Data practices and privacy in gaming: a consolidated cross-platform analysis of publishing platforms, online multiplayer games and community sites

Chunmeizi Su, Andreas Schellewald, Jina Yoon

(email: aschellewald@acm.org)

This is the pre-peer reviewed version of the following article: Su, C., A. Schellewald, and J. Yoon. 2025. " Data Practices and Privacy in Gaming: A Consolidated Cross-Platform Analysis of Publishing Platforms, Online Multiplayer Games and Community Sites." Policy & Internet 17: 1–13, which has been published in final form at https://doi.org/10.1002/poi3.70023. This article may be used for non-commercial purposes in accordance with Wiley Terms and Conditions for Use of Self-Archived Versions.

Data practices and privacy in gaming: a consolidated cross-platform analysis of publishing platforms, online multiplayer games and community sites

Abstract

Video games are mainstream cultural artefacts that millions engage with everyday. More so, gaming has become an increasingly data-intensive aspect of people's leisure time, with previous research establishing the foundational role data plays in the production and distribution of video games, as well as the management of gamers as platform users and advertising audiences. This paper consolidates this view and establishes a baseline of data practices in gaming. Addressing a broad audience of privacy researchers and policy stakeholders, the aim of the paper is to open a comparative view on the issue of data privacy in gaming as it relates to other digital platform domains and social media use cases. To this end, the paper presents the results of a qualitative analysis that investigated 37 cases of online multiplayer games, video game publishing platforms, and online community sites. By analysing their privacy policies, the paper sketches the common data practices in the gaming context. Doing so, the paper lays the foundations for future systematic research assessing user privacy, trust, and data literacy amongst gamers and enables cross-disciplinary engagement with gaming and the gaming data subject position.

Keywords: data, privacy, trust, social media, gaming, platforms, algorithms

Introduction

Digital platforms increasingly gather and analyse extensive datasets to manage user experiences (Flew and Wilding, 2020). While scholarship on related privacy issues in social media is expanding (Rossotto et al., 2018), the context of online gaming privacy remains underexplored from a user perspective (Bourdoucen et al., 2023). This is concerning given that there are roughly 3 billion gamers worldwide (Newzoo 2024), suggesting an urgent need for scholars and policy makers to better understand the problem field of gaming data privacy. This paper contributes towards this goal by consolidating existing scholarship and surveying the landscape of privacy policies in the gaming context.

Previous work has established the foundational role of data in the political economy of video games (Bernevega and Gekker, 2019; Egliston and Padua, 2023; Kerr, 2017; Nieborg, 2015; Mäntymäki et al., 2019; Whitson, 2019). However, much of it has focussed exclusively on video games themselves. Yet, gamers are active across a variety of sites - including games and other digital platforms (Consalvo, 2017; Schwarzenegger et al., 2025). Additionally, there is a gap in systematic inquiries measuring levels of privacy, trust, and data literacy amongst gamers (Bourdoucen et al., 2023; Kroeger et al., 2023; Lazcano et al., 2018).

A reason behind the lack of more holistic, systematic scholarship on data privacy is insufficient consolidation of commonalities in data collection addressing the gamer data subject across sites and platforms. This paper thus aims to provide a holistic generalisation of gaming data practices. It is explicitly not a primary contribution to game studies - where scholars unpack game-specific data practices - but rather offers a consolidated view on shared data practices across gaming platforms to open the problem field for policy stakeholders and scholars outside game studies. To do so, the paper presents findings from a systematic

analysis of 37 case studies across three types of gaming platforms: online multiplayer games, video game publishing platforms, and community sites.

Based on this analysis, the paper consolidates four issues as areas of significant concern for future research on data privacy and trust in gaming: consent management, personalisation, moderation, and advertising. By generalising these practices across platform types, the paper enables two things. Firstly, it provides a baseline model for future user research to systematically measure user trust and data literacy across platforms and social contexts. Secondly, it offers an empirically grounded entry point for non-gaming scholars and policy experts into the problem field of gaming data privacy.

Previous work

The relevance of video games in the media landscape

Gaming is a mainstream leisure and social activity with market research estimates showing around 3 billion gamers worldwide (Newzoo, 2024). At this scale, video gaming profoundly shapes people's everyday lifeworlds (Hjorth and Richardson, 2020) and serves as a vital catalyst connecting people (Flew and Humphreys, 2005). In that function, some argue that as sites of large-scale social interaction, online games even predate the kinds of platforms we refer to as social media today (Taylor, 2023).

While gaming can be seen as vital to mediated social life, the topic of gaming remains often seen as "as distinct from other … compartments of media studies" (Chess and Consalvo, 2022: 159). Scholars argue that this is problematic considering how gaming is deeply woven into media industrial processes, socio-political dynamics of media culture, and people's everyday experiences (Chess and Consalvo, 2022). In short, gaming is not a peripheral but an integral "part of deeply mediatised lifeworlds" (Schwarzenegger et al., 2025: 2).

This paper follows this position acknowledging the popularity, importance, and deep integration of video games into society. More specifically, the paper's focus is on the role that data plays herein, understanding gaming as an inherently data-intensive cultural sphere (Kerr, 2017). Therefore, studying data practices is relevant to understanding not just the gaming context but also to better make sense of the logic of everyday data cultures in general (Burgess et al., 2022).

The paper's approach towards data in gaming is anchored in the rise of a "data imperative" (Fourcade and Healy, 2017). This shift is embodied by the concentration of economic power around platforms (e.g., social media sites, online marketplaces, or video games). Platforms do not merely facilitate interactions between consumers, creators, advertisers, and other actors, but actively structure and extract value from their interaction (Srnicek, 2017). Doing so, platforms leverage data to optimise engagement, determine market conditions, and reinforce their governance position (Nieborg et al., 2022; Van Dijck, 2021).

