in turn, shares this sensitive information with gaming companies Roblox and Sony. Currently there is no explicit or implicit requirement under the *Federal Privacy Act* (n 11) to ensure that gaming companies collecting personal information indirectly from third party ensure that personal information was originally collected from the individual using only lawful and fair means. Thus, collection would be considered lawful but may not be reasonably necessary to carry out organisation's function.

175 Playtika Privacy Notice (n 99).

176 *Federal Privacy Act* (n 11) pt 1 s 2A(b).

This also involves scenarios where the collection of personal information is needed to fulfil public interests even though such collection may be disadvantageous to the individual concerned. Some examples set out in the Act include where personal information is collected for 'enforcement-related activity'[177] (such as lawful surveillance), permitted general situations (preventing a serious threat to life),[178] or permitted health situations (to provide a health service).[179] Consider, for instance, where a law enforcement officer uses a game chatbox to collect personal information of a child sexual predator to investigate or prosecute a crime.[180] Here, covert indirect collection of the preparator's personal information is necessary to identify the perpetrator without alerting them — the indirect collection is accordingly justified.

4 *Privacy Risks Associated with Obtaining the Information from an Alternative Source*

An organisation that collects excessive personal information about gamers runs the risk of creating additional personal information,[181] which may include personal information that is not reasonably necessary for it to perform its functions (thus violating APP 3 provisions). For example, information including the age, location and gameplay style of an individual over time can be analysed to determine how gamers of a similar demographic will play the game in the future. However, when combined, this information can also create a personality profile of the gamer[182] — including motivation factors such as family, power, status and saving — from which further inference can be made such as determining if a gamer has strong family bonds or is from a low socioeconomic background.

As noted in Part IV, gaming companies combine personal information and create new personal information (by drawing inferences). Unfortunately, there is limited understanding of the true extent of analytics in the gaming industry because such analysis techniques are considered proprietary.[183] For this reason, privacy policies

---

177 Ibid s 6(1) (definition of 'enforcement related activity').

178 Ibid s 16A.

179 Ibid s 16B.

180 Nellie Bowles and Michael H Keller, 'Video Games and Online Chats Are "Hunting Grounds" for Sexual Predators', *The New York Times* (Web Page, 7 December 2019) <https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html>.

181 World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage* (Report, World Economic Forum, 2013) 8 <https://www.weforum.org/reports/unlocking-value-personal-data-collection-usage/>.

182 Alessandro Canossa, Josep B Martinez and Julian Togelius, 'Give Me a Reason to Dig: Minecraft and Psychology of Motivation' (Conference Paper, IEEE Conference on Computational Intelligence and Games, 2013) 1.

183 Anders Drachen et al, 'A Comparison of Methods for Player Clustering via Behavioral Telemetry' (Conference Paper, International Conference on the Foundations of Digital Games, 2014) 3.

rarely mention how gamer information is used to draw inferences and so shield the full extent of inferences drawn. For instance, Blizzard states that it collects personal information to draw inferences about gamers such as 'reputation, experience, influencer type, interests'.[184] Blizzard mentions the broad categories of inferences drawn about gamers (such as influencer type) but not how the inferences are drawn or what personal information is used to draw them.

Some insights on how analytics can be used to draw inferences can be gleaned from academic research conducted using gamer information. It has been used to determine the demographic traits of gamers, such as gender,[185] education level,[186] psychologic[187] and social traits (how gamers interact with other gamers),[188] personality traits[189] and skills (including gamers' problem-solving skills[190] and learning skills).[191]

Previous survey-based research has demonstrated that most Australians are uncomfortable with companies combining personal information about them in general.[192] From this, it is reasonable to infer that most gamers will also uncomfortable with gaming companies combining their personal information. It is difficult to imagine

184 Blizzard Entertainment Privacy Policy (n 5).

185 John Murray, Edmond Chow and Christopher Connolly, 'Something in the Way We Move: Quantifying Patterns of Exploration in Virtual Spaces' (Conference Paper, International Conference on the Foundations of Digital Games, 2015) 3.

