Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games

AMEL BOURDOUCEN, LEYSAN NURGALIEVA, and JANNE LINDQVIST, Aalto University, Finland

Online games engage players in sharing their personal data with the games themselves and other players, which can pose security, privacy, and integrity risks to players. This paper presents an analysis of data practices in 21 online games and a qualitative interview study (N=20) that explores players' views on sharing their data in online games. Our results show that players' willingness to share personal information is contextual and related to game settings and game design elements. Our findings also highlight players' misconceptions and concerns surrounding data collection in games, and approaches to mitigate these concerns. Finally, this work identifies questionable design practices with online games and suggests design implications that will increase transparency and player control over data sharing.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → **Usability in security and privacy**.

Additional Key Words and Phrases: privacy, security, online games

ACM Reference Format:
Amel Bourdoucen, Leysan Nurgalieva, and Janne Lindqvist. 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 (November 2023), 43 pages. https://doi.org/10.1145/3611064

1 INTRODUCTION

Online games are popular. Previous studies have established that playing online games can improve well-being [30, 123] and foster social relations [29]. However, online games also collect personal data, including players' location data, gender, and age [20] or even biometric data [22, 72]. A past smartphone study discovered that smartphone players were unaware of the nature and amount of their data collected, and the purposes of its use [11]. Moreover, players are often encouraged to share more about themselves or even other players [78], for instance, when being rewarded with in-game assets for sharing [90, 110].

Games collect personal data from users for various purposes, such as advertising [95] or personalization [61]. Prior research has highlighted privacy, security, and integrity risks to users as a result of sharing information with the game and other players. For example, players may face discrimination in games if they reveal personal information, such as race, gender, or sexual orientation [91].

The lack of user awareness and transparency of data collection has been previously recognized as an issue with online games [72, 111]. However, no prior research has explored the effectiveness of user risk mitigation strategies and evaluated game design elements that hinder or support them. To the best of our knowledge, our work is the first (1) to explore users' understanding of data

Authors' address: Amel Bourdoucen, amel.bourdoucen@aalto.fi; Leysan Nurgalieva, leysan.nurgalieva@aalto.fi; Janne Lindqvist, janne.lindqvist@aalto.fi, Aalto University, Finland.

2573-0142/2023/11-ART418
https://doi.org/10.1145/3611064

collection practices in online games, including their expectations and preferences in sharing their personal data with the game and other players, (2) to review what personal data games claim to collect and share as well as related design patterns, and (3) to provide design recommendations to improve privacy with games.

To address this objective, we defined the following research questions (RQs):

- **RQ1:** What are the user views on privacy and security when choosing, setting up, and playing online games?
- **RQ2:** What are the factors that affect users to share personal data in online games?

For this study, we explore users' reasoning, understanding, and potential misconceptions related to sharing their personal data in games. We highlight what privacy settings users opt to set, the personal information that they share with the game and other players, methods they use to protect their privacy, and their general understanding of the data handling practices of games. To propose informed recommendations based on our interviews, we reviewed the most popular games for their data collection practices, privacy policies, and design patterns. Using the results of our interviews and the information obtained from studying the games, we explain the role of game design in influencing users to share personal data and recommend design guidelines to researchers and designers to limit privacy-compromising practices by the games.

2 RELATED WORK

Players share personal information with games and with other players while playing. The popularity of online games with social interaction channels such as Massively Multiplayer Online Role-Playing Games (MMORPGs) has enabled players to connect and share with their peers. Previous research has highlighted various privacy and security concerns associated with sharing of personal information in online games. There has also been a number of studies that have identified the use of deceptive user interface designs (dark design patterns) to collect users' personal information. Next, we discuss user views on sharing their data in online games and provide an overview of the purposes of data collection and associated security and privacy risks to players of online games.

2.1 Users' perceptions of data collection practices

Although there is limited work exploring users' attitudes and awareness of data sharing practices in specific online gaming contexts, there is a rich line of literature studying users' perceptions of sharing personal data online *in general*. Often, many instances of sharing data are revealed to be unintentional by users on online platforms [38, 81].

When informed about data sharing practices, users often are surprised and feel a lack of control over the data sharing process [60]. However, previous research has also highlighted that users are indeed willing to trade their privacy for convenience in certain contexts, such as when using social media [2]. Even so, many users still end up with a sense of "learned helplessness" [114] and feeling *creeped out* [60] by online data sharing practices. This is specifically puzzling when apps collect personal data that may not seem evident to be part of the app functionality. For example, where a game like *Angry Birds* would need access to the user's location, phone number, and other personal data that is not evident to be required for the game to function [81, 114]. Past studies suggest that users do not read permissions before agreeing to share their data, which makes this issue troublesome [38, 43, 44, 67, 81, 87].

To date, several efforts were aimed at improving users' information about the data collected. Past studies have suggested that users consider the collection of their data and its purpose to be important information to know about [13, 81]. Moreover, transparency from service providers helps people make confident decisions regarding their privacy [125]. Yet, according to various

studies, privacy interfaces do not provide users with enough information and control over data collection practices [39, 57]. That is a significant concern since privacy information is typically communicated to users through legal documents (for example, privacy policies) that are known to be lengthy and filled with legal jargon. One approach to address this issue proposed by Kelley et al. is creating "privacy labels" (similar to nutrition labels found on food packaging) that inform users of the data collected by apps [63]. A similar approach has been adopted in Apple's App Store's privacy nutrition labels [7]. Another approach is using personalized recommendations that alert users to any additional resources that the app might need, such as the camera or extra storage space [41]. However, approaches of this kind either were not adopted within the context of online gaming or did not go beyond an academic contribution.

To summarize, there is a need for additional extensive research to connect user behaviors and views on data collection practices with the privacy-aware designs of online games. By studying users' understanding of privacy and security in online games, our work highlights potential misconceptions and challenges users face with having control over their data, both when playing and interacting with other players.

2.2 Purposes of collecting users' data

The purposes of collecting and using player data in online games vary and might not be evident to the players. Collected data is often used for advertisements and marketing, game troubleshooting and technical improvement, and game personalization and customization. Still, each of these common purposes involves associated risks to users' data.

2.2.1 Advertisement and marketing. Advertising and personalized marketing are one of the purposes of data collection in online games to gain revenue using players' data. For instance, the data can be shared with third parties [95], or games can place ads directly on their platforms [124] and provide in-game rewards for viewing advertisements [24]. Such practices are especially common in free-to-play games [124]. Player data can also enable targeted marketing content, which is often achieved by tracking users' online behaviors over time [72, 128], and they are often oblivious or not expecting it to occur [35].

2.2.2 Game troubleshooting and technical improvement. Other purposes of collecting player data, such as user feedback, crash reports, or in-game player behavior, include game troubleshooting and improvement of game performance and reliability [103]. For example, user feedback is collected via app store reviews for the purposes of improving the app, and marketing [97]. Prior work suggests that reviews may contain sensitive user information [27].

2.2.3 Personalization and customization. Another common purpose of player data use is game personalization for player experience. Personalization can be defined as "the automatic customization of content and services" and "constructing a system capable of tailoring video game rules and content to suit some aspect of the player, for example, a player's gameplay preferences, playing style, or skill level" [61].

To provide personalization and customized interaction combinations, games capture various user data, for instance, performance data and interaction events, such as starting or stopping the game, and technical data, such as changes in network connection bandwidth [120]. Personalized games can be especially engaging for players, improve game performance [22], and support players' autonomous motivation [99], for instance, through certain game design elements, such as avatar customization [17]. However, previous research shows that online games often collect excessive user data for purposes beyond game adaptation, and not all data that can be technically captured is strictly necessary for game personalization [120].

Although users appreciate personalized player experience, they still suspect that their personal information is being collected and tracked unknowingly, creating negative feelings about personalization [23] and contributing to "personalization–privacy paradox" [46, 77]. While many enjoy the facets of personalization, the privacy of their personal information remains a concern.

Previous studies highlight the importance of considering user views on data collection in games, learning and addressing potential misconceptions, and considering ethical constraints when implementing data acquisition methods.

2.3 Risks to player data in online gaming

As discussed earlier, by collecting players' personal data, online games can introduce security, privacy, and even integrity risks to the players. However, unlike digital health interventions or financial services [5, 130], such risks in the gaming context might be less evident to the users [19]. Addressing this phenomenon, a stream of research investigated various threats to player data in the context of online games.

2.3.1 Security risks. Gaming platforms are not exempt from security attacks and potential personal data breaches, and there were a number of large-scale personal data leaks from gaming websites, such as the leak of 32 million passwords from the gaming website RockYou in 2009 [33, 134] and a 2011 leak of roughly 500k passwords from the gaming website Battlefield Heroes [131]. In 2011, Sony PlayStation shut down its online store as a result of an attack where hackers gained unauthorized access personal information of 77 million Sony PlayStation users [36, 83]. Other gaming companies experienced similar incidents: EA Games (2021) and Capcom (2020) [18].

Cheating in online games provides unfair advantages [139] and can compromise the gaming experience [16]. Common cheating forms in online games include compromising passwords, modifying client infrastructure, exploiting the lack of authentication, and compromising game servers [25]. One practical example of cheating is the use of Denial of Service (DoS) attacks against other players to create unfair advantages in MMORPGs [139]. Other harmful forms of creating unfair advantages are using game bots, destroying the in-game economy through gold farming, and stealing virtual belongings [138].

2.3.2 Privacy risks. Players can desire to remain anonymous in online games even if they do not completely understand the data sharing process [11]. This can be seen in multiplayer games: when players meet other players, they can be overly concerned about their own privacy [59]. Players' privacy concerns can be stronger when other parties are unidentifiable or anonymized [59].

The lack of user authentication in games may lead to theft of gaming accounts. One such example is when adversarial actors use another player's personal information to impersonate them online, which can enable criminal activities online [76]. A study by Chen et al. [25] suggests over 90% of online games lack authentication.

Another way that players share their identities in online games is through character sharing by exchanging account information between players. When needed, character sharing occurs between guild member friends in Role-Playing Games (RPGs) if a task is time-consuming or if an agreement is already established [137]. Research also suggests that players who play MMORPGs share high levels of their personal information with other players [109]. A study by Osmanovic and Pecchioni [96] suggests that the closeness of a relationship positively influences self-disclosure in gaming.

Social media has enabled personal data to be shared with games. For example, many popular Facebook apps, including games, have transmitted users' personal information to third-party apps [132]. Using social media accounts in games, users need to grant various permissions for games to access their personal information. A study of Wang and Bashir [133] shows that by

allowing users to link their gaming accounts to their social media accounts, 9 out of the 20 popular games were able to modify players' personal information.

Games request permissions from users to access their microphone for communication, camera for streaming, and location for tracking and personalization. Having a microphone and camera on can lead to other people listening and watching without the players' knowledge [127].

2.3.3 Integrity risks. Many games today rely on social interactions between players, and to establish such social connections and relationships, players often disclose personal information [141]. Such genuine intentions can expose them to safety and integrity risks ranging from in-game discriminatory behaviors from other players [91], trash-talking, offensive objectionable language [15], and exploitation [109].

Previous studies indicate that revealing personal details, such as race, gender, sexual orientation, or political stance, can result in abuse and bullying from other players [91]. Revealing a player's gender can be risky for women players [40]. To mitigate these risks, some women players hide or camouflage their gender by carefully managing the game character or adopting aggressive behavior to steer away harassers [32] or withdraw from the game completely [40].

2.4 Design of data collection practices online

Design features of user interfaces of online platforms and services have a great impact on user behavior and, in particular, on sharing personal data. Although some design strategies can encourage informed consent to share and increase the transparency of data practices, others can be deceptive and coerce users into disclosing personal information.

2.4.1 Dark design patterns and associated privacy risks. Deceptive designs or dark design patterns emerged as a manipulative or coercive way to make users give up personal information for businesses to harvest [92]. This is often done without necessarily informing users why their personal data is needed [56]. Dark design patterns rely on a variation of emotion, colors, language, and cognitive biases to influence users [84]. An example dark pattern is to reassure users that they are always able to cancel the purchase before the free trial period is over, which may turn out to be a difficult task [84, 108].

Another common example of a dark design pattern is so called infinite scrolling, that is, content is loaded automatically and constantly as the user scrolls down a page [89]. Other forms of dark patterns and strategies have been studied by Gray et al. [51] some of which include (1) *Nagging*: redirection of anticipated functionality that lasts longer than one or more interactions; (2) *Obstruction*: making a process more challenging than it is; (3) *Forced action*: requiring the user to take a specific action in order to access (or maintain access to) a specific functionality; (4) *Interface Interference*: manipulating the user interface to give some activities priority over others, which includes hiding information from users or aesthetic manipulation.

2.4.2 User protection mechanisms. To address the problems that occur from the use of dark design patterns in online platforms and their detrimental outcomes on users, previous research indicates a number of strategies to reclaim users' agency. For example, the use of repair tools allows easing the use of websites by altering the design or blocking ads. Such repair tools include AdGuard (ad blocker) [3], Greasemonkey (a tool for customizing website aesthetics) [79], and *GreaseDroid*, a tool that allows non-expert smartphone users to reduce dark patters on mobile apps [66].

Another strategy is to use modified versions of popular apps, such as Facebook [37] and Whatsapp [80]. Such modifications exist in online games as well: many online services offer alternative software that replaces the official game, including The Sims (life simulation video game) [86] and League of Legends (multiplayer online battle arena) [47]. Although extremely popular among users,

these solutions can pose security and privacy risks [50, 136], since such modifications rely on software vulnerabilities. In addition, they require consistent development support that may not be available [66].

Previous research indicated various privacy, security, and integrity risks to data sharing in online games. No work yet has explored users' awareness and knowledge about data collection practices, the mitigation strategies they adopt, and their effectiveness and potential misconceptions. As games evolve and new ways of data collection emerge, it is important to identify user beliefs and behaviors that might make them more vulnerable to such risks and promote designs that would support player awareness and control over their data.

3 METHOD

We combined qualitative interviews and game analysis in this work. We first conducted semi-structured interviews with 20 participants to investigate their experiences in playing online games. We then evaluated data practices and associated user interface design patterns of the games typically played by the participants. Next, we present the interview and analysis methods followed by our process for evaluating the sample of 21 online games.