Platforms and data collection in video games

Video games constitute virtual worlds in which any activity relies on the execution of code and generation of data (Cybulski, 2014). This data is vital to facilitating play experiences. Many game features - such as maps, progression trackers, or leaderboards - rely on data collected inside the game (Medler and Margerko, 2011). Similarly, some forms of gaming, like competitive play, are accompanied by ancillary data-driven services that quantify and analyse player behaviour (Egliston, 2019). These foundational modes of activity data collection are not in themselves an issue for privacy and trust. However, game companies utilise these and additional data within complex socio-technical systems that govern gamers as data subjects.

The dominant model in the game economy today is a freemium and live services one (Kerr, 2017). Games are no longer seen as finished products but as platforms on which companies continuously engage players and extract value (Nieborg, 2015). Game companies increasingly follow a "data imperative" (Fourcade and Healy, 2017), illustrated by industry accounts describing vast player data collection as unquestioned and self-evident (Mäntymäki et al., 2019). Following platform capitalist logics (Srnicek, 2017), companies need to "make legible user scale, engagement and attention" to attract capital (Egliston and Padua, 2023). They are concerned with growing user networks as assets that can generate income without sale (Bernevega and Gekker, 2019) .

In short, game companies engage in audience commodification similar to other media sectors (Nieborg, 2015), with revenues increasingly derived from advertising or premium add-on services driven by targeted marketing (Kerr, 2017). To manage these processes, game developers engineer "tracking events" to observe play and behaviours, managing gamers as platform users (Werder et al., 2020). Data has a key economic function herein by "telling developers what players want and how to design for them" (Whitson, 2019: 5), affording "control, security, and prosperity within a highly precarious and competitive industry" (Egliston, 2024: 20).

This extends to domains of concern, such as moderation, deceptive design, and personalisation techniques. Online multiplayer games use player data to tackle issues like cheating or toxicity, using software that processes play activity data to detect cheating software (De Paoli and Kerr, 2010) or penalise behaviour conflicting with community guidelines (ADL, 2023; Frommel and Mandryk, 2024; Wijkstra et al., 2024). Player data is also vital to managing attention flows and user networks (Nieborg, 2015), and has given rise to deceptive design practices some games deploy to increase engagement and shape

behaviour in ways that benefit commercial goals (Hadan et al., 2024; Tulloch and Johnson, 2021).

Developing a holistic view of data practices in gaming

This paper builds on and extends this existing literature. In particular, it addresses a gap in missing discussions of gaming data from an angle of privacy (Bourdoucen et al., 2023; Kroeger et al., 2023; Lazcano et al., 2018). The aim of the paper is to consolidate the understanding of what common data practices in the gaming context are, laying the foundation for future research to more systematically and comparatively assess how these practices intersect with user privacy, levels of trust, and people's experiences as gamers. Working towards this goal, the paper aims to also extend the scope of the existing literature. Thus far, research in the field has mostly concentrated on gamers as players. Yet, the subject position of the gamer exists not just as a player but in a broader platform environment (Nieborg, 2015).

This broadening in scope of the gaming context is a consequence of various shifts. One is the result of the changing distribution and monetisation models discussed earlier (Kerr, 2017; Nieborg, 2015). Another reason is related to what some have discussed as the "paratexts" of gaming, the cultural artefacts that gamers engage with around games (Consalov, 2017), creating a wider game cultural environment made up of various platforms, media contents, fandoms, and communities where gamers engage with games "beyond play" (Schwarzenegger et al., 2025). Against this backdrop, this paper maps common data practices in the gaming context by taking a non-player-centric view that more broadly captures such data practices across different types of platforms.

Research method

Analytical framework

This project examined the data practices of gaming platforms through qualitative analysis of 37 cases, primarily via their privacy policy documents. “Case studies” are not a specific method but an analytical approach (Stake, 2007). A key strength of this - particularly for political economy analysis - is the ability to focus on significant cases to outline complex economic relationships and develop meaningful typologies for future inquiry and debate (Odell, 2001). Likewise, case studies have been a common approach in game studies to address the complexity of data relations (see Bernevega and Gekker, 2019; Egliston, 2024; Noeborg, 2015). The study aligns with this approach and adopted a strategy that analysed multiple case studies to map the terrain gamers navigate as they access and buy game content, interact with others, and connect with other gaming content and communities.

Case selection

The goal of qualitative research is not representativeness but rather understanding the breadth and depth of the research object. To ensure broadly surveying the gaming landscape and being receptive to various practices, cases were selected to create a heterogeneous mix. Case selection was carried out by the second and third authors, who are both gamers and have prior professional experience in the video game industry. The selection was made to include cases across major geographic regions (especially Chinese and non-Chinese regulatory spheres), a variety of major game publishers, and games that are relevant in terms of having large communities and player bases (checked through available information on escharts.com, steamcharts.com, app store downloads, and gaming market research company Newzoo). Three types of platforms surveyed are:

(a) Publishing platforms are the sites that allow gamers to purchase games, manage game content libraries, download and install game content on local devices, and launch games via

client applications (Kerr, 2017; Nieborg, 2015; Thorhauge, 2023). The selected cases of publishing platforms are: Apple App Store and Google App Store as dominant distribution platforms for mobile games; PlayStation, Xbox, and Nintendo as dominant platforms for accessing console games; Steam and WeGame as key platforms for the distribution of PC games; Epic Store, Riot Games, and Roblox as cases for developers with prominent distribution systems for their game contents.