186 Carl Symborski et al, 'The Use of Social Science Methods to Predict Player Characteristics from Avatar Observations' in Muhammad Aurangzeb Ahmad et al (eds), *Predicting Real World Behaviors from Virtual World Data* (Springer International, 2014) 19.

187 Emmanuel Guardiola and Stephane Natkin, 'A Game Design Methodology for Generating a Psychological Profile of Players' in Christian Loh, Yanyan Sheng and Dirk Ifenthaler (eds), *Serious Games Analytics: Advances in Game-Based Learning* (Springer, 2015) 363, 363.

188 Maude Bonenfant, Patrick Deslauriers and Issam Heddad, 'Methodological and Epistemological Reflections on the Use of Game Analytics toward Understanding the Social Relationships of a Video Game Community' in Günter Wallner (ed), *Data Analytics Applications in Gaming and Entertainment* (CRC Press, 2019) 183, 188–91.

189 Halim et al (n 140) 568, 568.

190 Valerie Shute, Gregory Moore and Lubin Wang, 'Measuring Problem Solving Skills in Plants vs Zombies 2' (Conference Paper, International Conference on Educational Data Mining, 2015) 428, 428.

191 Wim Westera, Rob Nadolski and Hans Hummel, 'Serious Gaming Analytics: What Students Log Files Tell Us about Gaming and Learning' (2014) 1(2) *International Journal of Serious Games* 35, 35.

192 Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020* (Office of the Australian Information Commissioner, September 2020) 111 <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/>: 53% of respondents reported being uncomfortable with a business combining data about them.

gamers would agree to gaming companies combining their information in the manner suggested above, especially when the information from the gaming context is combined with real-world information about them. Consider, for instance, a third-party advertising company Red Shell whose technologies were used by gaming companies to advertise their products and services. For this advertising purpose, gaming companies shared gamers' personal information with Red Shell, which then used this personal information (including user ID, IP address, and browser details) to track gamers *outside* the gaming context and thus collect more personal information, without obtaining gamers' prior consent.[193] Red Shell thus had access to gamers' combined personal information, both within and outside the gaming context, which it proceeded to share with other third-party advertisers outside the gaming context. This allowed third-party advertisers to target gamers with personalised advertisements based on their interests within the game.[194] Such collection, use and disclosure of gamers' personal information by Red Shell without gamers' consent, once revealed, was vehemently protested by gamers. Curiously enough, gaming companies considered the use of Red Shell to be unproblematic until gamers opposed it as a violation of their privacy.[195] Thus, gaming companies themselves inadvertently breached privacy obligations by not understanding the full implications of information collection.

Additionally, as personal information is combined with other information, companies can use this information for other purposes mentioned in their privacy policies, including commercial purposes. This too raises the question of whether gamers would 'reasonably expect' the kinds of inferences that will be drawn about them and how such information will be used. In turn, this calls into question the legitimacy of such information collection.

5 *The Time and Cost Involved in the Collection of Personal Information*

The time and cost required to collect personal information directly must be excessive and not merely 'inconvenient, time-consuming or impose some cost'.[196] Some personal information collected from third parties (say, other gamers) would be impossible to collect directly from gamers. Consider a scenario where a third-party

---

193 Owen S Good, 'Marketing "Spyware" Caught in PC Games but Makers Reject That Label', *Polygon* (Web Page, 20 June 2018) <https://www.polygon.com/2018/6/20/17485762/red-shell-spyware-pc-games-controversy-steam>. See also Smith, 'Gamers: Is Red Shell 'Spyware' Being Used in the Games You Play?' *CSO* (Web Page, 17 June 2018) <https://www.csoonline.com/article/565668/gamers-is-red-shell-spyware-being-used-in-the-games-you-play.html>.