3.1 Ethical considerations

The ethical board of our institute ruled that this research does not require an ethics review. We followed the best practices for informed consent with participants. Before conducting the study, participants were provided with information sheets, privacy policies, and consent forms. Participants were encouraged to contact the researchers for any questions about the data handling process before, during, and after interview sessions. These documents provided to participants contained information about the data handling practices of this study (for example, how long the data is stored) and general information about the project. During the interview sessions, the researchers explained the content of the information sheet and privacy policies to participants to ensure informed consent. After the participants completed the study and gift cards were sent out to them, all personal data was anonymized and stored in accordance with the institute's guidelines for storing personal data.

3.2 Semi-structured interviews

The semi-structured interviews were conducted remotely between February and March 2022 and lasted approximately 30 minutes.

3.2.1 Screening survey. To balance the sample of interview respondents by age and gender, we conducted a 30-question screening survey with those interested in participating (see Appendix A.1). The survey was conducted between the 16th of February and the 24th of March 2022. It was advertised through online gaming forums and university social media accounts as well as through word of mouth and snowball sampling. The decision to participate in the study was voluntary. Participants who completed a screening survey wered entered to a random draw for a 20-euro restaurant gift card.

Interview eligibility criteria included age 18 and higher, experience with playing online games, the level of English from intermediate or higher, and residing in Finland (participants needed to reside in Finland for the purpose of the institute's remuneration policies). To check for diversity in the sample, we asked participants whether their current residence was different from their country of birth. To participate in the study, participants needed to (1) play online games, (2) specify their country of residence, and (3) provide a list of games they play.

A total of 283 individuals started the survey and consented to participate. After removing incomplete and fraudulent responses, we had a sample of 31 complete and unique responses

(completion rate = 11%), and 20 of them were then invited for the interviews. The 20 participants were the first to respond to the interview invitation and agreed to participate in the interview study.

Table 1. Central interview topics, research intentions, and sample questions from interview script.

Topic	Research Intention	Sample questions
Gaming experience and preferences	To understand what do users enjoy and experience in games.	*Can you describe the games you like to play in few words?*
Permissions and privacy policies	Participants' thoughts on game permissions and privacy policies.	*When you installed the game, did it ask for any permissions?*
Use of communication channels	Participants' perceptions of social media integration and use of communication channels.	*Was there an opportunity to interact with other players? (in the game) Do you connect your social media account to the games you play?*
Account creation and online identity	What information do games collect during sign up and how do participants like to express parts of themselves in games?	*How do you create an account in the game you play? What information is asked about you? Do you think the games you play collect any information about yourself?*
Views on anonymization	If users prefer to stay anonymous and in what context.	*Do you want to be anonymous? How do you make yourself anonymous?*
Sharing personal information in games	Users sharing information with other players or the game itself.	*What information do you consider private and what is not when you play online games?*
Expectations on data flows	To uncover users' understanding of data collection practices of games.	*Do you think the games you play collect any information about yourself?*

3.2.2 Participants. Most participants were 18 to 30 years old (13/20 or 65%) and obtained higher education from universities and universities of applied sciences (19/20 or 95%). Although we did not collect participants' occupations, we diversified participants based on education and age groups. Participants' online gaming experience ranged between 2 and 27 years (median = 14 years, SD = 7.1 years). The gaming experience was self-reported by participants as the number of years they actively played games. Table 2 presents basic demographic information of our study cohort (N=20), full demographic data can be seen in Table 7 and participants' gameplay characteristics in Table 8 (Appendix A.5).

3.2.3 Qualitative analysis. The semi-structured interviews covered the following central topics and example questions (as shown in Table 1): (1) gaming experience and preferences, (2) permissions and privacy policies, (3) the use of social and communication channels, (4) account creation and online identity, (5) views on anonymization, (6) sharing personal information in games, and (7) expectations on data flows.

Table 2. Demographic characteristics of interview participants (N=20). To check for diversity in the sample, we asked participants whether their current residence was different from their country of birth.

Attribute	Range	Sample size
Gender	Female	8 (40%)
	Male	11 (55%)
	Prefer not to say	1 (5%)
Age	18 - 30	13 (65%)
	31 - 40	5 (25%)
	41 - 50	2 (10%)
Current residence is different from country of birth	Yes	14 (70%)
	No	6 (30%)
Assistance needed to download new software or app to device(s)	No	18 (90%)
	I'm not sure	1 (5%)
	Yes	1 (5%)
Level of English language proficiency	Intermediate	1 (5%)
	Advanced	17 (85%)
	Native or bilingual proficiency	2 (10%)
Education	Higher education	19 (95%)
	Upper Secondary	1 (5%)

We initially conducted three pilot interviews to validate the order of topics, flow of the interview script and clarity of questions, but the topics of the interviews remained unchanged (see the final interview guide in Appendix A.2). Interviews were then conducted by the first and second author; all of them were voice recorded and transcribed using professional transcription services.

Due to the focused nature of the semi-structured interviews, we adopted a hybrid approach to our qualitative data analysis [28, 75]. Initially, the first two authors discussed and agreed on higher-level categories for the codebook, which corresponded to the main topics of the interview guide. The interviews included the following categories: general gaming preferences and experiences, social interactions in and out of games, awareness of gaming rules and data practices, and data protection techniques in games. While the interviews were being conducted, authors regularly discussed preliminary insights. After 20 interviews, the authors agreed that data saturation for the primary interview questions was reached, and no more participants needed to be recruited.

Next, the authors proceeded to code the three interviews, resolved disagreements, and agreed on a common codebook. Two researchers then proceeded to code additional same two interviews using the agreed codebook and then discussed any new codes to be added. Since no other codes were introduced, coding of the remaining interviews was distributed amongst the first two authors using the finalized codebook.

The codebook was developed after the interview data collection, transcription, and anonymization were completed. Using the codebook, the first two authors generated themes based on recurring patterns of meaning across the participants. At this step, the codes were interpreted against contexts, understanding, beliefs, and self-reported behaviors present in participants' quotes.

3.3 Evaluation of data collected by games

We conducted an analysis of the games reported in the screening survey to gain additional understanding of player experiences with data sharing practices of games they play. The sample included 21 individual games. We examined the data types collected by games from users. We extracted

the following characteristics from the list of online games for comparison: the name of the game, platform, genre, player mode, and game purchase (paid or free) (Table 3). For the full list of game characteristics, see Table 5 in Appendix A.3.

Table 3. Characteristics of online games played by interview participants (N=21). This list of games was compiled from the online games played by the study participants. We use the following abbreviations: Massively Multiplayer Online Games (MMOs) and Role-Playing Games (RPGs).

Category	Subcategory	Number of games	Examples
Platform	Mobile only	3 (14%)	Candy Crush
	Desktop only	3 (14%)	Dota 2
	Cross-platform	15 (71%)	PUBG
	Console only	0 (0%)	N/A
Genre	Battle Royale	3 (14%)	Warzone, PUBG
	Simulation	4 (19%)	Sims 4
	MMO	2 (9%)	Destiny 2, Black Desert
	Action RPG	3 (14%)	Monster Legends
	Rhythm Games	2 (9%)	Phigros, Arcaea
	Casual Games	4 (19%)	Candy Crush
Player Mode	Single player	7 (28%)	Sims 4
	Multi-player	15 (71%)	League of Legends
Purchase	Free	17 (80%)	Arcaea
	Fully or partially paid	4 (19%)	Black Desert

In addition, the analysis covered the evaluation of the following sources and documents:

(1) Personal information handling in games: (i) data types required or optional during the registration process (by examining games interfaces presented to users), (ii) reasons why personal information is collected (descriptions provided by games), (iii) personal information displayed or accessed in the game and to whom, (iv) user profiles on games.
(2) Data protection regulations relevant to the games.
(3) Privacy policies of games, game cloud providers, and game stores.

In this technical evaluation of games, back-end processes of the data collection practices were out of the scope of this work, as many of the games in the sample were *closed source* [62]. After noting down these characteristics for each game, we ranked them based on the amount of personal information collected to uncover issues with the game design features around users' personal data collection. These are discussed in Section 6.

4 QUALITATIVE STUDY RESULTS

This section highlights that the players' decisions to install an online game are often based on game characteristics, developer's reputation, peer recommendations, and security and privacy considerations. Players often share also their personal information in the process of customization as well as through in-game social interactions with other players.

4.1 User journey within the game

The first part of the interviews explored participants' views and experiences within the games: from the decision to choose and play certain games to the process of set up, including their authentication and customization preferences.

4.1.1 Decisions to adopt online games. Among the most common reasons for selecting online games to play, participants mentioned game characteristics, the community and peers, and privacy and security considerations.

Game characteristics. Game characteristics were the first category of reasons to choose an online game. Participants often described being attracted to games that had an interesting storyline or diverse engaging scenarios or games that helped them develop their skills and interests.

Several participants (6/20) valued games that had an aesthetically pleasing look and feel, and saw the game graphics as an important factor in choosing a game to play.

More than half of the participants (11/20) mentioned that the platform where the game is available to download (e.g., Google Play) or game ecosystem (e.g., EA games, Steam, or Facebook games) as important trust factors ensuring the game has gone through a certain validation process and can be considered to be trust worthy to play (*"If you download it from a trusted source like Steam of Google Play, it's mostly not sketchy, because at least there's Google or Steam who will verify it for you that it's from that trusted source,"* P16).

Game developers. Game developers' characteristics were another important factor in selecting games. A few participants (4/20) shared that the reputation of game developers influenced their choice to download online games, for instance, being known for manufacturing specific types of games, such as educational or political games (*"I downloaded it from the website of the developer, who is very famous, so I trusted his reputation,"* P10). The size of a company also contributed to the decision to adopt, and large companies that have existed for a long time were seen as more trustworthy.

Peer recommendations. The role of the community and peers was often mentioned as a factor influencing game adoption decisions, as a source of game recommendations, and as a motivation to connect with friends and family through online games.

Several participants (5/20) shared that they followed recommendations from the gaming community members on social media or downloaded the game because it was popular in their social circle (*"I do somewhat follow gaming news from Twitter, from Kotaku, other gaming news organisations too... so I know what games have been published and what people think about them and that's mostly how I get interested in new games,"* P03). Other participants (6/20) mentioned peer pressure or recommendations from friends to influence their choice of games.

The cooperative aspect of online games was also seen as a way to connect with peers, and one participant found it especially beneficial during the COVID-19 pandemic when it was challenging to meet face to face (*"Very recently, I played Battle Royale games for the cooperative aspect of it. So in the pandemic and outside now that we cannot sit together, it has become a way for our friends to get together, chat it just so happens that you are also playing the game,"* P13).

Security and privacy considerations. Security and privacy were considered at the adoption stage by all participants but one (19/20). However, they often were mentioned in relation to concerns and reasons for *not to adopt* certain games. For almost half of the participants (9/20), potential privacy and security risks negatively affected the levels of trust they experienced with games or even prevented them from adopting certain games (*"If there's some sketchy things going on, when you see the reviews, people are telling that this seems to be logging something stuff and this is pushing advertising or something like that,"* P20).

One of such concerns related to the vulnerability to security attacks, such as Distributed Denial of Device Attacks (DDoS) or taking the benefit of learning players' IP addresses (*"There are big games, who have really, really bad security and privacy. A good example would be Grand Theft Auto*

Online [...] It's really easy to DDoS people and it's really easy to get their IPs and do all kinds of horrible stuff to their machines, like force it to restart and stuff like that," P06).

Games that ask for extensive personal information upon sign up and mobile games were often perceived as privacy-infringing. Other signs included questionable behavior of other players, such as stalking (*"People would find out where you live and then call the SWATs (Special Weapons And Tactics) on you or something like that,"* P06) or pressure to get personal information from unknown contacts (*"They want to know your real identity, or at least not identity but some picture of you, so they want to see a picture,"* P10).

Games without advertisements or paid games were among the indicators that the game was secure and private. Participants believed that paid games had less incentive to distribute players' information (*"They [reference to paid games] have less incentive to sell your data yes, but that doesn't mean they won't. But they have less incentive to,"* P13).

4.1.2 Authentication mechanisms. Only two participants (2/20) shared that they use *regular sign up* (with email) to create gaming accounts. Almost half of the participants (8/20) reported using social media login to authenticate in online games. The reasoning for signing in with social media accounts included its convenience, such as no need to enter profile details or remember multiple passwords for gaming accounts, and receiving in-game rewards (2/20). Finally, one participant believed that social media login is more secure than creating a dedicated game account (*"I think it's more secure rather than I use my own email and password, because it means if someone hacking the game, they cannot take my password from the game, because the game will not have my password. They only have my Facebook and then my email,"* P16).

Only a few participants (3/20) shared that they preferred *not to connect* their social media to the games out of concerns of sharing too much information (*"That is a limit I will not cross. If the games that I play with friends start asking for [social media to login to games] I'll basically force all of my friends to switch to a different game,"* P13).

4.1.3 Online game setup. In addition to exploring participants' initial authentication preferences, interviews also covered their experiences with game settings, configuring permissions, and customization of games. Participants specifically discussed security and privacy settings, sharing what they found challenging with privacy policies and suggesting the changes they thought would improve game data handling practices.

Permissions. During the interviews, participants were asked about their attitudes to game permission requests and the types of permissions they usually accept or decline during the game installation process.

The majority of them (18/20) did not allow games to collect one or more of the following permissions: photos, contacts, messages, browser history, location, files, devices, and sharing with third-party. The reasons for that included the perceptions of such permissions being too personal, concerns of excessive notifications, suspecting permissions could cause advertisements and not feeling comfortable with that, concerns of their information being collected automatically if permissions to access are provided, the lack of information and trust to game companies or developers, or apps coming from certain countries (*"There's this app which asks for wide permissions, like the addresses and stuff. I don't trust the [country] company that runs the application, so that wouldn't be okay,"* P17), or previous negative experiences (*"I had some very nasty occasion actually with the delivery app and the location, and that made me very aware of when I'm sharing my location, and that's why, that's first thing that I don't want to do, never share my location with games,"* P04).

Participants' permission concerns often related to the collection of personal data in online games, and several participants (5/20) specifically mentioned that they do not allow games to access their

media or location out of concern of compromising their physical safety (*"If they would ask my precise position [...] if there's some hacker that wants to know where I precisely am [...] I would not like to have someone on my door,"* P05).