(b) Online multiplayer games were defined as video games played over the internet with and against other players. This genre was selected as it frequently uses data-intensive technologies to facilitate social interaction and community moderation and ensure fair play conditions - for example, anti-cheat (De Paoli and Kerr, 2010) and anit-toxicity technologies (Frommel and Mandryk, 2024). The selected cases are: Apex Legends (EA), Fortnite (Epic Games), PUBG (Krafton) for the Battle royale genre; Call of Duty (Activision), Counter-Strike (Valve), Valorant (Riot Games) for the First-person shooter genre; DotA2 (Valve) and League of Legends (Riot Games) for the multiplayer online battle arena genre; Brawl Stars, Clash of Clans (both Supercell), Mobile Legends (Moonton), PUBG Mobile (Tencent) for the mobile gaming context; FIFA (now EA FC) and Rocket League (Epic Games) as popular non-combat games; Minecraft (Microsoft) and Roblox (Roblox Corp.) for online sandbox gaming context.

(c) Community sites were defined as platforms where individuals connect with other gamers. This encompasses interactions with friends, participation in public online communities, and engagement with content and creators on various social media platforms. This allowed to broaden the view “beyond play” (Schwarzenegger, 2015) and towards the platforms where gamers engage with the “paratexts” of games (Consalvo, 2017). The selected cases are: Reddit, Discord, KOOK, and YY as popular sites for online communities and social

interactions within gaming groups; Facebook Gaming, Twitch, and Douyu as key sites on which live-streamed gaming content is broadcast and consumed; YouTube Gaming and Huya as the most significant sites for video-on-demand gaming content; FACEIT and PerfectWorld Arena as platforms for competitive video gaming and esports communities.

Data collection

The analysis focused on privacy policies as primary data source. The study builds on the rationale of Bernevega and Gekker (2019: 57), who, in their analysis of the Battle Royale game genre, argue that "carefully reading through these legal documents reveals the scale of the companies' data collection and application". Analysing legal documents such as End User License Agreements has been a common analytical strategy in the field to infer the rights companies reserve themselves in terms of collection and usage of gaming data (e.g., Cybulski, 2014 or De Paoli and Kerr, 2010). The focus on privacy policies was thus made by understanding them as documents in which platforms are required to reveal their data practices, as well as doing so in a largely standardised format, making it suitable for systematic and comparative analysis.

All authors collected data in an iterative process. First, a Google Sheets table listing all the cases for the three categories. Then, fields were added for the primary data source (Privacy Policies) and secondary supporting documents (T&Cs, EULA, developer blogs, general news/patch notes, Google patents search, and other resources). Then, each author filled in relevant documents for one of the three categories.

Data analysis

Data analysis was thematic in nature (Clarke and Braun, 2017). Authors collectively screened material to familiarise themselves with the data and assess the quality and then engaged in

open coding, descriptive coding, and reflexive thematic analysis. In the first step, authors engaged in a round of open coding for a subset of the total cases using NVivo. In the second stage, the authors then coded all cases, outlining the key data practices in each. Authors together defined data practices as patterns of collecting, storing, and using data, justifying the practice, and managing consent around it. In this stage, authors engaged with secondary data sources, like Data Retention policies, where applicable, to gain a deeper understanding of given practices. In the third stage, authors grouped the coded data into overarching themes.

Limitations

Overall, the case study approach offers a holistic and systemic view on platform data practices. At the same time, limitations need to be acknowledged. Privacy Policies are limited in how much they reveal about data practices. Often, they were vague, for example, in terms of types of information collected about people's in-game behaviour. This was offset by drawing on secondary documents where necessary and available. Moreover, privacy policies are limited in the sense that they only reveal what platforms are legally required to reveal and might outline practices that a platform has not yet implemented but stated in its policy to enable future use of such. The study thus aims to make a next-step contribution to enable further systematic research by creating a consolidated baseline assessment through the available material.

Findings

This section begins by giving a summative outline of the data practices outlined through thematic analysis of privacy policies. Then, a concentrated discussion of consent management, moderation, personalisation, and advertising as critical areas of the data privacy problem field in gaming will follow.

Consent and Data Management

Consent management refers to practices relating to the management of data collection through the platform, including the positioning of platform users as data subjects in legal terms. Privacy policies created a relational dynamic here in which users are positioned with, at times, high degrees of self-responsibility. Practices were aggregated under four types: Automatic collection, Opt-in collection, User controls, and Security (See Table 1).

Table 1: List of data practices under Consent and Data management

Type	**Examples**
Automatic collection	Device and system data
	Platform usage data
	Gameplay data
	Purchase information
	In-game actions
	Cookies information
	Other tracking data
	Voice and text chat
	Social interaction data
	User-generated content
	Geolocation information
Opt-in collection	Personal information

	Account information
	Payment data
	Health and physical data
	Survey data
	Underage user's information processing
User controls	Adjust settings
	Update and correct
	Delete data/account
	Data access requests
	Contact platform
	Local subject rights
	Right to portability
	External privacy tools
	Engage legal representation
Security	Framing security expectations
	Technical data security management
	Organisational data security management

Data practices in this group are typical compliance items implemented across various digital services, with little variation between different policies of the publishing platforms, community sites, and online multiplayer games analysed. Due to the opaqueness of the privacy policy terms, it is hard to systematically compare the concrete details of data

collected. In terms of privacy dynamics, however, they establish how platforms allow users to adjust settings, opt out of certain collection methods, and update information. Findings suggest that the bottom line of provided user control is limited because platform use is data-reliant (see also Hartzog, 2021; Solove, 2013).