194 Ibid.

195 Andy Chalk, 'Red Shell Analytics Software Causes Privacy Uproar, Over a Dozen Developers Vow to Drop It (Updated)', *PC Gamer* (Web Page, 19 June 2018) <https://www.pcgamer.com/red-shell-analytics-software-causes-privacy-uproar-over-a-dozen-developers-vow-to-drop-it/>.

196 Office of the Australian Information Commissioner, 'Chapter 3: APP 3 Collection of Solicited Personal Information' (n 168) [3.65].

game distribution platform, like Steam, provides gaming companies with information regarding the amount of time gamers spend playing games of a particular genre through the Steam platform. Gaming companies do not have access to this information by themselves but might need the information to determine how best to advertise games. That is, if a gamer has spent more time playing action games than strategy games, it is assumed that they like action games and so are more likely to buy action games.

Consequently, one could posit that — despite the considerable time and cost involved in directly collecting personal information — indirect collection of personal information by gaming companies may be unreasonable in view of the sensitivity of the information gathered, gaming companies' lack of notification to gamers about the extent of indirect data collection, and the privacy risks involved in gathering information from alternate sources. Accordingly, it may violate APP 3.6, which mandates the direct collection of personal information.

(a) Lawful and Fair Means

The term 'lawful' is not defined under the *Federal Privacy Act*. The OAIC gives examples of unlawful collection that may occur by means such as hacking or doing anything that can be construed as a civil wrong.[197] 'Fair means' implies that the collection of information is not achieved via intimidation, deception or unreasonably intrusive means.[198] For instance, personal information should not be collected covertly using phone tapping.[199] The gaming companies studied in this paper have not, to the best of the authors' knowledge, directly collected personal information using any unlawful or unfair means.

(b) Legitimate Functions or Activity

The functions and activities of an organisation can include any current and proposed function or activity.[200] It can also encompass any other support activity that is necessary to perform an organisation's function. For instance, if a purchase is made via the company Take-Two Interactive directly, Take-Two Interactive indicates that it will collect the shipping address (such as name and address) along with payment details to ensure the product is delivered to the gamer.[201]

197 Ibid [3.61].

198 Explanatory Memorandum to Privacy Bill (n 31) 77.

199 Office of the Australian Information Commissioner, 'Chapter 3: APP 3 Collection of Solicited Personal Information' (n 168) [3.63].

200 Ibid [3.13].

201 Take-Two Interactive Software Inc (n 111).

Generally, an organisation's function or activity is described in its website, corporate brochures and/or annual report.[202] An organisation can perform any function or activity that is lawful.[203] In other words, companies can declare that they perform any function or activity and, so long as it is not illegal, it will be deemed legitimate. This allows gaming companies to self-determine what their functions or activities are.

Analysis of all 37 privacy policies determines that companies have seven broad purposes for which they use gamers' personal information: (1) personalisation; (2) service improvement and analytics; (3) service functionality and security; (4) marketing and advertising; (5) fair gaming; (6) legal compliance; and (7) direct marketing.

While the purpose of the information collection listed above seems *prima facie* unproblematic, in practice it is not so innocuous. For example, Rockstar games, which collects personal information and makes inferences to 'help create a personalized profile so [they] can identify goods and services that may be of interest'.[204] Here, it is unclear what kind of profile is created and how gaming services will be personalised. This practice allows gaming companies, such as Rockstar, to make an inference about gamers' likes and interests such as their favourite football team to suggest places where gamers could buy football jerseys.[205] Rockstar can also broadly interpret the privacy policy and make an inference that the gamer is frequently disloyal[206] and likely to cheat on their partner,[207] and suggest sites enabling extramarital affairs like Ashley Madison. This is intimate personal information that could negatively impact gamers if further shared.

Thus, the ambiguous language used by gaming companies raises doubt over what personal information is being collected and whether such collection could qualify as 'reasonably necessary' (that is, a reasonable person would agree if such collection were necessary) and thus legitimate (examined further below in the context of fair gaming).

---

202 Office of the Australian Information Commissioner, 'Chapter 3: APP 3 Collection of Solicited Personal Information' (n 168) [3.14].