Game Settings. Our interviews explored participants' experiences with two types of settings: general, including video resolutions or graphic and sound controls, and privacy/security settings, such as profile data controls or passwords. In particular, interviews explored participants' awareness and use of the game settings: initially and during the gameplay.

The majority of participants (17/20) modified one or more of the game settings, and the most used settings were audio, graphics, and keyboard controls. When concerning *privacy and security settings*, more than half of the participants (11/20) said they understood the privacy settings to consist of one or several of the following controls: name, flag, profile visibility, and progress data. A few participants (4/20) mentioned that they had checked privacy settings before. Others (4/20) remembered seeing privacy controls only early in the setup process and considered the Terms & Conditions or privacy policies to be privacy settings. For instance, one participant specified seeing privacy policies only through the service providing the game (e.g., Steam) and not in the game itself (*"I think it's probably before the game installation. [...] For example, Steam has privacy policies, so if I bought a game through Steam, I assume that it's the Steam privacy policy that applies. I think that is the case, yes, "* P13).

Other participants (7/20) shared that they were not sure what privacy settings meant, what controls they included, or where to find them (*"I think there are no privacy settings. I think you just decide everything, when you're selecting the character and the name. Then you can change the flag of your country if you want,"* P05). There were also a few participants (5/20) who either did not care about modifying privacy settings or did not check them at all, and 3/20 participants (P05, P06, P13) believed the games they play do not provide any privacy settings.

The interviews also focused on participants' views and preferences regarding *game customization.* Almost all of the participants (19/20) expressed that they customized or altered their game character(s) by modifying the skins, outfits and weapons. One interesting reason to modify their character in the game included camouflage purposes (*"Usually, the default player is basically only wearing panties, so you immediately notice. I just put this kind of normal trousers or dark clothes, so you can be hidden in dark,"* P05), and the lack of such camouflage could reveal certain characteristics or skills of the player, a knowledge that can be used by others.

Character and profile customization often enabled the reflection of one's self or identity within the game. Half of the participants (10/20) shared that the customizations reflected true things about themselves when customizing the game, for example, by adding their real name or gender.

Still, many participants (14/20) shared that they did alter some or all parts of their real-life identity when playing online games. For example, they would choose specific clothing styles and facial features and enhancements (makeup) (3/20), skin color (1/20), living lifestyle, and house building (1/20). The reasons for such alternations included creating a fictional character and a story in the game different from the player's real life, choosing a gender that the player prefers to be identified with (*"I don't really want to be identified as a woman, and I try not to be identified as a woman [...] I just construct my avatar, as I look like, minus the boobs, then it's generally more or less the same,"* P10) or to hide the real gender for anonymity.

Privacy Policies. Interviews also explored players' awareness of game privacy policies and their understanding of data handling practices within them, as the ambiguity of general privacy policies has been extensively reported in previous research [63].

Similarly to other contexts, many participants (11/20) saw privacy policies of online games as being too long and complicated. Most of them (9/20) would not read or think about navigating the

privacy policy and often skipped them to get started with the gameplay. One participant mentioned privacy concerns as the only reason to read a section of the privacy policy, as they were worried about *Steam* sharing their personal data with third parties (*"Except that one case where I went to the reviews, and they mentioned that they asked for a phone number and their privacy policy says that they would share information with third party publishers, effectively selling your information,"* P13).

Several participants (6/20) suggested how privacy policies can be improved, for instance, by providing its summary instead of long chunks of text, information on reasons why users' data is required, or showing relevant pop-up messages during the gameplay.

4.2 Personal data sharing in online games

The interviews explored what information participants considered private and what information they were willing to share with the games and peers. In addition, we navigated participants' anonymity preferences and why they preferred to remain anonymous when playing online games.

4.2.1 Private vs. non-private information. When discussing whether the information is private or not, participants often mentioned categories of personal data that they consider private and they are not willing to share within the game. Data categories that were considered private by participants included personally identifiable information (PII), such as real name, social security or phone number, bank card information, political or religious views (10/20), demographics including age or country (6/20), and gameplay data, for example, progress level, achievements, or info on the teammates (5/20).

Although considered private, participants discussed acceptable amounts, recipients, and purposes for these data categories. For instance, several participants (4/20) mentioned that they were okay with sharing one or more personal data types *to an extent* that would not identify them in real life (*"Email address, maybe address if payment is involved, and that's it [..] So how I play, what I play, what my system requirements are and they can ID me and that is also fine. But anything beyond that that relates directly to me as a person in the real world,"* P13) or that would not let other players to label them accordingly, for example, for supporting certain causes (*"It could be Black Lives Matter matters, or the Asian hate one or the LGBTQ+ community, they is certain cosmetic items and banners that you can put which other players in the game then see that you are supporting those,"* P13).

Similarly, different recipients for specific data types were considered more or less acceptable. For instance, third-party applications were predictably considered as a non-acceptable recipients of PII and demographic data, but one participant would not even share the gameplay progress data with them (*"The data brokers can then use it and sell it [reference to personal information] for anyone. My data should be between [me and] the game developer,"* P13). As a way to deal with such concerns, two other participants shared that since they play with fake profiles, they are not very worried about the data handling practices for games; (*"They're kind of collecting my fake personality that I made up,"* P08).

4.2.2 Community and peer interaction in online games. In addition to participant views on sharing their data with the game, another important theme is sharing with peers and the gaming community. The discussions on peer communication often revolved around their preferred communication modality (that is, video, audio or text) and the types or the amount of personal information to be shared with others.

Peer communication channels in online games. The use of specific communication channels is often related to convenience and privacy considerations. For instance, none of the participants preferred to use video streaming as a means of communication with other players, and the hesitation

often related to the high use of resources (*"For video you're already killing a lot of resources, and it's not a good idea I think,"* P18) or just lack of necessity during the gameplay.

Meanwhile, the voice chat modality was seen as more acceptable, and 14/20 participants saw it as a useful communication channel in online games. For instance, they commented on its convenience compared to typing (*"About voice, actually I think it's useful. Sometimes you can spend time on typing and you want to tell some, your teammate, what to do,"* P07).

However, several participants (6/20) considered voice chat as private and preferred to use it only with friends and not with strangers or after reaching a certain level of comfort through text (*"If I'm playing with random people on the internet, then it's only chat until I realise that OK, this is absolutely necessary that I use voice,"* P13) Indeed, seven participants had specific privacy and security concerns about using voice chat to communicate with strangers. Such concerns related to receiving threats or inappropriate language from other players, accidentally revealing personal information (*"In a multiplayer game, if they choose to be silent, you don't really know who it is, so it worries me,"* P18), or even potential recording and criminal use of players' voices (*"Maybe blackmailing someone, [...] your voice that they recorded from somewhere and making you saying some things, and when the case happens, the police [could] track it,"* P16).

As for the text chats in games, participants saw them useful, for instance, in case of the lack of screen space and for saving time in mobile games (*"I mean, for the mobile screen, [it] is really small, so we don't have time to type, it's not easy to type long words and while you type the sentence actually you already lose a lot of time on it,"* P14) or when a game does not allow other communication mediums, such as sound/audio to protect players. One participant also commented that game text chats are monitored for inappropriate language or threats, something that is possible in voice chat (*"So what happened was that somebody spoke on the voice chat something very offensive based on the characters customization. He responded to them in the chat. The company monitors chat for toxic behavior but not the voice chat. So people are telling him hey, if you like to curse, you should have used the voice chat,"* P13).

Personal information shared between players. As for the types of personal information shared with peers in online games, participants would disclose different types of information depending on whether the person they are interacting with was a friend or a stranger. For example, in the conversations with strangers, they would be okay to share or hear background noise in case of audio chats (children screaming or the use of a foreign language), weather conditions of residence area, hobbies or interests, or even reveal their real name. They would also be fine to discuss things relevant discussions to gameplay, such as game strategy (*"I would then write in that chat and try to discuss who might be the killer or the imposter,"* P02).

As for the interactions with friends, participants would share private information, as they saw online games as a channel to stay connected. For example, players living in different countries would share life events while chatting in a game. Players during COVID-19 lockdown, when face-to-face meetings were not possible, would use online games to stay in touch.

5 ANALYSIS OF DATA COLLECTED BY GAMES

We conducted an analysis of the games played by participants based on their screening survey responses. This section contributes to answering *RQ2: what are the factors that affect users to share personal data in online games?* We investigated the role of game design elements in influencing users to share their personal data in online games. Our findings also assists to address *RQ1: What are the user views on privacy and security when choosing, setting up, and playing online games?* We do this by highlighting concerns related to sharing practices of online games. We also examine

whether data practices and associated player beliefs match and identify possible misconceptions and limitations or opportunities for game designs.

To record player data collected in the games, we reviewed the collection of personal data at the advertisement, download, registration, and gameplay stages. In addition to the online games played by the study participants, the analysis also covered the most popular gaming platforms and mobile app stores that host these games (see Appendix A.7).

5.1 Games

We analyzed 21 games. Most of these games were cross-platform games (15/21), which are available on multiple devices, such as mobile devices, desktops or consoles. The most common genre of game was casual games. These are games that have fun, simple and easy-to-understand simulations. Other types of games were action Role-Playing Games and Massively Multiplayer Online games. See Table 5 (Appendix A.3) for complete game characteristics.

5.2 Collected Data Types and Practices in Games

As the first step in our analysis, we reviewed personal user data categories collected by the games and related data collection data practices. See Table 6 (Appendix A.4) for a complete list of all recorded data types. We present the results of this section as follows: (a) collected data types (what types of data is shared), (b) data collection practices and game design patters (how data is shared and concerns related to these practices).

5.2.1 Collected data types. Data types collected in our set of online games can be generally categorized as player characteristics, represented through characters or avatars and Personal Identifiable Information (PII), such as email, name, location, gender, age, mobile number, and bank details or credit card information.

Figure 1 shows personal information collected by games. It shows that the cross-platform games with complex game scenarios, such as *Final Fantasy* and *League of Legends*, that collected users' data the most amount of personal data. On the contrary, mobile casual games, such as *Cats and Soups* and *My Singing Monsters* that collected the least amount of personal data.

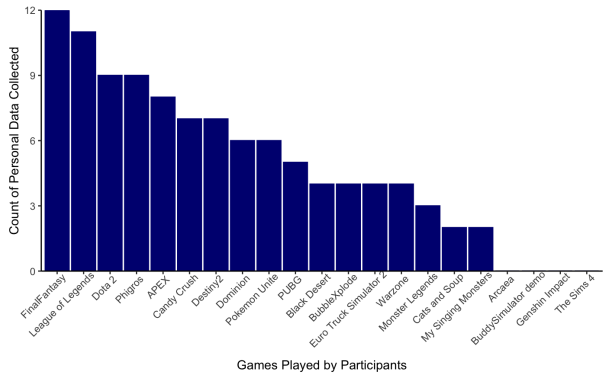

Fig. 1. Games that were listed by users in the screening survey and the number of personal data types collected by these games. Note that the count of data types is based on the information provided by the game developers.

5.2.2 Data collection practices and game design patterns. Each game was analyzed based on the design features and methods that are used to collect players' personal information. We also analyzed game privacy policies and relevant protection regulations.

Table 4 (Full table in Appendix A.4) provides a summary of the analysis. We observed that most of the games collect players' account name (15/21), email address (11/21), and age (9/21). More than half of the games restricted player age to above 13 (11/21). Most games disclose users' personal information to third-party applications (10/21). Most of the games used text (14/21) followed by voice (10/21).

The majority of games follow the General Data Protection Regulation (GDPR) (12/21), and California Consumer Act (CCPA) (9/21). This information was not available for (6/21) games.

Table 4. Summary of data types collected from games (N=21).

Category	Subcategory	Number of games	Game examples
PII	Email	11 (52%)	League of Legends
	Account Name	15 (71%)	Dota 2
	Location	7 (33%)	BubbleXplode
	Age	9 (42%)	Warzone
Communication Method	Audio	10 (47%)	APEX
	Text	14 (66%)	Black Desert
Privacy Policy Compliancy	GDPR	12 (57%)	APEX
	CCPA	9 (42%)	My Singing Monsters
	Not stated	6 (28%)	CandyCrush
Age Restriction	Above 13	11 (52%)	League of Legends
	Above 16	1 (4%)	APEX
Third-Party Regional Data	Sharing with Third-party	10 (47%)	My Singing Monsters

In addition, we collected and analyzed game design patterns that involve players sharing their personal data during stages of game installation, user age verification and authentication, social media integration, and sharing user data with third parties.

A. User prompts at the installation stage. Prior to installing online games, users are often presented with Terms & Conditions to accept before downloading a game. Usually, game platforms have a separate privacy policy from the games.

Gaming platforms such as *Steam* share some personal information with games registered on the platform. It is unclear to players what entity – the game platform or the game itself – collects what information. It is not easy to find this information since users need to read both the privacy policy of the platform and the game.

For example, *Player Unknown's Battlegrounds (PUBG) [14]* and *League of Legends [94]* can be downloaded from *Steam* and the games have their own privacy policies. If users would like to know what data was collected from them, they need to read through both *Steam's* privacy policy and those of the games.

Another example of such a case is *Destiny 2* hosted on the gaming platform Steam. At the game setup stage, *Destiny 2* requires users to accept *Steam's* Terms & Conditions, where it is unclear whether the Terms & Conditions the user agrees to are extended to the game itself (see Figure 2 in Appendix A.6).

Another common installation issue arises when games force players to install additional software. In *Destiny 2*, players are required to install an anti-cheat software *Battleye*. Otherwise, they are not allowed to continue the installation process and play the game (see Figure 3). Anti-cheat software typically can gain access to both user and device information [49].

B. User age verification. Online games often specify an age limit, disallowing minors to play the game due to the graphic content or violent game scenarios. For example, the age limit for *League of Legends* is 13+ years old. If you state your age as younger, the game instantly rejects the sign-up process, as shown in Figures 4 and 5. However, if a user tries to repeat the sign-up session with a different age, for example, 15 years old, the game immediately approves the sign-up process.

C. Linking accounts and authentication options. Some games allow players to link their social network accounts. Sometimes, this enables players to login to the game. Sometimes, it just allows to post events from the game to the social media. When social media accounts are linked to games, it is unclear what access the games have to these accounts and what information the games receive from the social media accounts.