The findings here broaden the argument of Bernevega and Gekker (2019) in relation to the "data rent" players pay to access online gaming sites. In other words, even though users can adjust settings, there is no meaningful way to participate on the platform without data collection, complicating the notion of consent. In this way, privacy policies do not just position the gamer data subject in legal terms. Instead, they more generally establish the power dynamics of gamers in relation to platforms. Future research on negotiations of consent by gamers seems thus vital to unravel these complex economic dynamics and the nuances of how gamers navigate consent.

Marketing and Business Operations

Marketing and business operations refer to practices where data is used for a variety of business-related purposes, such as marketing, customer support, research analytics, or legal and financial reporting compliance. Overall, findings overlapped across the different types of platforms analysed. An overview of the data practices has been provided below in Table 2.

Table 2: List of data practices under Marketing and Business Operations

Type	**Example**
Marketing and advertising	Opt-in communications
	Localized promotions

	Cookies-based personalisation
	Predictive analytics
	Marketing measurement
	Internal data aggregation
	Third party sources
Customer relations and support	Processing personal info
	Accessing technical info
	Verification of identities
	Storing interactions
Research and analytics	Analysing platform features
	Analysing user needs and trends
	Training data models
	Developing data-driven features
	Analytics cookies
	Product reviews
	Feedback polls
	Rating pop-ups
	Research surveys
Management and legal	Analysing and reporting on business performance
	Data transfer in case of sale of platform

	Data transfer inside a corporate group
	Responding to law enforcement requests
	Compliance and safety duties (e.g. mitigate harm)
	Retaining data for potential legal disputes

At its core, these practices underline the inherently commercial nature of both data in gaming and the data subject position of the gamer. For example, privacy policies reveal how platforms establish data and data subjects, broadly speaking, as assets under their ownership and management (Bernevega and Gekker, 2019). This becomes evident through the rights that all types of platforms establish in their policies in terms of utilising data for business reporting and transferring data in case of a change of ownership in the platform. These findings align with the observations by Egliston and Padua (2023) on the importance of data in signalling commercial viability to investors and shareholders in the games industry.

This positionality of the gamer data subject becomes evident furthermore if we look at the set of Marketing practices. These clearly delineate the boundaries within which platforms will approach users as customers - through direct opt-in communications, localised campaigns, or tracking data-driven technologies. This aligns with the management of user networks, attention economics, and audience commodities that have been noted in the literature (Kerr, 2017; Nieborg, 2015). In this context, platforms like PlayStation note, for example, how they use data to reach users on “our and third party websites (such as social network sites) that show purchase recommendations or advertisements from us.”

Platform Experience

Platform experience management refers to practices concerned with using data to modulate the user's experience on the platform. They differ from the marketing and business practices

as they are primarily focused on shaping users' platform experience, as opposed to, for example, explicitly marketing the overall platform. The table below provides an overview. Those that stood out from analysis were personalisation and moderation.

Table 3: List of data practices under Platform Experience

Type	**Examples**
Personalisation	Basic customisation, localisation, preferences (cookies)
	Friends and social recommendations (communities to join)
	Content personalisation (usage, interests, localisation)
	Personalisation of interactions (game matchmaking systems)
Moderation	Anti-cheat systems for fair play conditions
	Various fraud detection (e.g. payment related)
	Anti-toxicity systems for in-game moderation
	Content detection, filtering, moderation
	User reports and complaint processing
	Tools for community moderators
Technical maintenance	Improve and deliver the “expected” experience
	Maintain the service on the user's device
	Device-related information to enable automatic updates
	Errors report for troubleshooting and system safety

Platform access	Login via personal and account information
	Checking technical device and system identifiers
	First-party cookies and similar technologies
	Verifying products, licences, subscriptions, etc.

All the platforms analysed engaged in some form of personalisation. Generally, four types of platform experience personalisation can be differentiated. The first is basic personalisation and customisation. For example, platforms use cookie data to remember a user's location and adjust interface languages and other features. The second is content personalisation. Drawing on usage data, user interests, or location, content offering is personalised accordingly. The third is friend and social recommendations. For example, community sites like Discord note the use of data to "power our discovery surfaces so that you see relevant communities", i.e., recommending other users to engage with. The fourth type is related more closely to multiplayer games in their use of matchmaking systems - a form of personalised interaction. These systems determine who players are matched against. The most common version is skill-based algorithms, which place players of equal skill in a match (Graepel and Hebrich, 2006). Matchmaking showcases how behavioural data is used to score people and shape online interactions.

The documents analysed revealed no specific details about what types of data are used; these are deemed business secrets. This makes it hard for players and the wider public to assess such automated systems. Players have little choice but to accept them. Otherwise, they cannot participate in playful interactions created through the system. Similarly, opting out of advanced systems puts users in a bind: "Would you like a smart AI or a dumb one?" (see Su, 2023).

Moderation is another dimension of this bind—exchanging ambiguous data for user experiences. This includes general moderation like fraud detection in payment processing. For example, Apple notes that "information about how you use your device, including the approximate number of phone calls or emails you send and receive, will be used to compute a device trust score when you attempt a purchase". Similar approaches draw on third-party vendors and financial institutions moderating such interactions.

Other general forms include content filtering and moderation (Gillespie, 2018). Most platforms filter content based on legal requirements. In online multiplayer games, specific moderation like anti-toxicity and anti-cheat technologies are found. Anti-cheat technologies are deployed to combat people using third-party software to gain unfair advantages (De Paoli and Kerr, 2010). A recent trend is kernel-based anti-cheat technologies. The kernel is the core of a user's operating system where anti-cheat technology moderates detect anomalies, i.e. cheating software being used.