203 Ibid [3.15].

204 Rockstar Games (n 4).

205 Eli Hodapp, '"We Own You": Confessions of an Anonymous Free to Play Producer — TouchArcade' (Web Page, 16 September 2015) <https://toucharcade.com/2015/09/16/we-own-you-confessions-of-a-free-to-play-producer/>.

206 Dragana Martinovic et al, '"You Are What You Play": Breaching Privacy and Identifying Users in Online Gaming' in Ali Miri et al (eds), *2014 Twelfth Annual Conference on Privacy, Security and Trust* (Institute of Electrical and Electronics Engineers, 2014) 31, 31.

207 Patrick Stafford, 'The dangers of in-game data collection', *Polygon* (Webpage, 9 May, 2019) <https://www.polygon.com/features/2019/5/9/18522937/video-game-privacy-player-data-collection/>.

(c) Reasonably Necessary

The term 'reasonable' is not defined by the *Federal Privacy Act* and so arguably bears its ordinary meaning.[208] The term 'necessary' does not mean that collection is 'essential' or 'indispensable'; rather, it must be 'proportional', that is, 'reasonably appropriate and adapted'.[209] It requires that collection, uses and even disclosure be not 'merely helpful, desirable or convenient'.[210] The OAIC considers the collection of information for any undefined future use as an unnecessary collection.[211]

What is 'reasonably necessary' invites an objective test that demands consideration from the perspective of a reasonable person, not just that of the APP entity collecting and handling personal information.[212] It requires that a reasonable person, once properly informed of how an APP entity would collect and handle personal information, would agree that its collection and handling is necessary.[213] This test 'must be applied in a practical sense'.[214] The question to be determined is whether a function cannot be effectively performed without collecting personal information[215] and whether there are no reasonable alternatives available (such as public information) that can be used to perform the activity or function.[216] Thus, the 'reasonably necessary test' is concerned with minimising the collection of personal information.

As evidenced by Table 3 and summarised in Part V, gaming companies collect extensive personal information on gamers. The quantity of personal information collected appears to exceed what is reasonably required, potentially infringing APP 3. Companies seek to justify collection as necessary to perform their functions. Consider, for instance, the following provision in Activision's privacy policy:

> To provide a fair gaming experience … Activision may monitor and/or record your gameplay and communications (including without limitation chat text or voice communications) and activities on your device including information about the programs running alongside the game.[217]

---

208 Office of the Australian Information Commissioner, 'Chapter B: Key Concepts' (n 39) [B.108].

209 *Mulholland v Australian Electoral Commissioner* (2004) 220 CLR 181, 200–1 [39] (Gleeson CJ).

210 *7- Eleven* (n 28) [58].

211 Office of the Australian Information Commissioner, 'Chapter 3: APP 3 Collection of Solicited Personal Information' (n 168) [3.21].

212 Explanatory Memorandum to Privacy Bill (n 31) 53.

213 Ibid.

214 Office of the Australian Information Commissioner, 'Chapter B: Key Concepts' (n 39) [B.118].

215 Ibid.

216 Ibid.

217 Activision (n 112).

In so doing, Activision is collecting personal information and sensitive information.[218] Gamers would agree that the collection of some personal information to prevent cheating is necessary, as cheating is counterproductive to gaming.[219] However, what must also be considered is the *extent* of information being collected to prevent cheating. For instance, Activision's anti-cheating technology (Ricochet) claims it 'monitor[s] analytics to identify cheating'.[220] Here, it is not clear how Activision monitors players. Does it embed artificial intelligence into the chat box that scans for keywords and collects personal information only when certain keywords associated with cheating are detected? If so, would this be a 'reasonably necessary' collection? However, if Activision monitors and records anything said and done using chat and voice communications at any time, the collection is excessive — especially considering that Ricochet has access to virtually all programs running on a gamer's personal computer,[221] which leaves gamers particularly vulnerable to privacy invasion in case of any security breach.[222]