For example, *PUBG*, a popular battle royal game, allows users to login with a guest account or use email and social media sign-ups. Users can also link multiple social media accounts in the game settings even if they had initially logged in with their email, as seen in Figures 10 and 11. *PUBG* does not specify what data is collected from such integration.

D. Incentives to integrate social media accounts. Another common design pattern in online games is encouraging users to link their social media accounts and invite others in order to receive game rewards. For example, *Monster Legends* offers exclusive rewards (Gems) for logging in with Facebook (see Figure 6) and for sharing the game with friends (up to 50K in rewards), as shown in Figure 9. This is an incentive to share their social media account details and also their contacts.

E. Sharing user data with third parties. Several games share user data with third-party apps. Several prior studies suggest that games benefit monetarily from sharing user data [112, 124].

Players may have limited control on how and when their data is shared to third parties. Even when there is a possibility to opt out from data sharing, this may not be straightforward. For example, *Monster Legends* offers an option in the app Settings for players to choose that their data should not be sold (see Figure 7). When clicking this option, players are redirected to a web page that presents the California Consumer Privacy Act (CCPA) [93]. CCPA applies to players who are residents of California in the United States. What happens to player data in other parts of the world or how players can prevent personal data sharing is not clear.

To summarize, we discovered several issues with design patterns used in popular online games. We highlighted with examples how dark designs 1) facilitate the collection of player data, 2) encourage integrating social media accounts, and 3) enable sharing player data with third-parties.

6 DISCUSSION AND IMPLICATIONS

Our goal was to explore participants views, including their understanding and concerns about sharing personal data in online games as well as the strategies they adopt to preserve their privacy. We also reviewed the games and gaming platforms participants tend to play to investigate typical personal data collection practices and associated design patterns. This section summarizes our main findings and provides design recommendations for developers and designers to support players in having higher awareness and more control over sharing their data in comparison to the current state. Finally, we discuss potential future research directions.

In line with previous research, our study shows that online games attract players with their design, graphics, and engaging game scenarios, but also as a way to connect with peers and

improve their skills [29, 58, 140]. Social factors are important both when playing games and at the stage of choosing games to play and setting them up, for instance, by connecting various social media accounts. Moreover, online games collect Personal Identifiable Information (PII) for various purposes such as social interconnectedness. This collection of information may contribute to additional risks to players' privacy, security, and even safety.

6.1 Contextual views on personal data privacy (RQ1)

Our interviews show that the privacy and sensitivity of different personal data types for players of online games depend on the context, such as game characteristics, purposes of data use, and its recipients. From the player's point of view, disclosure of personal information in online games can be both active (for example, filling in the game profile, connecting social media accounts, and sharing info with peers in communication channels) and passive, for example, by being aware of games collecting player data during the gameplay (for example, text chats or gaming performance). Players' risk awareness and privacy protection strategies also differ in these cases.

The same data can be considered both as private and not private in different contexts and depending on the potential consequences of its disclosure. For example, private information can be okay to share when players believe that by revealing it they could not be identified in real life or that other players would not stigmatize or judge them (for example, for political views, identity, or causes they support), even if these beliefs are not always true.

Although participants considered some personal information sensitive, we observed that they still shared such information with the game upon signing up. During the gameplay, participants would be mindful about disclosing personal information; however, as trust levels progressed towards the game and other players, players shared more personal information about themselves.

Game characteristics can also indicate when it is somewhat acceptable to disclose personal information. For example, participants viewed games that ask for extensive personal information to be less secure, and paid games were deemed to be more secure than free games and were expected to ensure better privacy. This finding also emerged in previous research on free vs. paid mobile apps: while participants tend to trust more in the privacy protection of paid apps and consider them more secure than those that are free, such views do not necessarily correspond to the reality [74, 113].

Monetization in games is particularly influenced by the advertisement industry. Contextual privacy factors can be addressed by existing solutions that could be applied to online games to shield players from tracking. One example is Apple's Ask App Not To Track, which allows players to block any app from collecting information that identifies the players or their device [9]. Another potential solution is contextual advertising, which is the opposite of behavioral targeting, where an advertisement matches the content of the app or webpage instead of creating user profiles [4]. Although player data is still collected in these scenarios, these may be less intrusive approaches.

6.2 Purposes of sharing personal data (RQ2)

We observed that participants' decisions to share personal data in online games are often purpose-specific and related to certain benefits of disclosure, such as receiving in-game rewards, achieving a more personalized game experience, the opportunity to reflect on one's identity, or connecting with peers.

6.2.1 Sharing for game rewards. Online games facilitate players to share more information than necessary to play. For instance, by offering generous in-game rewards to those who successfully link their social media accounts with the game or share the game with their social media contacts. Although social media integration can be convenient for players to enable a faster sign-up process, such games do not clearly show what data they gain access to or how the data is used. Our

interview data indicate that players' immediate benefits outweigh suspected privacy risks, which is consistent with earlier research on compromising privacy for convenience [2]. Players often receive no clear instructions on the consequences of linking their social network accounts to their gaming accounts, which might negatively impact their experiences when using these systems [11, 39, 57, 63]. Moreover, participants are actively encouraged and rewarded for signing up using their social media accounts. Prior work has explored the impacts of using deceptive designs and the potential harms on users' digital well-being [89], such as cognitive burden and distrust in the systems [26, 84]. Hence, game providers should consider the risks of losing longer-term engagement for short-term commercial benefits.

6.2.2 Sharing for personalization and identity representation. Personalization of player experience leads to more engagement and better game performance [22]. Players can often select from various options, for example, avatar features, environmental settings, or modifications, which are also reflected in our interviews. However, personalization requires more personal data, and players may not be aware of the potential consequences of sharing that data. Interviews show that some participants attempt to camouflage and hide some features of their characters to remain unnoticed by other players. As being unnoticed sometimes provides an advantage in games. These findings open a discussion of whether games should warn players of the potential consequences in choosing certain features when customizing their avatars, while still enjoying self-expression in the game. We suggest that these points should be incorporated into the privacy training that games could provide, that could also include information on game privacy and security configurations.

6.2.3 Sharing to connect with others. Online games are often used as communication channels or as a means to connect with others, and multiplayer games provide ample opportunities for building and maintaining interpersonal relationships [29, 140]. Our interviews show that players often share their personal data with other players even if they consider it private and sensitive, not only with the closest contacts but also even with strangers. We recognize that this may be so because participants value meaningful connections with other players, even if this results in sacrificing some of their privacy to do so, a form of "privacy paradox" to create positive interactions [12].

To achieve such meaningful connections and to avoid disclosure risks, such as bullying, discrimination threats, and the use of inappropriate language, players adopt a range of strategies to protect their privacy yet still connecting with others. One such strategy is *the choice of communication channels* that are not revealing and moderated, such as using text to chat instead of voice. While voice chats are common and very popular in online games [129], our review showed that games do not offer the same level of moderation to voice chats as they do to text chats. This can worsen the player experience or even make them stop playing [121].

Other strategies include distorting or revealing limited personal information and hiding parts of their identity when designing their characters or avatars, such as racial features, gender, clothing style, or makeup. Previous studies suggest that this strategy is also adopted to overcome security risks [11]. Gaming environments can be hostile towards women and minorities [122]. Our findings emphasize that women players felt the need to hide information about their gender, that is shown in previous research on concerns and risk perceptions of women players facing harassment in online games [32, 82]. Thus, resorting to hiding their gender by constructing their avatars without gender-revealing features or avoiding using voice chats when using a male character. Players could benefit from granular control over their data within general privacy settings. Such implementation could help to prevent unintended information disclosure by allowing players to decide for which players they want to display their full avatar, depending on how secure they feel while playing. Players could also change their voice when using voice chat to gain more control over their representation. One such existing solution in online gaming is Voicemod [126].

6.3 Player views on game data collection practices (RQ1)

We examined the security and privacy concerns of participants in online games. The data collection in itself is not always obvious to the participants. For instance, participants might be aware of the monitoring of certain in-game communication channels (text chats) but not others (voice chats). While some purposes were expected, such as sharing the date of birth for age verification, participants were often unsure about the other purposes of games collecting their data.

Players are often unaware their chats might be used and disclosed to third-party services, as our game analysis shows. In other words, once gamers unmute themselves to speak to others, they may be unaware of how their personal data is transmitted during this process. One such case is *PUBG*, a game that uses real-time voice transmission processing by sharing it with third parties to provide voice chat services to players [14] yet does not notify users while playing of this process.

Our participants were also aware of only some of the risks involved in games automatically collecting their data, such as being targeted by ads or being susceptible to security breaches.

However, other common PII risks recognized in previous research on gaming were not evident to our participants. One is impersonation, for example, a player posing as an authoritative figure pretending to assist a player in the game, only to capture their financial account information [76]. Such risks can have serious consequences beyond the gaming environment, such as someone else using stolen personal information to buy goods or taking loans in the name of the victim [88]. The same applies to the game performance risks, which also were not evident to our participants. Such risks include exploitation, for example, cheating in online games to reap rewards and inflate player levels benefiting some players over others [25, 98], and stealing or damaging user's virtual assets [98, 138], leading to gaming account compromises and financial losses.

6.4 Game design and data practices (RQ1, RQ2)

Our findings show that game design patterns, privacy and security settings, privacy policies and terms of services impact player perception of online games.

6.4.1 Privacy and security settings. Privacy and security settings were generally expected in online games, even if participants could not often recall using them or were often unsure where to find them. Moreover, participants were unsure what personal information they could modify under privacy settings, which raises questions on their awareness and understanding of what personal data control are available to them in online games. For instance, they saw their name, country flag, profile visibility, and progress data as part of the privacy settings.

However, not all games provide such settings. For example, a popular game such as *PUBG* offers no privacy-specific controls, and players can adjust their personal information in general game settings ("Player Card"). The single-player game *Sims 4* provides no privacy settings to players (See Figure 12) and redirects them to the game's Privacy Policy or EA Games User Agreement [45].

6.4.2 Privacy Policies and Terms of Service. Privacy Policies and Terms of Service (PPs and ToS) can contain essential information for user data protection. A vast amount of prior work provides recommendations to improve the readability of privacy policies and Terms & Conditions, such as using tables to summarize content, interactive visuals [105], and nudges [10]. Our interviews also reveal various player suggestions to improve them. For instance, participants preferred the summaries of data handling practices related to specific data collection purposes and their representation as pop-ups during gameplay in case of any sudden change in data practices.

6.4.3 Design Patterns. Many design patterns used in games can be considered to be *dark patterns* intended to be deceptive, misleading, or coercive to users [1, 143]. These dark patterns, for example,

force players to use paid subscriptions or click on ads [108]. Our game analysis identifies several examples of them being used.

We found that games often make it easier to sign-up with social media accounts instead of signing up just with email (Figure 13). After signing up, games provide incentives (usually in-game rewards) for linking social media accounts or sharing contact lists (Figure 9). Forcing players to perform certain steps before proceeding aligns with the taxonomy by Gary et al. on dark designs [51]. Our findings show that many potentially dark patterns are used in games. As some dark design patterns might already be considered as a default design pattern, we encourage game designers to be critical about selecting design patterns and considering their players autonomy with privacy decisions.

6.5 Design recommendations

Our findings highlight the importance of games giving players control over their own data.

Privacy settings. Contrary to participants expectations, many games examined have no dedicated menu option for privacy settings, or privacy controls are often scattered across different menus. This problem is recognized beyond the context of online gaming [38, 64, 65], and there have been various initiatives to improve the design of privacy settings. One of them is implementing privacy prompts or friendly defaults [41] that remind users if a new type of data will be collected and what are the alternatives (for example, device information, game identifier, or updating software). These alerts may increase players awareness and the sense of control, but they should be used carefully, as excessive alerts may also become disruptive [135] and negatively affect the overall gaming experience. Moreover, we observed that participants are sometimes uncertain in identifying what is included in the privacy settings; therefore, online games should both help participants to navigate such privacy controls and clearly indicate what personal data items are being shared.

Player protection mechanisms. To protect specific player populations, such as underage players, games should improve the data validation mechanisms and monitor inappropriate behavior within game communication channels. Flagging is one approach for the player community to collaborate and report online bullying in games. However, flagging largely relies on human judgment, that might be insufficient for protecting players, given the difficulty of social decision-making [68]. The YouTube Trusted Flagger program [142] provides an illustration of how to identify and empower dependable flaggers as an attempt to resolve this challenge, by offering reliable flaggers critical roles in moderation. Future research could explore how to encourage players to help other players with bullying [73]

Previous studies have suggested several machine learning techniques to examine audio data from women players to assess game toxicity [104] and to predict the quality of interactions [42]. Machine learning could also address text chat. For example, *Overwatch* (a first-person shooter game) has shown promising results in reducing chat abuse [53]. Future studies could explore the applicability and efficiency of these tools and approaches to a wider range of online games.

Avoiding player manipulation. Earlier, we discussed how popular online games employ various deceptive designs to persuade players to share their personal data. Prior studies have examined the moral principles of popular games to reveal manipulative design tendencies and investigated their wider impact [1].

The existence of dark designs could be attributed to potential misalignment of what gaming industry and society considers to be important [92]. Many dark patterns may be unlawful according to regulations such as The United States Federal Trade Commission (FTC) Act Sec. 20 that prohibits "unfair or deceptive" commercial practices [31]. However, as such designs are still widely used, existing policies should revisit the application of existing regulations and identify the gaps within

them. On the application level, we call for the design community to establish guidelines that limit the use of dark patterns and empower participants in identifying and avoiding them.

6.6 Limitations and further work

As with any qualitative study, our participants cannot represent all players. The interviews included participants with a wide range of online gaming experience, however, the participants were mostly younger tech-savvy adults, representing one of the demographics who enjoy internet gaming [52]. The interviews were conducted in Finland, and participants in other regions or demographic groups might have different views on personal data disclosure in online games.

This study offers a broad discussion on perceptions of sharing personal information in the online gaming context without focusing on specific genres or platforms. Our work also provides design implications for additional transparency and control over user data flows. Further studies could target specific design features for sharing personal data and associated player views or focus on specific game platforms and their data practices. Finally, in this study, we analyzed online games based on the data openly available to players and did not cover paid online games.