Analysis of secondary documents, such as news coverage, revealed anti-cheat technology as invasive and attracting criticism (e.g., Wilde, 2020). Concerns often link to the continuity of monitoring activity. For example, community site Faceit notes in its Anti-Cheat Software EULA that it "runs continuously on the User's device and collects information on: the device … any other processes running on that device which may be used to Cheat … and User behaviours which may indicate potential Cheating." Such systems provide intrinsic benefit to gamers seeking fair play. Simultaneously, their invasive nature, collecting data at the core of devices, warrants further research to understand gamers' perspectives on this kind of moderation.

Third-party Interactions

All platforms analysed shared or received data from third-parties. With the exception of a few cases, such as Discord, most also sold data. Third parties are understood as actors distinct from the platforms (on an organisational level) and different from the individual users addressed in the privacy policies. Another legal entity working with platform data inside the organisational context of a corporate group was not classified as a third party. A content creator who makes recordings of in-game content, including, for instance, in-game communications and players' nicknames, was classified as a third party.

Table 4: List of data practices under Third-party Interactions

Type	**Examples**
Platform experience and content	Content moderation services
	Social media-related services (e.g. account linking)
	Add-on feature developers (e.g. Discord bots)
	Creators and community admins
	App and game developers
Commercial processing partners	Billing and payment services
	Tournament organisers
	Event ticket providers
	Merchandise vendors
Media and advertising services	Advertising partners (media buyers/sellers)
	Audience and ads measurement services

	Media partners
	Social media sites as advertising cookie owners
Technology related services	Data centre, cloud, hosting services
	Information security services
	IT hardware and software services
	Internet network providers
Business services	Customer support agencies
	Operational support agencies
	Compliance providers
	Marketing and user acquisition tools
	Business and management consulting
	Survey tool providers

Third parties were found to potentially be involved at any stage in given areas of practice and platform experience. The table above outlines the different kinds of service providers identified. They include infrastructural services around payment processing, data centres, or other IT services. Similarly, third-party interactions amongst community sites and multiplayer games emerged around data to develop content and tools. For example, Activision notes sharing "[i]nformation (for example, gameplay information) with our third-party partners and licensees who create applications and websites that benefit our player community (for example, tournaments, leaderboards and gameplay statistic tools)."

However, the most common and significant form of third-party interaction observed across platforms was advertising - which aligns with the general significance of advertising as a revenue mechanism in gaming (Kerr, 2017) and digital platform economy generally (Nieborg et al., 2022). The exact types of data that platforms use to deliver advertisements on their platforms remained largely opaque within the privacy policies. For example, games like Mobile Legends (Moonton) primarily work through the integration into larger advertising ecosystems, noting that they utilise Google Advertising ID "to monitor the advertising data and marketing programs … to manage advertising".

At its core, advertising as a data practice showcases the integration of platforms into a broader gaming ecosystem. Unpacking the full technical complexity of this ecosystem is a task that goes beyond the aims of this paper. However, an analysis of data practices and their relation to the gaming data subject position reveals the complexity of this position and its privacy implications. The centrality of advertising in establishing this connection becomes evident in the two-way interaction that it facilitates.

In one way, gaming platforms are sites where data is collected and/or shared back into the advertising network - for example, through platforms hosting tracking technologies of these networks on their sites. On the other hand, the data collection of these vast advertising networks is used to tie users back into the service. For instance, as Riot Games notes: "[w]e partner with third parties (like content providers, analytics companies, and advertising networks) to help us improve the Riot Services and better understand how you interact with them, as well as support our marketing initiatives".

Discussion

The analysis of 37 cases of gaming platforms has revealed a largely homogenous mix of types of data practices, showing little variation across types or regulatory spheres (e.g.,

Chinese vs non-Chinese platforms). Extending the existing literature, the present study broadened the scope by looking at a variety of platforms that included not just games but also publishing and community sites. Through that analysis, further supporting evidence has been added to the argument that gaming is inherently data-reliant (Kerr, 2017).

Consent Management

In this context, as noted earlier, the language of consent management of these platforms establishes a relational dynamic of "data rent" (Bernevega and Gekker, 2019). Simply put, there is no meaningful way of opting out of data collection in gaming unless gamers choose not to use gaming platforms at all. In that sense, the question of degrees of data collection seems crucial to be explored in the future, specifically focussing on how gamers experience their data positionality as either distinct for each platform or as unified across them.

Collecting further evidence on these experiences is vital because a general lack of meaningful control can create a culture of resignation (Draper and Turow, 2019). Research finds that users are not entirely opposed to data-driven systems, at times desiring more algorithmically personalised experiences (Ruckenstein and Granroth, 2020). Similarly, research in game studies has found that some data-driven aspects of gaming cultures are not inherently opposed - like "Achievements", which track, quantify, and, in many cases, publicly share information about one's performance in games (Jakobsson, 2011).

As scholars of algorithmic data cultures argue, people often occupy an in-between position in which they simultaneously enjoy the benefits of these new technologies while not fully agreeing with their underlying motives (Siles, 2023). Based on the analysis, personalisation, moderation, and advertising emerge as central areas of such data practices shaping gaming culture. Looking at these critically opens a productive opportunity to better conceptualise and make sense of the gamer data subject position and problem field of gaming data privacy.

Personalisation

Personalisation encapsulates the dominant logic through which platforms today seek to enhance and modulate the experience of individual users (Cohn, 2019). On the one hand, platforms justify the use of data for purposes of personalisation through the notion of experiential "relevance" (Kant, 2020). Features such as personalised recommendations for games to buy or explore, communities to join, creators and pro players to follow, content to watch, advertisements displayed, and so on all provide opportunities to enhance gamers' experience on and across gaming platforms. On the other hand, the practice of personalisation also has a problematic dimension to it. That is to say, it renders gamers as audience attention commodities (Nieboerg, 2015) or, more broadly, as targets of personalised marketing and advertising activity (Turow, 2011).