From the language Activision has chosen (that is, 'monitor and/or record'), it seems that the company may collect and store all the chat and video communications as personal information. The extent of information it collects thus ostensibly goes beyond what is necessary to effectively perform the company's function. Activision, it seems, seeks refuge in gamers' consent as a basis for its collection by mentioning in its Terms of Use that gamers' 'express consent' to such monitoring and recording is 'irrevocable'.[223] Notably, under the *Federal Privacy Act*, consent is not an exception to the 'reasonably necessary' requirement. This appears from the terms of APP 3 itself, which provides no consent exception. Additionally, gaming companies collecting sensitive information must obtain the consent of gamers *in addition to* ensuring that the collection of information is 'reasonably necessary'.[224] Therefore, while the collection of personal information is necessary to determine

218 This information is also sensitive information as voice print is used to verify the identity of gamer.

219 Irdeto, *Irdeto Global Gaming Survey: The Last Checkpoint for Cheating* (Report, 2018) 3: '77% of online gamers would be likely to stop playing a multiplayer game online if they thought other players were cheating to gain an unfair advantage'.

220 Activision, 'Ricochet Anti-Cheat: Call of Duty's Anti-Cheat Initiative', *Activision Support* (Web Page, 24 October 2024) <https://support.activision.com/articles/ricochet-overview>.

221 Serif Pilipovic, 'What Kernel-Level Anti-Cheat is and Why You Should Care', *LEVVVEL* (Web Page, 24 March 2023) <https://levvvel.com/what-is-kernel-level-anti-cheat-software/>.

222 See, e.g., Sarah Fielding, 'Hackers Gave Pro Players Cheats During EA's North American Finals of Apex Legends', *Engadget* (Web Page, 18 March 2024) <https://www.engadget.com/hackers-gave-pro-players-cheats-during-eas-north-american-finals-of-apex-legends-122102739.html>.

223 Activision, 'Terms of Use', *Activision* (Web Page, 26 September 2024) <https://www.activision.com/au/en/legal/terms-of-use>.

224 *Federal Privacy Act* (n 11) sch 1 pt 1 cl 3: APP 3.3.

whether a gamer is cheating, the full extent of information collected by Activision is potentially beyond what is necessary to perform this function.

Regrettably, gaming companies rarely explain what information is collected and for what purpose. Rather, as noted in Part VI (c), these companies list the kinds of personal information they collect and the purposes for which they use personal information. This obscurity makes it difficult to conclusively determine whether the collection of each piece of personal information (such as device information) is reasonably necessary for the entity to fulfil its functions. Nonetheless, considering the amount of information collected by gaming companies — which, when combined, can reveal unexpected correlations that can lead to the creation of more sensitive information — and the fact that some information may be excessive as noted above, such collection may not reasonably be required. For instance, Warner Bros collects and shares information from games that include address, phone number, interests, political and religious beliefs and ethnicity.[225] While some of the information collected (like movie interests) might aid the personalisation of content to media streaming companies, it does not appear relevant for a gaming company concerned with making games.[226] In a similar vein, collecting information about gamers' political leanings is not 'reasonably necessary' to make a better game. As the Cambridge Analytica scandal proves, there is significant harm in gaming companies like Activision collecting political information as it may be used to influence, for example, election outcomes.[227]

(d) Collection of Sensitive Information and Consent

APP 3 requires that APP entities (here, video gaming companies) obtain consent from gamers if they are collecting sensitive information[228] or are using personal information for purposes other than one reasonably expected.[229] An example of unexpected use would include a gaming company claiming to collect gamers' personal information for game personalisation when, in reality, the company uses it for personalisation beyond the gaming context.

In terms of consent for collection, it is necessary to determine whether companies are collecting only personal information or also sensitive information. Of the 10 companies examined, eight collect sensitive personal information.[230] The two exceptions are Nintendo and Playtika. Hence, only Nintendo and Playtika need not obtain the consent of gamers before collecting their personal information. However, it must be noted that Nintendo does not deny that it *can* collect sensitive information;

225 Warner Media (n 67).

226 See, e.g., 'Microsoft Privacy Statement' (n 7).

227 Ball (n 128). Activision's game Candy Crush was used to collect data to allow advertising companies to target voters believed to be Donald Trump supporters with advertisements.