7 CONCLUSIONS

Online games collect players' personal data. In this study, we analyzed data collection practices openly available to players and reviewed designs of 21 games. We then compared our analysis with players' views on sharing their data. Our findings show that the perception of privacy in online games is contextual. It can change with time and often depends on the perceived collection purpose or attitudes towards potential data recipients. For example, in multiplayer games, players tend to share more to connect with other players, especially as their trust levels increase. Perceived benefits of disclosure affect players' decisions to share their personal data. This can be manipulated by dark patterns in games. We also identified the lack of awareness and a range of user misconceptions about game data collection practices and the potential risks of sharing personal data in online games. Based on our findings, we offer design recommendations for online games to support user awareness and equip them with the means to have more control over sharing their personal data with games or other players.

ACKNOWLEDGMENTS

This work was funded by the Academy of Finland via grant numbers: 339350, 345991, and 345992. We are grateful to all study participants for their time, experiences and insights.

REFERENCES

[1] Jacob Aagaard, Miria Emma Clausen Knudsen, Per Bækgaard, and Kevin Doherty. 2022. A Game of Dark Patterns: Designing Healthy, Highly-Engaging Mobile Games. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 438, 8 pages. https://doi.org/10.1145/3491101.3519837

[2] Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Proceedings of the 6th International Conference on Privacy Enhancing Technologies* (Cambridge, UK) *(PET'06)*. Springer-Verlag, Berlin, Heidelberg, 36–58. https://doi.org/10.1007/11957454_3

[3] AdGuard. 2023. *AdGuard*. AdGuard. Retrieved May 24, 2023 from https://adguard.com/en/welcome.html Weblink.

[4] Adjust. 2023. *Contextual advertising's comeback: Everything you need to know*. Adjust. Retrieved May 24, 2023 from https://www.adjust.com/blog/contextual-advertisings-comeback/ Weblink.

[5] Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. 2021. Security Awareness of End-Users of Mobile Health Applications: An Empirical Study. In *MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (Darmstadt, Germany) *(MobiQuitous '20)*. Association for Computing Machinery, New York, NY, USA, 125–136. https://doi.org/10.1145/3448891.3448952

[6] Apple. 2021. *Apple Privacy Policy*. Apple. Retrieved August 24, 2022 from https://www.apple.com/legal/privacy/en-ww/ Web link.
[7] Apple. 2022. *Apple Privacy Labels*. Apple. Retrieved September 9, 2022 from https://www.apple.com/privacy/labels/ Web link.
[8] Apple. 2022. *Game Center & Privacy*. Apple. Retrieved September 7, 2022 from https://www.apple.com/legal/privacy/data/en/game-center/ Web Link.
[9] Apple. 2023. *If an app asks to track your activity*. Apple. Retrieved May 24, 2023 from https://support.apple.com/en-us/HT212025#:~:text=If%20you%20choose%20Ask%20App,device%2C%20like%20your%20email%20address. Weblink.
[10] Rebecca Balebako and Lorrie Cranor. 2014. Improving App Privacy: Nudging App Developers to Protect User Privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58. https://doi.org/10.1109/MSP.2014.70
[11] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616
[12] Susanne Barth and Menno D.T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013
[13] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* 55, 3, Article 63 (feb 2022), 37 pages. https://doi.org/10.1145/3502288
[14] PUBG Battlegrounds. 2022. *Privacy Policy*. Battlegrounds. Retrieved September 12, 2022 from https://na.battlegrounds.pubg.com/pp-steam/ Web Link.
[15] Elizabeth Behm-Morawitz and Shannon Schipper. 2015. Sexing the Avatar. *Journal of Media Psychology* 28 (01 2015), 1–14. https://doi.org/10.1027/1864-1105/a000152
[16] Darrell Bethea, Robert A. Cochran, and Michael K. Reiter. 2008. Server-Side Verification of Client Behavior in Online Games. *ACM Trans. Inf. Syst. Secur.* 14, 4, Article 32 (dec 2008), 27 pages. https://doi.org/10.1145/2043628.2043633
[17] Max V. Birk, Cheralyn Atkins, Jason T. Bowey, and Regan L. Mandryk. 2016. Fostering Intrinsic Motivation through Avatar Identification in Digital Games. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 2982–2995. https://doi.org/10.1145/2858036.2858062
[18] Gaming bolt. 2021. *5 Unfortunate Cyber Attacks Against Gaming Companies*. Gaming Bolt. Retrieved August 29, 2022 from https://gamingbolt.com/5-unfortunate-cyber-attacks-against-gaming-companies Web Link.
[19] Chiara Braghin and Marilisa Del Vecchio. 2017. Is Pokémon GO Watching You? A Survey on the Privacy-Awareness of Location-Based Apps' Users. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, Turin, 164–169. https://doi.org/10.1109/COMPSAC.2017.158
[20] Stefan Brückner, Yukiko Sato, Shuichi Kurabayashi, and Ikumi Waragai. 2018. The Handling of Personal Information in Mobile Games. In *Advances in Computer Entertainment Technology*, Adrian David Cheok, Masahiko Inami, and Teresa Romão (Eds.). Springer International Publishing, Cham, 415–429.
[21] Inc. Bungie. 2023. Terms & Conditions when installing Destiny 2 on mobile platforms. https://www.bungie.net/7/en/destiny/newlight © 2023 Bungie, Inc. All rights reserved (images not licensed).
[22] Oğuz 'Oz' Buruk, Mikko Salminen, Nannan Xi, Timo Nummenmaa, and Juho Hamari. 2021. Towards the Next Generation of Gaming Wearables. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 444, 15 pages. https://doi.org/10.1145/3411764.3445785
[23] Ramnath K Chellappa and Raymond G Sin. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management* 6, 2 (2005), 181–202. https://doi.org/10.1007/s10799-005-5879-y
[24] Yu Chen, Haihan Duan, and Wei Cai. 2021. The Advertising in Free-to-Play Games: A Game Theory Analysis. In *Proceedings of the Workshop on Game Systems (GameSys '21)* (Istanbul, Turkey) *(GameSys '21)*. Association for Computing Machinery, New York, NY, USA, 7–12. https://doi.org/10.1145/3458335.3460812
[25] Ying-Chieh Chen, Jing-Jang Hwang, Ronggong Song, G. Yee, and L. Korba. 2005. Online gaming cheating and security issue. In *International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II*, Vol. 1. Association for Computing MachineryNew YorkNYUnited States, Hawthorne NY, 518–523 Vol. 1. https://doi.org/10.1109/ITCC.2005.215
[26] Ishita Chordia, Lena-Phuong Tran, Tala June Tayebi, Emily Parrish, Sheena Erete, Jason Yip, and Alexis Hiniker. 2023. Deceptive Design Patterns in Safety Technologies: A Case Study of the Citizen App. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing

Machinery, New York, NY, USA, Article 193, 18 pages. https://doi.org/10.1145/3544548.3581258
[27] Gordon Chu, Noah Apthorpe, and Nick Feamster. 2018. Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things Journal* 6, 1 (2018), 978–985. https://doi.org/10.1109/JIOT.2018.2866423
[28] Victoria Clarke and Virginia Braun. 2013. *Successful Qualitative Research: A Practical Guide for Beginners*. Sage, London, UK.
[29] Helena Cole and Mark D Griffiths. 2007. Social interactions in massively multiplayer online role-playing gamers. *Cyberpsychology & behavior* 10, 4 (2007), 575–583. https://doi.org/10.1089/cpb.2007.9988
[30] Emily Collins, Anna Cox, Caroline Wilcock, and Geraint Sethu-Jones. 2019. Digital games and mindfulness apps: comparison of effects on post work recovery. *JMIR mental health* 6, 7 (2019), e12853.
[31] Federal Trade Commission. 2021. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*. FTC. Retrieved May 25, 2023 from https://www.ftc.gov/about-ftc/mission/enforcement-authority Weblink.
[32] Amanda Cote. 2017. "I Can Defend Myself": Women's Strategies for Coping With Harassment While Gaming Online. *Games and Culture* 12 (03 2017), 136–155. https://doi.org/10.1177/1555412015587603
[33] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. 2010. Password strength: An empirical analysis. In *2010 Proceedings IEEE INFOCOM*. IEEE, San Diego, 1–9. https://doi.org/10.1109/INFCOM.2010.5461951
[34] Electronic Arts (EA). 2022. *EA Privacy Policy Agreement*. EA Games. Retrieved August 24, 2022 from http://tos.ea.com/legalapp/WEBPRIVACY/US/en/PC// Web link.
[35] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2014. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *ACM Trans. Comput. Syst.* 32, 2, Article 5 (jun 2014), 29 pages. https://doi.org/10.1145/2619091
[36] Eurogamer. 2016. *Five years ago today, Sony admitted the great PSN hack*. Eurogamer. Retrieved August 29, 2022 from https://www.eurogamer.net/sony-admitted-the-great-psn-hack-five-years-ago-today Web link.
[37] Evilwombat. 2017. *A de-bullshified version of Facebook (less ads, less clutter, less crap)*. XDA. Retrieved May 24, 2023 from https://forum.xda-developers.com/t/a-de-bullshified-version-of-facebook-less-ads-less-clutter-less-crap.3586318/ Weblink.
[38] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. https://doi.org/10.1145/2335356.2335360
[39] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. https://doi.org/10.1145/2335356.2335360
[40] Jesse Fox and Wai Yen Tang. 2017. Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies. *New Media & Society* 19, 8 (2017), 1290–1307. https://doi.org/10.1177/1461444816635778
[41] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 407, 24 pages. https://doi.org/10.1145/3491102.3517504
[42] Julian Frommel, Valentin Sagl, Ansgar E. Depping, Colby Johanson, Matthew K. Miller, and Regan L. Mandryk. 2020. Recognizing Affiliation: Using Behavioural Traces to Predict the Quality of Social Interactions in Online Games. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3313831.3376446
[43] Huiqing Fu and Janne Lindqvist. 2014. General Area or Approximate Location? How People Understand Location Permissions. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (Scottsdale, Arizona, USA) *(WPES '14)*. Association for Computing Machinery, New York, NY, USA, 117–120. https://doi.org/10.1145/2665943.2665957
[44] Huiqing Fu, Yulong Yang, Nileema Shingte, Janne Lindqvist, and Marco Gruteser. 2014. A field study of run-time location access disclosures on android smartphones. *Proc. USEC* 14 (2014), 10 pages.
[45] EA Games. 2022. *User Agreement*. EA Games. Retrieved September 13, 2022 from https://www.ea.com/legal/user-agreement Web link.
[46] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002

[47] Getmondsapk. 2023. *League of Legends MOD APK v4.1.0.6545 (Unlimited Money/Map Hack).* Getmondsapk. Retrieved May 24, 2023 from https://getmodsapk.com/league-of-legends-mod-apk/ Weblink.
[48] Google. 2020. *Google Privacy Policy.* Google. Retrieved August 24, 2022 from https://developers.google.com/games/services/terms Web link.
[49] Google. 2022. *Battleye Anti-cheat Software.* Battleye. Retrieved September 9, 2022 from https://www.battleye.com/privacy-policy/ Web link.
[50] Google. N/A. Security risks with modified (rooted) Android versions. https://support.google.com/accounts/answer/9211246?hl=en
[51] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108
[52] Mark D. Griffiths, Mark N.O. Davies, and Darren Chappell. 2004. Demographic Factors and Playing Variables in Online Computer Gaming. *CyberPsychology & Behavior* 7, 4 (2004), 479–487. https://doi.org/10.1089/cpb.2004.7.479 PMID: 15331036.
[53] Iain Harris. 2020. *Toxicity in Overwatch has seen an "incredible decrease" due to machine learning.* PC Games N. Retrieved May 25, 2023 from https://www.pcgamesn.com/overwatch/toxic-behaviour-machine-learning Weblink.
[54] Electronic Arts Inc. 2023. The Sims4 settings on mobile platform. https://www.ea.com/games/the-sims/the-sims-4 © 2023 Electronic Arts Inc. (images not licensed).
[55] Battleye Innovations. 2023. BattlEye installation wizard on mobile platform. https://www.battleye.com Copyright © 2004-2023 by BattlEye Innovations. All rights reserved (images not licensed).
[56] Privacy International. 2023. *Challenging Corporate Data Exploitation.* Privacy International. Retrieved May 24, 2023 from https://privacyinternational.org/strategic-areas/challenging-corporate-data-exploitation
[57] Qatrunnada Ismail, Tousif Ahmed, Kelly Caine, Apu Kapadia, and Michael K Reiter. 2017. To Permit or Not to Permit, That is the Usability Question: Crowdsourcing Mobile Apps' Privacy Permission Settings. *Proc. Priv. Enhancing Technol.* 2017, 4 (2017), 119–137.
[58] Signe Hannibal Jensen. 2017. Gaming as an English language learning resource among young children in Denmark. *Calico Journal* 34, 1 (2017), 1–19.
[59] Zhenhui Jiang, Cheng Heng, and Ben Choi. 2013. Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research* 24 (09 2013), 579–595. https://doi.org/10.1287/isre.1120.0441
[60] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 39–52. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang
[61] Stephen Karpinskyj, Fabio Zambetta, and Lawrence Cavedon. 2014. Video game personalisation techniques: A comprehensive survey. *Entertainment Computing* 5, 4 (2014), 211–218. https://doi.org/10.1016/j.entcom.2014.09.002
[62] Kaspersky. 2023. *Closed-source software (proprietary software).* Kaspersky. https://encyclopedia.kaspersky.com/glossary/closed-source/
[63] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538
[64] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Financial Cryptography and Data Security*, Jim Blyth, Sven Dietrich, and L. Jean Camp (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 68–79.
[65] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466
[66] Konrad Kollnig, Siddhartha Datta, and Max Van Kleek. 2021. I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 393, 8 pages. https://doi.org/10.1145/3411763.3451632
[67] Awais Rashid Kopo M. Ramokapane, Anthony C. Mazeli. 2019. Skip, Skip, Skip, Accept: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (April 2019), 209 – 227. https://doi.org/10.2478/popets-2019-0027
[68] Yubo Kou and Xinning Gui. 2021. Flag and Flaggability in Automated Moderation: The Case of Reporting Toxic Behavior in an Online Game Community. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing*

Systems (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 437, 12 pages. https://doi.org/10.1145/3411764.3445279

[69] INC. KRAFTON. 2023. PUBG logging in with social media on mobile platform. https://pubg.com/en-eu © 2023 KRAFTON, INC. PUBG IS A REGISTERED TRADEMARK OR SERVICE MARK OF KRAFTON, INC. (images not licensed).