Gaming-specific forms of matchmaking emerge in this context as examples that could add meaningful perspectives to these broader debates. They constitute algorithmic systems that deeply monitor individual behaviours and shape people's interactive abilities. They are interesting because the behavioural classifications they create seem largely desired, facilitating fair play and balanced gameplay experiences in online multiplayer games. Studying these data practices could thus better help us understand what forms of data collection, modes of processing, and types of resultant classifications are seen as beneficial by users. Moreover, studying how game companies operate these systems will be of benefit to understanding how trust and distrust emerge.

Personalisation seems relevant particularly in how trust in these data-driven systems seems to operate beyond a general moral dichotomy of good and evil (Amoore, 2020). For example, following the work of O'Neill (2018), trustworthiness is judged by evaluating competence, reliability, and honesty. Put differently, gamers might not oppose personalisation activities

and the necessary data collection in general. Nonetheless, tensions might arise around this data practice when they feel platforms are incompetent or unreliable in delivering on their promises - for example, not creating a more relevant experience but merely using it for their commercial benefit, and being dishonest in that sense.

Moderation

Moderation practices form another crucial area of data practice that reveals such tensions and the complex positions that the gamer data subject occupies. Moderation has the intrinsic benefit of ensuring the integrity of gaming platforms and communities that are put under strain by cheaters and scammers or ruined by toxic interactions. At the same time, gaming platforms face the same tensions of increasingly data-driven moderation systems that scholars have discussed more broadly (e.g., Gillespie, 2018).

As Kerr et al. (2014: 334) note for the case of anti-cheating tools, concerns arise around "the methods used, their lack of visibility, and the implications … anti-cheating tools that scan player machines introduce less transparent and more hierarchical forms of surveillance." In other words, they emphasise that while data-driven systems might help alleviate the pains of cheating, they come at a price that is hard to assess due to the prevailing issue of transparency.

Understanding how gamers negotiate such a condition appears thus fruitful. Precisely because compared to other forms of online moderation, anti-cheating operates and collects data in distinct ways - monitoring not just what people do on platforms but what happens on their devices, that is, highly intimate parts of their lives (Pink et al., 2018). While these tools are not designed to have the technical ability to extract sensitive personal information from people's devices, the intimacy of this practice nonetheless warrants more scholarly attention from a privacy and trust perspective.

Anti-toxicity systems are another important area in understanding moderation. Although toxicity is not unique to gaming, it is pervasive and normalised (Beres et al., 2021), alongside pervasive stereotypes of the heterosexual, single, white, male gamer (Gray, 2020; Taylor, 2006; Shaw, 2014). Moderation in gaming thus constitutes a complex cultural issue, mapping out across platforms in modalities of in-game content, forum discussions, content and live streams, or interactions inside games.

In this last element specifically, data's role stands out as moderation occurs in settings of relative anonymity where strangers who might never meet each other again are placed in a virtual room (Frommel and Mandryk, 2024). It is here where moderation occurs precisely in settings that are intimate, experientially rich, and multimodal - combining dimensions of expressions in text and speech, yet also through actions in the game environment as the context in which behaviour is moderated through data-driven systems.

Advertising

Finally, advertising constitutes a key area of tension within gaming and the experience of the gaming data subject. As noted earlier, advertising and third-party data sharing have become a key economic logic through which games operate and generate revenue (Kerr, 2017; Nieborg, 2015). The analysis has revealed how advertising networks constitute a kind of connective tissue that enables individual platforms to reach and grasp gamers beyond the boundaries of singular platforms. The role of advertising for understanding the data subject position of the gamer emerges in these networks' capacity to constitute the gamer as such - that is, not just as a player, but also viewer, follower, buyer, and so on. The interoperability of data across gaming platforms creates the gamer data subject position as one that can be addressed and targeted by the actors involved in the video game economy.

As noted, this becomes apparent in how some platforms inform their users about their ability to address them with, for example, personalised advertisements beyond their platform - tying them back into a game or platform even though they are navigating the web elsewhere. Future research on how gamers perceive and experience this grasp and reach is needed to better understand the material consequences of this integration into more extensive advertising networks. This emerges also from how Tulloch and Johnson (2021) caution about the increasing data capture inside gaming. They note that games are increasingly emerging as platforms for the extraction of data "mapping the performances and preferences of subjects: desires, social life, social connections … biometric possibilities from health, ability and endurance, to stress triggers and response" (Tulloch and Johnson, 2021: 12).

In sum, studying personalisation, moderation, and advertising in conjecture is crucial to understanding the privacy and trust implications of these conditions of data capture. They outline how gaming platforms tap into the intimate spheres of people's leisure and social lives, using data to enhance gamers' experiences while also creating commercial value from it. As gaming platforms' data practices continue to evolve, understanding how such can be designed to be trustworthy and beneficial, with meaningful consent opportunities for gamers, will be crucial.

Conclusions

This paper has presented the findings of a formative study into the data privacy problem field of gaming. It analysed the data practices of three different types of gaming platforms (publishing sites, online multiplayer games, and community sites) and found a homogeneity of data-intensive activity across all. By doing so, the paper picked up on the discussion in the games studies literature on the growing centrality of data in the industry (e.g., Kerr, 2017)

and extended with a focus on the phenomenon of gaming “beyond play” (Schwarzenegger et al., 2025).

From this angle, the paper has consolidated the view on data’s role in gaming in relation to common practices across platforms that gamers inhabit and discussed the emerging relationships of these practices to trust and privacy. More focused investigation on key practices - consent management, personalisation, moderation, advertising - seems necessary to further unpack these data practices and their role in constituting the gamer data subject position.