228 *Federal Privacy Act* (n 11) sch 1 pt 1 cl 3: APP 3.3(a).

229 Ibid sch 1 pt 3 cl 1: APP 6.1(a).

230 See Table 3.

it claims that 'normally, Nintendo does not collect Sensitive Information'.[231] Due to this ambiguous wording, no definitive conclusions can be drawn about Nintendo's collection of sensitive information. In the case of Playtika, there is a possibility that the personal information it collects and shares can be combined to create sensitive information. Nevertheless, in the case of both Nintendo and Playtika, assuming that they only use personal information for the purpose notified and not for any other purpose, consent before the collection of personal information need not be obtained. For the other eight companies, however, consent for the collection of personal information is required. All 10 gaming companies analysed collected consent from gamers using privacy policies as a consent-collecting vehicle.

Thus, as far as collection is concerned, the gaming companies examined in this research do not fulfil fundamental requirements under the APP 3 of the *Federal Privacy Act* relating to the collection of personal information, by: (1) failing to properly inform gamers about information indirectly collected in a way that gamers would reasonably expect such collection; and (2) collecting and combining excessive personal gamer information in a manner that raises doubt about whether its collection is reasonable or even necessary to perform functions associated with the companies' game offerings.

VII Conclusion

This paper details the richness of information collected by the gaming companies studied. It establishes that the true extent of personal information collected by gaming companies requires consideration of its totality. Accordingly, thematic analysis was used to review the privacy policies of the gaming companies to discern what kinds of personal information were collected, the findings from which were grouped according to 10 different themes. The collection of information was not limited to the collection practices explicitly disclosed by the respective privacy policies but also encompassed inferences arising from combining existing information.

In fact, the personal information gathered by gaming companies is often linked to gamers' internet behaviour (such as shopping habits and websites browsed). As a result, it is possible to collate information obtained through engagement in the gaming environment with intimate details about gamers that are not conventionally obtainable, such as a person's decision-making skills combined with their browsing habits. Thus, video games have become a new hub for gathering information about gamers, by offering new opportunities and forms of information to both the gaming companies studied and the digital marketplace in general. This also highlights how the collection of personal information might go beyond what may be strictly necessary to optimise the gamer experience, such as the gamer's gambling habit or marital status. Such excessive collection is not only a security risk but poses privacy risks to gamers.

---

231 Nintendo (n 121).

The video game industry is expanding. Parallel thereto is an increasing trajectory of companies collecting gamers' personal information. This information is used to boost in-game purchases or in-game advertisements to encourage spending by gamers and generate revenue.[232] Concurrently, personal information helps to anticipate gamers' needs and streamlines game production. For instance, it allows companies to allocate resources to more popular and profitable features of a game. Thus, personal information is not just a gold nugget, but a gold mine.

Given these findings, the next fundamental issue for consideration is whether the *use* and *disclosure* of this information is privacy law compliant. This requires consideration of how gaming companies inform gamers about their information-handling activities and grant control to gamers over their personal information, against the framework for privacy protection under the *Federal Privacy Act*. To this end, further investigation into the gaming industry's compliance with relevant openness and notification requirements under the *Federal Privacy Act* is necessary.

232 See generally: Erica L Neely, 'Come for the Game, Stay for the Cash Grab: The Ethics of Loot Boxes, Microtransactions, and Freemium Games' (2021) 16(2) *Games and Culture* 228, 228; Matti Mäntymäki, Sami Hyrynsalmi and Antti Koskenvoima, 'How Do Small and Medium-Sized Game Companies Use Analytics? An Attention-Based View of Game Analytics' (2019) 22(5) *Information Systems Frontiers* 1163, 1163.