[70] INC. KRAFTON. 2023. PUBG settings on mobile platform. https://pubg.com/en-eu © 2023 KRAFTON, INC. PUBG IS A REGISTERED TRADEMARK OR SERVICE MARK OF KRAFTON, INC. (images not licensed).

[71] INC. KRAFTON. 2023. PUBG social media linking on mobile platform. https://pubg.com/en-eu © 2023 KRAFTON, INC. PUBG IS A REGISTERED TRADEMARK OR SERVICE MARK OF KRAFTON, INC. (images not licensed).

[72] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. 2023. Surveilling the gamers: Privacy impacts of the video game industry. *Entertainment Computing* 44 (2023), 100537. https://doi.org/10.1016/j.entcom.2022.100537

[73] Haewoon Kwak, Jeremy Blackburn, and Seungyeop Han. 2015. Exploring Cyberbullying and Other Toxic Behavior in Team Competition Online Games. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 3739–3748. https://doi.org/10.1145/2702123.2702529

[74] Pierre Laperdrix, Naif Mehanna, Antonin Durey, and Walter Rudametkin. 2022. The Price to Play: A Privacy Analysis of Free and Paid Games in the Android Ecosystem. In *Proceedings of the ACM Web Conference 2022* (Virtual Event, Lyon, France) *(WWW '22)*. Association for Computing Machinery, New York, NY, USA, 3440–3449. https://doi.org/10.1145/3485447.3512279

[75] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann, Cambridge, USA.

[76] Eunjo Lee, Jiyoung Woo, Hyoungshick Kim, and Huy Kang Kim. 2018. No Silk Road for Online Gamers! Using Social Network Analysis to Unveil Black Markets in Online Games. In *Proceedings of the 2018 World Wide Web Conference* (Lyon, France) *(WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1825–1834. https://doi.org/10.1145/3178876.3186177

[77] Namyeon Lee and Ohbyung Kwon. 2015. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications* 42, 5 (2015), 2764–2771. https://doi.org/10.1016/j.eswa.2014.11.031

[78] Yao Li, Yubo Kou, Je Seok Lee, and Alfred Kobsa. 2018. Tell me before you stream me: Managing information disclosure in video game live streaming. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–18. https://doi.org/10.1145/3274376

[79] Anthony Lieuallen. 2023. *Greasemonkey*. Greasemonkey. Retrieved May 24, 2023 from https://addons.mozilla.org/en-US/firefox/addon/greasemonkey/ Weblink.

[80] Anthony Lieuallen. 2023. *WhatsApp Plus*. Whatsapp plus. Retrieved May 24, 2023 from https://www.waplus.me messaging app for Android.

[81] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 501–510. https://doi.org/10.1145/2370216.2370290

[82] Jennifer Malkowski and TreaAndrea M. Russworm. 2017. *Gaming Representation: Race, Gender, and Sexuality in Video Games*. Indiana University Press, Indiana, USA.

[83] Kirsten Martin and Katie Shilton. 2012. Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. *Washington University Journal of Law & Policy* 40 (2012), 257–277.

[84] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (nov 2019), 32 pages. https://doi.org/10.1145/3359183

[85] Microsoft. 2022. *Microsoft Privacy Statement*. Microsoft. Retrieved August 24, 2022 from https://privacy.microsoft.com/en-gb/privacystatement Web link.

[86] ModTheSims. 2023. *Mod The Sims is one of the largest Sims 2, Sims 3 and Sims 4 custom content websites*. ModTheSims. Retrieved May 24, 2023 from https://modthesims.info Weblink.

[87] Nurul Momen, Sven Bock, and Lothar Fritsch. 2020. Accept-maybe-decline: introducing partial consent for the permission-based access control model of android. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*. Association for Computing Machinery, New York, NY, USA, 71–80. https://doi.org/10.1145/3381991.3395603

[88] Luciano Mondragon. 2021. *Fsecure: 5 tips for secure gaming.* Fsecure. Retrieved May 25, 2023 from https://blog.f-secure.com/secure-gaming-tips/ Weblink.

[89] Alberto Monge Roffarello and Luigi De Russis. 2022. Towards Understanding the Dark Patterns That Steal Our Attention. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 274, 7 pages. https://doi.org/10.1145/3491101.3519829

[90] Christian Montag, Bernd Lachmann, Marc Herrlich, and Katharina Zweig. 2019. Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International journal of environmental research and public health* 16, 14 (2019), 2612. https://doi.org/10.3390/ijerph16142612.

[91] Lisa Nakamura. 2013. *"It's a Nigger in Here! Kill the Nigger!" User-Generated Media Campaigns Against Racism, Sexism, and Homophobia in Digital Games.* Vol. 6. Wiley Online Library, Online, 21–15. https://doi.org/10.1002/9781444361506.wbiems159

[92] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces. *Queue* 18, 2 (may 2020), 67–92. https://doi.org/10.1145/3400899.3400901

[93] State of California Department of Justice. 2022. *California Consumer Privacy Act (CCPA).* Rob Bonta. Retrieved September 6, 2022 from https://oag.ca.gov/privacy/ccpa Web Link.

[94] League of Legends. 2021. *Privacy Notice.* Riot Games. Retrieved September 12, 2022 from https://www.riotgames.com/en/privacy-notice Web Link.

[95] Office of the Privacy Comissioner of Canada. 2019. *Gaming and personal information: playing with privacy.* Office of the Privacy Comissioner of Canada. Retrieved September 7, 2022 from https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/gd_gc_201905/ Web Link.

[96] Sanela Osmanovic and Loretta L Pecchioni. 2019. Playing with words: The experience of self-disclosure in intergenerational gaming. In *Human Aspects of IT for the Aged Population. Social Media, Games and Assistive Environments: 5th International Conference, ITAP 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26-31, 2019, Proceedings, Part II 21.* Springer, Orlando, FL, USA, 189–203. https://doi.org/10.1007/978-3-030-22015-0_15

[97] Dennis Pagano and Walid Maalej. 2013. User feedback in the appstore: An empirical study. In *2013 21st IEEE international requirements engineering conference (RE).* IEEE, Brazil, 125–134. https://doi.org/10.1109/RE.2013.6636712

[98] Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, Mohammad Hammoudeh, and Gregory Epiphaniou. 2019. *Security in Online Games: Current Implementations and Challenges.* Springer International Publishing, Cham, 367–384.

[99] Mario Passalacqua, Marc Fredette, Lennart E Nacke, Robert Pellerin, Pierre-Majorique Leger, et al. 2021. Should Gamification be Personalized? A Self-deterministic Approach. *AIS Transactions on Human-Computer Interaction* 13, 3 (2021), 265–286.

[100] We PC. 2022. *Google Play Games.* Google. Retrieved September 5, 2022 from https://play.google.com/store/apps/details?id=com.google.android.play.games&hl=en&gl=US Web Link.

[101] Google Play. 2020. *Google Play Games Services Terms of Service.* Google. Retrieved August 24, 2022 from https://developers.google.com/games/services/terms Web link.

[102] PlayStation. 2021. *PlayStation Privacy Policy.* PlayStation. Retrieved August 24, 2022 from https://www.playstation.com/en-fi/privacy-security-safety/#dataprivacy Web link.

[103] Lenin Ravindranath, Suman Nath, Jitendra Padhye, and Hari Balakrishnan. 2014. Automatic and Scalable Fault Detection for Mobile Applications. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services* (Bretton Woods, New Hampshire, USA) *(MobiSys '14)*. Association for Computing Machinery, New York, NY, USA, 190–203. https://doi.org/10.1145/2594368.2594377

[104] Elizabeth Reid, Regan L Mandryk, Nicole A Beres, Madison Klarkowski, and Julian Frommel. 2022. "Bad Vibrations": Sensing Toxicity From In-Game Audio Features. *IEEE Transactions on Games* 14, 4 (2022), 558–568.

[105] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 66, 12 pages. https://doi.org/10.1145/3411764.3445465

[106] Inc. Riot Games. 2023. Age verification failed if age is less than 12 years old when installing League of Legends on mobile platform. https://www.leagueoflegends.com/en-us/ ™ & © 2023 Riot Games, Inc. League of Legends and all related logos, characters, names and distinctive likenesses thereof are exclusive property of Riot Games, Inc. All Rights Reserved (images not licensed).

[107] Inc. Riot Games. 2023. Age verification when installing League of Legends on mobile platform. https://www.leagueoflegends.com/en-us/ ™ & © 2023 Riot Games, Inc. League of Legends and all related logos, characters, names and distinctive likenesses thereof are exclusive property of Riot Games, Inc. All Rights Reserved (images not licensed).

[108] Yvonne Rogers, Margot Brereton, Paul Dourish, Jodi Forlizzi, and Patrick Olivier. 2021. The Dark Side of Interaction Design. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 152, 2 pages. https://doi.org/10.1145/3411763.3450397

[109] Benjamin Sanders, Vivian Chen, Daniel Zahra, Paul Dowland, Shirley Atkinson, Maria Papadaki, and Steven Furnell. 2010. Online Addiction: Privacy Risks in Online Gaming Environments. In *Proceedings of the International Conference on Management of Emergent Digital EcoSystems* (Bangkok, Thailand) *(MEDES '10)*. Association for Computing Machinery, New York, NY, USA, 114–121. https://doi.org/10.1145/1936254.1936275

[110] Jessica Schroers. 2019. I have a Facebook account, therefore I am–authentication with social networks. *International Review of Law, Computers & Technology* 33, 2 (2019), 211–223.

[111] Magy Seif El-Nasr and Erica Kleinman. 2020. Data-Driven Game Development: Ethical Considerations. In *Proceedings of the 15th International Conference on the Foundations of Digital Games* (Bugibba, Malta) *(FDG '20)*. Association for Computing Machinery, New York, NY, USA, Article 64, 10 pages. https://doi.org/10.1145/3402942.3402964

[112] Ellen Seiter. 2004. The internet playground. In *Toys, games, and media*. Routledge, New Jersey, 93–94.

[113] Suranga Seneviratne, Harini Kolamunna, and Aruna Seneviratne. 2015. A Measurement Study of Tracking in Paid Mobile Applications. In *Proceedings of the 8th ACM Conference on Security; Privacy in Wireless and Mobile Networks* (New York, New York) *(WiSec '15)*. Association for Computing Machinery, New York, NY, USA, Article 7, 6 pages. https://doi.org/10.1145/2766498.2766523

[114] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421

[115] Social Point S.L. 2018. Logging in with Facebook account on Monster Legends mobile platform. https://www.monsterlegendsgame.com © 2018 Social Point S.L. All Rights Reserved. Social Point, Social Point logo, the game names and related marks are the trademarks of Social Point S.L. or related entities. All other trademarks are the property of their respective owners (images not licensed).

[116] Social Point S.L. 2018. Monster Legends link to CCPA on mobile platform. https://www.monsterlegendsgame.com © 2018 Social Point S.L. All Rights Reserved. Social Point, Social Point logo, the game names and related marks are the trademarks of Social Point S.L. or related entities. All other trademarks are the property of their respective owners (images not licensed).

[117] Social Point S.L. 2018. Monster Legends settings view on mobile platform. https://www.monsterlegendsgame.com © 2018 Social Point S.L. All Rights Reserved. Social Point, Social Point logo, the game names and related marks are the trademarks of Social Point S.L. or related entities. All other trademarks are the property of their respective owners (images not licensed).

[118] Social Point S.L. 2018. Monster Legends social settings on mobile platform. https://www.monsterlegendsgame.com ©2018 Social Point S.L. All Rights Reserved. Social Point, Social Point logo, the game names and related marks are the trademarks of Social Point S.L. or related entities. All other trademarks are the property of their respective owners (images not licensed).

[119] Steam. 2022. *Steam Privacy Policy Agreement*. Steam. Retrieved August 24, 2022 from https://store.steampowered.com/privacy_agreement/ Web link.

[120] Alexander Streicher and Jan D. Smeddinck. 2016. *Personalized and Adaptive Serious Games*. Springer International Publishing, Cham, 332–377. https://doi.org/10.1007/978-3-319-46152-6_14

[121] Otto Söderlund. 2022. *Why Games Need Better Voice Chat Moderation*. Speechly. Retrieved May 24, 2023 from https://www.speechly.com/blog/why-games-need-better-voice-chat-moderation Weblink.

[122] Wai Yen Tang and Jesse Fox. 2016. Men's harassment behavior in online video games: Personality traits and game factors. *Aggressive behavior* 42, 6 (2016), 513–521.

[123] April Tyack and Peta Wyeth. 2021. "The Small Decisions Are What Makes it Interesting" Autonomy, Control, and Restoration in Player Experience. *Proceedings of the ACM on Human-Computer Interaction* 5, CHI PLAY (2021), 1–26. https://doi.org/10.1145/3474709

[124] Narseo Vallina-Rodriguez, Jay Shah, Alessandro Finamore, Yan Grunenberger, Konstantina Papagiannaki, Hamed Haddadi, and Jon Crowcroft. 2012. Breaking for Commercials: Characterizing Mobile Advertising. In *Proceedings of the 2012 Internet Measurement Conference* (Boston, Massachusetts, USA) *(IMC '12)*. Association for Computing Machinery, New York, NY, USA, 343–356. https://doi.org/10.1145/2398776.2398812

[125] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, and Nigel Shadbolt. 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5208–5220.