Here, it appears crucial to look beyond a good and evil dichotomy and explore how users navigate trade-offs (Siles, 2023). Approaching privacy as a question of trust, particularly from a relational point of view (Scheman, 2020) in which expected potential vulnerabilities are negotiated (Baier, 1986), will be vital. Trust reflects the messy and often contradictory terrain of commercial media landscapes that people navigate. It will thus be crucial for scholars and policy makers to explore how 3 billion gamers worldwide (Newzoo, 2024) understand their position in these messy data networks - mediated by technologies of consent, personalisation, moderation, and advertising. Doing so can offer rich insights that help us prepare for a future where data-driven and algorithmic systems are becoming ever more central to people’s intimate, leisure, and social lives - in gaming and beyond.

References

Amoore L (2020) Cloud ethics: Algorithms and the attributes of ourselves and others. Durham: Duke University Press.

Anti-Defamation League (2023) Hate is No Game: Hate and Harassment in Online Games 2023. Available at: https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023 (accessed 11 April 2025).

Baier A (1986) Trust and Antitrust. Ethics 96(2): 231–260.

Beres NA, Frommel J, Reid E, et al. (2021) Don't You Know That You're Toxic: Normalization of Toxicity in Online Gaming. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama Japan, 6 May 2021, pp. 1–15. ACM. Available at: https://dl.acm.org/doi/10.1145/3411764.3445157 (accessed 11 April 2025).

Bernevega A and Gekker A (2022) The industry of landlords: Exploring the assetization of the triple-a game. Games and Culture 17(1): 47–69. DOI: 10.1177/15554120211014151

Bourdoucen A, Nurgalieva, L and Lindqvist J (2023) Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games. Proc. ACM Hum.-Comput. Interact. 7(CHI PLAY): Article 418. DOI: 10.1145/3611064

Burgess J, Albury K, McCosker A and Wilken R (2022) Everyday data cultures. Cambridge: Wiley.

Chess S and Consalvo M (2022) “The future of media studies is game studies.” Critical Studies in Media Communication 39(3): 159–164. DOI: 10.1080/15295036.2022.2075025

Clarke V and Braun V (2017) Thematic analysis. The Journal of Positive Psychology 12(3): 297–298. DOI: 10.1080/17439760.2016.1262613

Cohn J (2019) The burden of choice: Recommendations, subversion, and algorithmic culture. Rutgers University Press.

Consalvo M (2017) When paratexts become texts: De-centering the game-as-text. Critical Studies in Media Communication 34(2): 177–183. DOI: 10.1080/15295036.2017.1304648

Cybulski AD (2014) Enclosures at play: Surveillance in the code and culture of video games. Surveillance and Society 12(3): 427-432. DOI: 10.24908/ss.v12i3.5329

De Paoli S and Kerr A (2010) Assemblage of Cheating; How to Study Cheating; Imbroglio in MMORPGs. The Fibreculture Journal 16.

Draper NA and Turow J (2019) The corporate cultivation of digital resignation. New Media and Society 21(8): 1824-1839. DOI: 10.1177/1461444819833331

Egliston B (2019) Videogame analytics, surveillance, and memory. Surveillance and Society 17(1/2): 161-168. DOI: 10.24908/ss.v17i1/2.12918

Egliston B (2020) Surveillance technicity: Affect, retention and videogame analytics. Media, Culture and Society 42(6): 915-931. DOI: 10.1177/0163443719880139

Egliston B (2024) Game development, data analytics, and discourses of care. Creative Industries Journal. Epub ahead of print 13 August 2024. DOI: 10.1080/17510694.2024.2338960

Egliston B and Padua D (2023) Techniques of commensuration in the videogame industry. Convergence: The International Journal of Research into New Media Technologies 29(2): 362–378. DOI: 10.1177/13548565221123761

Flew T and Humphreys S (2005) Games: Technology, industry, culture. Oxford: Oxford University Press.

Flew T and Wilding D (2021) The turn to regulation in digital communication: the ACCC's digital platforms inquiry and Australian media policy. Media, Culture and Society 43(1): 48-65. DOI: 10.1177/0163443720926044

Fourcade M and Healy K (2016) Seeing like a market. Socio-Economic Review 15(1): 9-29. DOI: 10.1093/ser/mww033

Frommel J and Mandryk RL (2024) Toxicity in esports. In Jenny SE, Besombes N, Brock T, Cote, AC and Scholz TM (eds) Routledge Handbook of Esports. Lodnon: Routledge, pp 529-539.

Gillespie T (2018) Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media. New Haven, CT: Yale University Press.

Graepel T and Herbrich R (2006) Ranking and matchmaking. Game Developer Magazine 10. Available at: https://www.microsoft.com/en-us/research/wp-content/uploads/2006/10/Game-Developer-Feature-Article-Graepel-Herbrich.pdf (accessed 11 April 2025).

Gray, K. L., and Sarkeesian, A. (2020). Intersectional tech: Black users in digital gaming. Baton Rouge, LA: Louisiana State University Press.

Hadan H, Sgandurra SA, Zhang-Kennedy L and Nacke LE (2024) From motivating to manipulative: The use of deceptive design in a game's free-to-play transition. Proceedings of the ACM on Human-Computer Interaction 8(CHI PLAY): 1-31. DOI: 10.1145/3677074

Hartzog W (2021) What is privacy? That's the wrong question. University of Chicago Law Review 88: 1677-1688

Hjorth L and Richardson I (2020) Ambient play. Cambridge, MA: MIT Press.

Jakobsson M (2011) The Achievement Machine: Understanding Xbox 360 Achievements in Gaming Practices. Game Studies 11(1).

Kant T (2020) Making it personal: Algorithmic personalization, identity, and everyday life. Oxford: Oxford University Press.