[126] Voicemod. 2023. *Free voice changer for PC.* Voicemod. Retrieved May 24, 2023 from https://www.speechly.com/blog/why-games-need-better-voice-chat-moderation Weblink.
[127] Proton VPN. 2020. *The complete guide to online gaming privacy.* Proton VPN. Retrieved August 29, 2022 from https://protonvpn.com/blog/online-gaming-privacy/ Web link.
[128] Nevena Vratonjic, Mohammad Hossein Manshaei, Jens Grossklags, and Jean-Pierre Hubaux. 2013. *Ad-Blocking Games: Monetizing Online Content Under the Threat of Ad Avoidance.* Springer Berlin Heidelberg, Berlin, Heidelberg, 49–73. https://doi.org/10.1007/978-3-642-39498-0_3
[129] Greg Wadley, Marcus Carter, and Martin Gibbs. 2015. Voice in Virtual Worlds: The Design, Use, and Influence of Voice Chat in Online Play. *Human–Computer Interaction* 30, 3-4 (2015), 336–365. https://doi.org/10.1080/07370024.2014.987346 arXiv:https://doi.org/10.1080/07370024.2014.987346
[130] Isabel Wagner, Ying He, Duska Rosenberg, and Helge Janicke. 2016. User interface design for privacy awareness in eHealth technologies. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).* IEEE, Las Vegas, USA, 38–43. https://doi.org/10.1109/CCNC.2016.7444728
[131] John Walker. 2011. LulzSec over, Release Battlefield Heroes Data. https://www.rockpapershotgun.com/lulzsec-over-release-battlefield-heroes-data
[132] Na Wang, Heng Xu, and Jens Grossklags. 2011. Third-Party Apps on Facebook: Privacy and the Illusion of Control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '11).* Association for Computing Machinery, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/2076444.2076448
[133] Tian Wang and Masooda Bashir. 2021. Gaming Apps' and Social Media Partnership: A Privacy Perspective. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Springer International Publishing, Cham, 475–487.
[134] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '10).* Association for Computing Machinery, New York, NY, USA, 162–175. https://doi.org/10.1145/1866307.1866327
[135] Tilo Westermann, Sebastian Möller, and Ina Wechsung. 2015. Assessing the Relationship between Technical Affinity, Stress and Notifications on Smartphones. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct* (Copenhagen, Denmark) *(MobileHCI '15).* Association for Computing Machinery, New York, NY, USA, 652–659. https://doi.org/10.1145/2786567.2793684
[136] Whatsapp. N/A. About unofficial apps. https://faq.whatsapp.com/1217634902127718
[137] Nelson Wong, Anthony Tang, Ian Livingston, Carl Gutwin, and Regan Mandryk. 2009. Character Sharing in World of Warcraft. In *ECSCW 2009*, Ina Wagner, Hilda Tellioğlu, Ellen Balka, Carla Simone, and Luigina Ciolfi (Eds.). Springer London, London, 343–362.
[138] Jiyoung Woo and Huy Kang Kim. 2012. Survey and Research Direction on Online Game Security. In *Proceedings of the Workshop at SIGGRAPH Asia* (Singapore, Singapore) *(WASA '12).* Association for Computing Machinery, New York, NY, USA, 19–25. https://doi.org/10.1145/2425296.2425300
[139] Jeff Yan and Brian Randell. 2005. A Systematic Classification of Cheating in Online Games. In *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support for Games* (Hawthorne, NY) *(NetGames '05).* Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/1103599.1103606
[140] Nick Yee. 2006. The demographics, motivations, and derived experiences of users of massively multi-user online graphical environments. *Presence: Teleoperators and virtual environments* 15, 3 (2006), 309–329. https://doi.org/10.1162/pres.15.3.309
[141] Nick Yee. 2007. Motivations for Play in Online Games. *Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society* 9 (01 2007), 772–5. https://doi.org/10.1089/cpb.2006.9.772
[142] Youtube. 2022. *About the YouTube Trusted Flagger program.* Google. Retrieved May 25, 2023 from https://support.google.com/youtube/answer/7554338?hl=en Weblink.
[143] José Pablo Zagal, Staffan Björk, and Chris Lewis. 2013. Dark patterns in the design of games. In *FDG.* Foundations of Digital Games 2013, Chania, Greece, 8 pages.

A APPENDIX

A.1 Screening survey

Privacy Notice and Consent form signed before proceeding to the screening survey

A.1.1 Online Games and Personal Information.

(1) Do you play online games? (Required)
   - □ Yes - proceed
   - □ No - not eligible

(2) In what country do you currently reside? (Required)
(3) What is your online gaming experience in years? *Please, enter the number of years*
(4) In the last month, how often did you play online games?
   - □ More than once a day
   - □ One a day
   - □ Once a week
   - □ 1-2 times a month
   - □ Rarely or never

(5) Which genre(s) of games do you play the most? Please, select up to 3:
   - □ Battle Royale (Fortnite, APEX, PUBG...)
   - □ FPS/Shooter (CSGO, COD, The Division, Destiny 2...)
   - □ Simulation (Racing, Flight, Sims...)
   - □ MOBA (DOTA 2, LOL, Heroes of the Storm...)
   - □ MMO (WOW, TESO, Guild Wars 2, FFXIV...)
   - □ Action RPG (Kingdom Come, The Witcher 3, Assissin's Creed Origins/Odyssey...)
   - □ Strategy/Management/RTS (Starcraft 2, Total War, Civilization...)
   - □ Adventure Games (Portal, The Witness...)
   - □ Platform Games/MetroidvaniaDungeon crawlers (Celeste, Super Meat Boy, Crosscode...)
   - □ Card Games (Heathstone, Gwent, Artifact, Duelyst...)
   - □ Party Games (Overcooked, Castle Crashers, Gang Beasts...)
   - □ Sport Games (FIFA, NFL, NBA 2K...)
   - □ Rhythm Games (Guitar Hero...)
   - □ Casual Games (Solitaire, Candy Crush, Hill CLimb...)
   - □ Sandbox/Open World/Building Games (Minecraft, Plant Coaster...)

(6) Styles of play in your games:
   - □ Social media games (Farmville)
   - □ Location-based games (PokemonGo)
   - □ Console games
   - □ Browser games
   - □ Player versus environment (PvE)
   - □ Player versus player (PvP) or multi-player
   - □ Simulation games
   - □ Other, please, specify:

(7) Please, write down the names of games that you play? (Required)
(8) Did you ever pay for an online game or game add-ons or assets?
   - □ Yes
   - □ No
   - □ I'm not sure

(9) What devices do you own and do you use them for playing games? (Please, choose all that apply)

List of devices	Used to play games	Do not use to play games	Do not own
Smartphone	☐	☐	☐
Keypad phone (phone with a physical keyboard).	☐	☐	☐
Laptop	☐	☐	☐
Desktop computer	☐	☐	☐
Tablet	☐	☐	☐
Game console	☐	☐	☐
AR/VR set	☐	☐	☐
Others, specify	☐	☐	☐

(10) Do you have social media profiles? If yes, which ones and how often do you use them?

Social media	Daily	Weekly	Less often	Don't use	Don't have
Facebook	☐	☐	☐	☐	☐
Instagram	☐	☐	☐	☐	☐
Tik Tok	☐	☐	☐	☐	☐
WeChat	☐	☐	☐	☐	☐
Whatsapp	☐	☐	☐	☐	☐
Snapchat	☐	☐	☐	☐	☐
QQ	☐	☐	☐	☐	☐
VK	☐	☐	☐	☐	☐
Telegram	☐	☐	☐	☐	☐
Odnoklassniki	☐	☐	☐	☐	☐
Others	☐	☐	☐	☐	☐

(11) Are you a professional gamer? That is, do you make money by competing against other gamers?
- ☐ Yes
- ☐ No
- ☐ I'm not sure

(12) Have you ever stream your gameplay (recorded gaming and shared it with others)?
- ☐ Yes, I stream gameplay for money

- ☐ Yes, I stream gameplay (non-monetary)
- ☐ No, I do not stream gameplay

(13) In what languages do you play games?

(14) Is English your first language? (Required)
- ☐ Yes
- ☐ No, Please enter your first language (s):

(15) How old are you?
- ☐ 18 - 30
- ☐ 31 - 40
- ☐ 41 - 50
- ☐ 51 - 60
- ☐ 61 - 70
- ☐ Older than 71

(16) What is your gender? (please select option that best applies)
- ☐ Male
- ☐ Female
- ☐ Nonbinary
- ☐ Prefer not to say
- ☐ Prefer to self-describe

(17) What is your highest level of education?
- ☐ Basic education (school)
- ☐ Upper secondary education (general upper secondary education or vocational education and training)
- ☐ Higher education provided by universities and universities of applied sciences
- ☐ Other, please, specify:

(18) Do you reside in the country differently from the country you grew up in?
- ☐ Yes
- ☐ No
- ☐ Prefer not to answer

(19) Would you need someone to help you download new software to your computer or an app to your phone?
- ☐ Yes
- ☐ No
- ☐ I'm not sure

(20) How do you prefer to be informed about whether you have been selected for the interview? Click all that apply.
- ☐ By email, please, provide you email address:
- ☐ By phone, please, provide your phone number:

End of the survey

A.2 Semi-structured interview guide

Hello. Thank you for answering the survey and your interest to participate in this interview, we greatly appreciate your help with our research. My name is [..] and I will conduct this interview. The interview will last around 40 minutes and will be audio recorded. The recording is to accurately record the information you provide and will be used for transcription purposes only. After the transcription, we will destroy the audio recording. If you don't wish to be recorded you can stop the interview. However, incomplete interviews will not be compensated. If you feel any discomfort, please, let me know and we

could pause or stop the interview. Please, do not name any third parties. Do you have any questions? You can have a break any time during the interview. Are you ready to start? Let me give you some introduction to our research first. We are interested to learn more about online games, what factors influence players' experience - both negative and positive - and what are the underlying data flow in online games. Let's start with a few questions about yourself and your gaming experience.

A.2.1 ***Ice breaker and introductory questions.***

(1) Can you describe games you like to play in a few words?
(2) Where do you usually play games (home, work, with friends)? Do you play alone or with other people?
(3) How do you choose the games, what do you pay attention to?
(4) What makes the game trustworthy to play for you? Could you give some examples?
(5) Do you consider the privacy and security of your information when you choose games to play?

A.2.2 ***Personalisation/Customization in games.***

(1) Do you think the game gets harder as you play it?
  (a) (If yes) Do you expect it to change based on your performance or other things you do?
  (b) (If no) For the games that do, do you think it's a good or a bad thing?
(2) Do you think games collect information about your progress?
  (a) (If yes) Can you provide examples?
  (b) How do you feel about this information being collected? Do you have any concerns about your performance data being collected? What do you think happens to it? Is there any information about your progress that you don't want to share with the game?
(3) Can you customize the game you play, can you change/choose anything there?
  (a) (If no) Would you like that? Why? [hypothetical sc enario] If you could, what would you like to change in the games you play?
  (b) (If yes) Could you tell me more, what can you change and why? For example, set an avatar/profile picture, customise your character or set any notifications (for example, when you get lives to play or other players start a game)?
(4) When you change the game elements, what are things you keep true about yourself and what not? Follow up: why?
(5) What information do you consider private and what is not when you play online games? Could you give me any examples?
(6) Do you spend money on games?
  (a) (If no) What do you think about it? What is good/ bad about it?
  (b) (If yes) How? What do you spend money on? How do you do that (bank card, Paypal, Apple pay, etc)? Do you think games store your bank information?
  (c) (If yes) What kind of information do you think they store? E.g., serial number, CVC, expiry date.
  (d) (If yes) What are your thoughts about games having access and storing such data? What are the good and bad think about it?

A.2.3 ***Permissions and PPs.***

(1) If we take one step back when you installed the game, did it ask for any permissions - access to your device or your data?
  (a) Where do you think these permissions are from? Are they from the device (OS) or from the game?
  (b) If you remember, could you name them? Why do you think the game asks for them?

(c) If you don't remember, what do you think is being collected? And why?
(d) Do you have any permissions you don't want to allow? Could you explain why?
(e) Do you think the game asks for more permissions than it needs?
(2) Does the game you play have a privacy policy (the description of data collection practices)?
(a) (If yes) Did you read it? If not, why? If yes, what is in it? Was it clear, did you have any remaining questions after reading it or doubts?
(b) (If no) Would you expect it to be there? What do you think it should have in it?

A.2.4 ***Game settings.***

(1) Did you ever check the game settings?
(a) (If no) What would you expect to be there? [If not mentioned] Would you expect anything regarding your personal data?
(b) (If yes) What was there? Did you change anything? (If not mentioned) What's about privacy settings, do you usually check them? Do you know how to find them?
(2) Where do you get game updates or extensions? Do you trust the sources you use to get updates?
(3) What makes a source trustworthy in your opinion?

A.2.5 ***The use of communication channels in the game.***

(1) Did you ever play games with other players (multiplayer mode)? Was there an opportunity to interact with other players?
(a) (If yes) Did you interact with them in the game? For example, in a text and voice chat, video calls, or posted on their profiles? What do you think about such game features, do you prefer having them? Why? Do you share anything about yourself? What do you share about yourself?
(b) (If no) Would you like to have it? Why or why not?
(2) Have you ever clicked any links shared in the chatbox? Why or why not?
(3) Do you know what is a bot? [Interviewer can explain here what bots mean] Did you ever encounter or you think you might have encountered a bot in a game? (if yes) if yes: Did bots affect your gaming experience? In what ways?

A.2.6 ***Account creation and online identity.***

(1) How do you create an account in the game you play? What information is asked about you? Are you comfortable providing it?
(2) Do you use your real in the game? Do you use a nickname/username, how do you choose it? Do you reveal your real name to other players? Was it always like this or did it change over time? (If changed) Why? What influenced that change?
(3) Do you want to be anonymous? How do you make yourself anonymous? Follow up: can you give examples of what would make you feel anonymous.
(4) What do you think about other players being anonymous? Does that affect you in any way?
(5) Does anyone else know the password to your account? Why and why not.
(6) Has your account ever been hacked?
(a) (if yes) by whom?
(b) (if no) Do you use any security measures to protect yourself online? Could you provide examples.

A.2.7 ***Social media questions.***

(1) Do you connect your social media account to the games you play?
(a) (if yes) What accounts and for what reason?

(b) (if mentioned - log in using social media) Did the game ask for any permissions? (If yes) Do you think the game can access or even control your account activity? What are the good and bad things about it?
(2) Do you invite your friends on social media to play games with you?
(3) Do you get any rewards when you connect your social media account?