Kerr A (2017) Global games: Production, circulation and policy in the networked era. London: Routledge.

Kerr A, De Paoli S and Keatinge M (2014) Surveillant assemblages of governance in massively multiplayer online games: A comparative analysis. Surveillance and Society 12(3): 320-336. DOI: 10.24908/ss.v12i3.4953

Kröger JL, Raschke P, Percy Campbell J and Ullrich S (2023) Surveilling the gamers: Privacy impacts of the video game industry. Entertainment Computing 44: 100537. DOI: 10.1016/j.entcom.2022.100537

Lazcano A, Avedillo A and Del Real F (2018) Artificial intelligence, privacy, and gaming: An equation with almost no regulation. Gaming Law Review 22(6): 295-301.

Mäntymäki M, Hyrynsalmi S and Koskenvoima A (2020) How do small and medium-sized game companies use analytics? An attention-based view of game analytics. Information Systems Frontiers 22(5): 1163-1178. DOI: 10.1007/s10796-019-09913-1

Medler B and Magerko B (2011) Analytics of play: Using information visualization and gameplay practices for visualizing video game data. Parsons Journal for Information Mapping 3(1): 1-12.

Newzoo (2024) Global games market report 2024. Available at: https://newzoo.com/resources/trend-reports/newzoos-global-games-market-report-2024-free-version (Accessed: 11 April 2025).

Nieborg DB (2015) Crushing candy: The free-to-play game in its connective commodity form. Social Media + Society 1(2). DOI: 10.1177/2056305115621932

Nieborg DB, Poell T and van Dijck J (2022) Platforms and platformization. In: Flew T, Holt J and Thomas J (eds) The SAGE Handbook of the Digital Media Economy. London: Sage, pp.29-49.

Odell JS (2001) Case study methods in international political economy. International Studies Perspectives 2(2): 161-176. DOI: 10.1111/1528-3577.00047

O'Neill O (2018) Linking trust to trustworthiness. International Journal of Philosophical Studies 26(2): 293-300. DOI: 10.1080/09672559.2018.1454637

Pink S, Lanzeni D and Horst H (2018) Data anxieties: Finding trust in everyday digital mess. Big Data and Society 5(1). DOI: 10.1177/2053951718756685

Rossotto CM, Lal Das P, Gasol Ramos E, Clemente Miranda E, Badran MF, Martinez Licetti M and Miralles Murciego G (2018) Digital platforms: A literature review and policy implications for development. Competition and Regulation in Network Industries 19(1-2): 93-109

Ruckenstein M and Granroth J (2020) Algorithms, advertising and the intimacy of surveillance. Journal of Cultural Economy 13(1): 12-24. DOI: 10.1080/17530350.2019.1574866

Scheman N (2020) Trust and trustworthiness. In: Simon J (ed.) The Routledge Handbook of Trust and Philosophy. London: Routledge, pp. 28–49.

Schwarzenegger C, Koenen E, Radde-Antweiler K and Wolf KD (2025) Beyond play: Researching the transformative power of digital gaming in deeply mediatized societies. Media and Communication 13: 8800. DOI: 10.17645/mac.8800

Shaw A (2012) Do you identify as a gamer? Gender, race, sexuality, and gamer identity. New Media and Society 14(1): 28–44. DOI: 10.1177/1461444811410394

Siles I (2023) Living with algorithms. Agency and user culture in Costa Rica. Cambridge, MA: MIT Press.

Srnicek N (2017). Platform capitalism. Cambridge: Polity.

Stake R (2007) Case studies. In: Denzin NK and Lincoln YS (eds) Strategies of qualitative inquiry. London: Sage, pp. 134-164.

Solove D (2013) Privacy self-management and the consent dilemma. Harvard Law Review 126: 1880-1903.

Su C (2023) Douyin, TikTok and China's online screen industry: The rise of short-video platforms. London: Routledge.

Taylor TL (2023) Games Matter. ACM Games 1(1): 1-4. DOI: 10.1145/3582928

Taylor TL (2006) Play between worlds: Exploring online game culture. Cambridge, MA: MIT Press. DOI: 10.7551/mitpress/5418.001.0001

Thorhauge AM (2023). Games in the platform economy: Steam's tangled markets. Bristol: Bristol University Press.

Tulloch R and Johnson C (2022) Games and data capture culture: Play in the era of accelerated neoliberalism. Media, Culture and Society 44(5): 922–934. DOI: 10.1177/01634437211045556

Turow J (2011) The daily you: How the new advertising industry is defining your identity and your worth. New Haven, CT: Yale University Press.

Van Dijck J (2021) Seeing the forest for the trees: Visualizing platformization and its governance. New Media and Society 23(9): 2801-2819.

Werder K, Seidel S, Recker J, Berente N, Gibbs J, Abboud N and Benzeghadi Y (2020) Data-driven, data-informed, data-augmented: How ubisoft's ghost recon wildlands live unit uses data for continuous product innovation. California Management Review 62(3): 86–102. DOI: 10.1177/0008125620915290

Whitson JR (2019) The new spirit of capitalism in the game industry. Television and New Media 20(8), 789–801. DOI: 10.1177/1527476419851086

Wijkstra M, Rogers K, Mandryk RL, Veltkamp RC and Frommel J (2024) How to tame a toxic player? A systematic literature review on intervention systems for toxic behaviors in online video games. Proceedings of the ACM on Human-Computer Interaction 8(CHI PLAY): 1–32. DOI: 10.1145/3677080

Wilde T (2020) The controversy over Riot's Vanguard anti-cheat software, explained. PC Gamer. Available at: https://www.pcgamer.com/the-controversy-over-riots-vanguard-anti-cheat-software-explained/ (accessed 11 April 2025)