A.2.8 ***Game rules.***

(1) Do you know if there is anything you are advised not to do in games, are there any rules on your gaming behaviour?
(a) (if no) If there were such rules, would you expect the game to know about breaking those rules?
(b) (if yes) Do you know if anything happens if you break those rules, what do you think could happen?
(2) Did you ever use cheats or other ways to gain an advantage in games?
(3) What about others doing it, what do you think about that? Did you have any negative experiences?

A.2.9 ***Data collected in the game.***

(1) Do you think the games you play collect any information about yourself?
(a) (if yes) What do you think it collects? Do you consider it sensitive? What's about any personal information?
(2) What information you don't want the game to collect?
(3) Do you think the game you play collects more information than it says or needs?
(4) What would it be and for what purpose? How long do you think your data is kept for? what happens to your data when you delete your account? Were you informed about that?
(a) (if yes) how were you informed?
(b) (if no) how would you wish you were informed about this?

A.2.10 ***Final remarks.***

(1) Is there anything you would like to tell me that I didn't ask about?
(2) Is there anything you expected me to ask?
(3) Did we discuss any topics that were of interest to you?

End of the interview guide

A.3 Full list of game characteristics

Table 5. Characteristics of online games played by interview participants (N=21). We use the following abbreviations: Massively Multiplayer Online Games (MMOs) and Role-Playing Games (RPGs).

Category	Subcategory	Number of games	Examples
Platform	Mobile only	3 (14%)	Candy Crush
	Desktop only	3 (14%)	Dota 2
	Cross-platform	15 (71%)	PUBG
	Console only	0 (0%)	N/A
Genre	Battle Royale	3 (14%)	Warzone, PUBG
	Simulation	4 (19%)	Sims 4
	MMO	2 (9%)	Destiny 2, Black Desert
	Action RPG	3 (14%)	Monster Legends
	Rhythm Games	2 (9%)	Phigros, Arcaea
	Casual Games	4 (19%)	Candy Crush
Player Mode	Single player	7 (28%)	Sims 4
	Multi-player	15 (71%)	League of Legends
Purchase	Free	17 (80%)	Arcaea
	Fully or partially paid	4 (19%)	Black Desert

A.4 Game handling of personal information

Table 6. Data types collected from games (N=21).

Category	Subcategory	Number of games	Game examples
PII	Email	11 (52%)	League of Legends
	Account Name	15 (71%)	Dota 2
	Location	7 (33%)	BubbleXplode
	Gender	4 (19%)	Euro Truck Simulator 2
	Mobile Number	3 (14%)	FinalFantasy
	Age	9 (42%)	Warzone
	Bank Details	6 (28%)	FinalFantasy
Communication Method	Video	0 (0%)	N/A
	Audio	10 (47%)	APEX
	Text	14 (66%)	Black Desert
	Not Available	4 (19%)	BudySimulator
Privacy Policy Compliancy	CCPA	9 (42%)	My Singing Monsters
	GDPR	12 (57%)	My Singing Monsters
	Not stated	6 (28%)	CandyCrush
Age Restriction	Less than 13	6 (28%)	Phigros
	Above 13	11 (52%)	League of Legends
	Above 16	1 (4%)	APEX
	Above 18	2 (9%)	Black Desert
Third-Party Regional Data	Sharing with Third-Party	10 (47%)	My Singing Monsters
	Not sharing	2 (9%)	League of Legends
	Not stated	6 (28%)	Arcaea

A.5 Full demographic characteristics of the interview sample

Table 7. Demographic characteristics of interview participants (N=20).

Attribute	Range	Sample size
Gender	Female	8 (40%)
	Male	11 (55%)
	Prefer not to say	1 (5%)
Age	18 - 30	13 (65%)
	31 - 40	5 (25%)
	41 - 50	2 (10%)
Current residence varies from place of birth	Yes	14 (70%)
	No	6 (30%)
Assistance needed to download new software to device(s)	No	18 (90%)
	I'm not sure	1 (5%)
	Yes	1 (5%)
Level of English language proficiency	Intermediate	1 (5%)
	Advanced	17 (85%)
	Native or bilingual proficiency	2 (10%)
Education	Higher education	19 (95%)
	Upper Secondary	1 (5%)
First Language	Arabic	1 (5%)
	Belarusian	1 (5%)
	Chinese	3 (15%)
	Finnish	5 (5%)
	Italian	1 (5%)
	Nepali	1 (5%)
	Pashto	1 (5%)
	Russian	3 (15%)
	Spanish	1 (5%)
	Turkish	2 (10%)
	Vietnamese	1 (5%)
Game Languages	Chinese	3 (15%)
	English	19 (95%)
	Finnish	2 (10%)
	Hindi	1 (5%)
	Russian	2 (10%)
	Spanish	1 (5%)
	Turkish	1 (5%)

Table 8. Table illustrates participant experiences in years, the genre and styles of the games they played.

Participant	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Experience (years)	10	22	17	10	27	6	14	16	18	10	2	6	12	14	15	2	20	5	10	25
Genre																				
Battle Royal					✓	✓						✓	✓		✓			✓		
FPS/Shooter	✓	✓		✓			✓		✓					✓	✓					
Simulation	✓	✓		✓			✓		✓								✓		✓	
MOBA (Multiplayer Online Battle Arena)									✓					✓						
MMO (Massively Multiplayer Online)			✓			✓					✓									
Action RPG	✓		✓			✓	✓	✓				✓		✓	✓	✓			✓	✓
Strategy						✓				✓										
Adventure Games			✓				✓					✓								
Platform Games															✓					
Card Games											✓									
Party Games															✓	✓				
Sport Games	✓														✓			✓		
Rhythm Games														✓		✓			✓	
Casual Games		✓		✓						✓			✓				✓	✓	✓	
Sandbox/Open World/Building Games		✓																		
Styles																				
Social Media		✓		✓						✓	✓			✓		✓	✓		✓	
Location-based													✓							
Console	✓		✓									✓		✓	✓	✓				
Browser		✓					✓										✓		✓	
PvE (Player Versus Environment)	✓	✓	✓			✓		✓				✓			✓	✓				✓
PvP (Player Versus Player)	✓		✓		✓	✓		✓	✓		✓	✓	✓		✓			✓		✓
Simulation		✓		✓			✓		✓										✓	✓
Others						✓								✓			✓	✓		

A.6 Examples from games

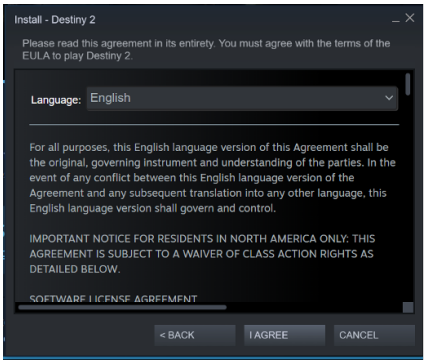

Fig. 2. Prior to installing *Destiny 2* on *Steam* players are required to accept Terms & Conditions [21].

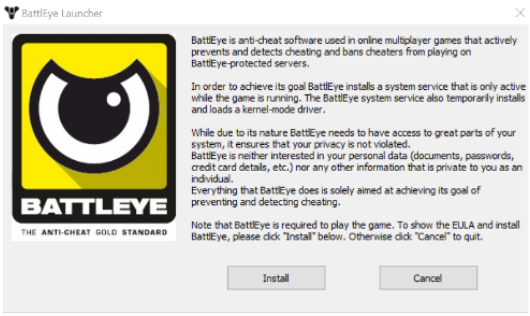

Fig. 3. Players are required to install an anti-cheat software *BattlEye* before playing *Destiny 2*. *BattlEye* collects both user data and device information [55].

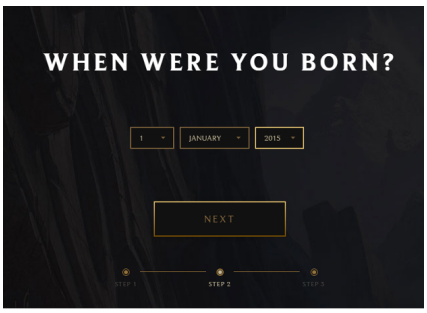

Fig. 4. Players are asked to enter their age upon sign-up in *League of Legends* [107].

Fig. 5. From *League of Legends*, Sign-up process **fails** if the age entered is less than 12 years old [106].

Fig. 6. Players are offered incentives to connect their Facebook account to *Monster Legends* [115].

Fig. 7. *Monster Legends* seemingly offers players an option to request the game not to sell their data. When players click the option on the bottom right they are requested to a web page that is directed at California residents whose data are protected by law not to be sold [117].

Fig. 8. Players who are from California are protected under CCPA for their data not to be sold. There is no mention of protection of data for users from other regions. *Monster Legends* [116].

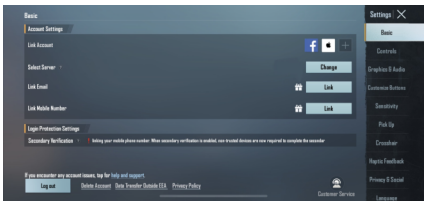

Fig. 10. Players can link one or multiple social media accounts to the same account on *PUBG* (Facebook and iCloud accounts) [70].

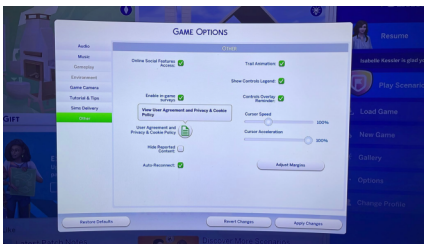

Fig. 12. *The Sims4* Game Options. Players are provided a link to EA Games privacy agreement for information about their data handling practices [54].

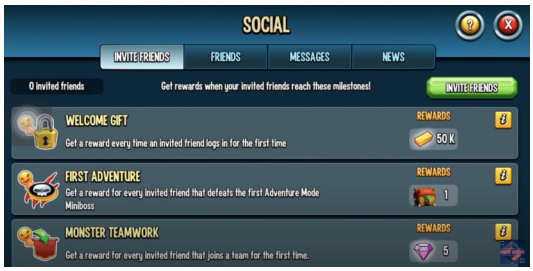

Fig. 9. Sharing *Monster Legends* on social media platforms, SMS or email rewards players points [118].

Fig. 11. Players can link one or multiple social media accounts to the same account on *PUBG* (Twitter and Game Center accounts) [71].

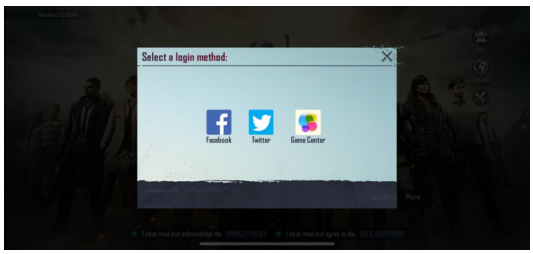

Fig. 13. Players can sign-up with one or multiple social media accounts on *PUBG* (Twitter, Facebook and Game Center accounts) [69].

A.7 Gaming platforms

Steam is a digital distributor that hosts thousands of video games coming from major developers and game manufacturers worldwide. Games available on Steam are mainly played on PCs. Steam's privacy policy is available in multiple languages for users [119]. The company collects and processes data according to GDPR and CCPA.

Steam collects basic account data of the users (email address, country of residence, username, password) and assigns an automatic number (*"Steam ID"*) during the setup process, so the real user name is not required. Steam hosts paid games, so it also requires transaction and payment data, such as name, address, credit card number, expiration date of card and 3-digit security code. It also collects data on Steam client and websites (browser and device information, usage data) and information required to detect violations, which is *not disclosed if disclosure compromises the mechanism of detection and investigation of the violation.* Other collected usage data includes user posts, comments or chats and so on.

Similarly to Steam, **Electronic Arts (EA)** provides online games for various devices (PCs, mobile and game consoles).

Following its Privacy Policy Agreement [34], EA collects users' basic account data (email address, username, real name, country, date of birth, password and telephone number) and device information (hardware identifiers, IP or platform type). In multiplayer mode, EA also registers game profile information, game-play, statistics, and might record the gameplay in certain multiplayer scenarios that can be later played to others. Using EA games through other third-parties like PlayStation and Xbox entails the transfer of users' information from third-party user accounts, but these do not include users' credit card information.

PlayStation and Xbox are gaming platforms for Consoles. **PlayStation** provides a Privacy Policy for its users [102]. In summary, it mentions the following collected user data types on PlayStation: basic information (name, email, country, phone number), console and other devices use, and progress information (trophies, rankings or friend lists). PlayStation also collects users' billing information (credit card details or address).

Xbox is a gaming division of Microsoft. Xbox does not provide a separate Privacy Policy statement, and its link redirects users to the Microsoft's privacy policy [85], which includes aa section on Xbox. While the section describes data handling practices of child players (under 13 years of age), there is no specific section that talks about adult players. We assume that adult players are subject to the general data collection practices of Microsoft, which also include Xbox. Following these practices, user data collected from Xbox includes purchase history. usage data (game progress, achievements or time play per game), content (uploaded, pictures, text and videos), and users' social activity.

A.7.1 Mobile app stores. Mobile app stores, such as Apple's App Store and Google Play Store, are most popular sources of online games.

Google Play Store is an online platform where users can download apps. Currently, users can download Google Play Games to play games without installing the game. Google Play Games has over 5 Billion downloads as of 2022 [100]. Google provides a dedicated Terms of Service for Google Play to guide developers when handling users' data [101]. However, it does not provide users with a separate Privacy Policy for Google Play, so we infer collected user data types from the general Google Privacy Policy [48]. These data types include basic user information (email or photos), users' apps, browsers and devices, user activities (search terms, watch history, voice and audio), and user location (GPS or IP).

Unlike to Google Play, Apple's **App Store** provides a general Privacy Policy with information related to data types collected from users [6], such as account information (Apple ID, email address,

devices, account status and age), device information (serial number or browser type), and other information (usage data or contact information). App Store includes paid apps, so it also collects users' payment Information (address or credit card information). Apple also provides a dedicated Game Center policy [8] that informs users about playing with Game-center enabled games. Apple collects data such as: Game center basic information (nickname, avatar and scores), Game center friends information and a dedicated section about children playing in the Game center.

Moreover, Apple provides user guidelines to check collected data types and compare them for different apps on the store in the form of *Privacy Labels* [7].

Received 2023-02-21; accepted 2023-07-07