

Surveilling the Gamers: Privacy Impacts of the Video Game Industry

Jacob Leon Kröger ^{a,b,*}, Philip Raschke^b, Jessica Percy Campbell^c,
Stefan Ullrich^{a,b}

^a*Technische Universität Berlin, Straße des 17. Juni 135, Berlin, Germany*

^b*Weizenbaum Institute for the Networked Society, Hardenbergstraße 32, Berlin, Germany*

^c*University of Victoria, David Turpin Building A316, Victoria BC V8P 5C2, Canada*

Abstract

With many million users across all age groups and income levels, video games have become the world's leading entertainment industry. Behind the fun experience they provide, it goes largely unnoticed that modern game devices pose a serious threat to consumer privacy. To illustrate the industry's potential for illegitimate surveillance and user profiling, this paper offers a classification of data types commonly gathered by video games. Drawing from patents and literature of diverse disciplines, we also discuss how patterns and correlations in collected gameplay data may leak additional information in ways not easily understood or anticipated by the user. This includes inferences about a user's biometric identity, age and gender, emotions, skills, interests, consumption habits, and personality traits. Based on these findings, we argue that video games need to be brought into the focus of privacy research and discourse. Considering the granularity and enormous scale of the data collection taking place, this industry deserves the same level of scrutiny as other digital services, such as search engines, dating apps, or social media platforms. The knowledge compiled in this paper can serve as a basis for privacy impact assessments, consumer education, and further research into the societal impact of video games.

Keywords:

Video game, Privacy, Surveillance, Behavioral analysis, Data mining, Inference

1. Introduction

Playing video games is an extremely popular leisure activity. With annual revenues of over \$116 billion, video games are the world's leading entertainment medium, producing twice the revenue of digital music and cinema movies combined [1].

*Corresponding author: Jacob Leon Kröger, kroeger@tu-berlin.de

In order to adapt to varying preferences and requirements on the demand side, companies in this fast-growing industry have always been interested in collecting data about individual users and their gaming behavior. When the first video games were commercialized in the 1970s and 80s, these efforts were limited to traditional data collection methods, such as direct observation and videotaping of game play sessions, interviews, and questionnaires [2]. Soon after, with the advent of the World Wide Web and more powerful computers, it became technically possible to monitor users from a distance. Almost all of today’s gaming devices are designed to transfer behavioral data to remote servers over the Internet [3]. The emergence of new business models, including free-to-play video games, microtransactions, and in-game advertising, have added to the industry’s interest in personal data collection and user profiling. Over the past few years, all major game companies have invested substantially in their behavioral analytics capabilities [4, 5].

Throughout a user-game relationship, which can extend over months and years and thousands of hours of play time, “every single action taken, every decision made, every communication” can be recorded [6], sometimes with dozens of parameters being captured per second [7]. In conjunction with large user bases, which comprise up to hundreds of millions of players [8], this continuous gathering results in enormous amounts of high-dimensional user data. Due to technological trends, such as virtual reality, location-based gaming, physiological sensing, and affective computing, gaming also increasingly involves voice, facial, heart rate, skin response, GPS, eye tracking, and gesture recognition data [9].

While there are many legitimate processing purposes (e.g., game customization, discovery of bugs and usability issues, cheat detection, balanced team matching), gaming data can also be used for less noble ends. For example, knowledge about a player’s psychological traits and vulnerabilities can be exploited for highly personalized persuasion and to increase the manipulative effect of targeted advertising [10] – not only to spur artificial demand for real-life goods and services or to sway political opinions and beliefs¹, but also to make players spend more time in a game and purchase premium content [14, 15, 16]. Certain susceptible users, commonly referred to as “whales” in the gaming industry, can be induced to spend exorbitant sums of real money on virtual items or upgrades, often amounting to several hundred times the expenses of the average player [3]. Other possible types of data misuse include arbitrary mass surveillance, identity theft, and all sorts of discrimination [10, 17, 18]. There are methods for computing a “financial risk factor” from gameplay behavior, for instance, based on which a user may be denied a loan or a credit line extension [19], or methods to assess “essential qualities” based on gameplay data in order to determine

¹As “transformative learning tools” which often cover aspects of human history, economy, geography, culture, technology, and war [11], video games can be intentionally designed to propagandize populations and influence users’ political leanings, functioning as an “interactive influence medium” [12] or “radicalising medium” [13].

a player’s suitability for certain jobs [20]. Besides the ever-present possibility of unintended data leaks, game companies regularly share user data with third parties, such as gaming networks, data brokers, middleware and analytics providers, government institutions, and advertising platforms [7, 9, 10, 21] who have their own intentions and may employ the knowledge unethically as well.

For an informed debate about these threats and to determine appropriate safeguards, an in-depth understanding of data collection and usage practices in the video game industry is crucial. Beyond Martinovic et al. [21], Moon [10], Russell et al. [9], and Whitson & Simon’s special issue of *Surveillance & Society* [12], there has been a lack of foundational research on the topic in recent years.

To provide a common basis of understanding for lawmakers, practitioners, and researchers of diverse backgrounds, this paper provides an overview and classification of the data categories commonly collected by video games (Sect. 2). Addressing an important issue that has been largely ignored in privacy research so far, we also explore how modern data analysis methods can be used to infer personal information from hidden patterns and correlations in collected gaming data (Sect. 3). Drawing from published patents and experimental studies, we found that in-game behavior can reveal information about a user’s biometric identity (Section 3.1), age and gender (Sect. 3.2), emotions (Sect. 3.3), skills (Sect. 3.4), interests (Sect. 3.5), consumption habits (Sect. 3.6), and personality traits (Sect. 3.7). The privacy implications of the sensors embedded in game devices will be the focus of Sect. 4. We then provide a discussion in Sect. 5 and a reflection on the limitations of our study in Sect. 6, before we conclude the paper in Sect. 7.

2. Data Categories Collected by Video Game Companies

Any interaction with a modern gaming system can be recorded in time-stamped log files, resulting in a history of all actions taken by the user and all player-related events happening in the game [15, 22]. This includes attributes and qualities, such as duration, frequency, direction, strength, speed, or accuracy of a player’s in-game actions.

Besides manual input, a range of sensors is increasingly being employed in gaming, e.g., to record a user’s voice, gestures, heart rate, facial expressions, or current geographical location (cf. Sect. 4). Gaming systems can also gather information about a user’s specific hardware and software setup and often use tracking technologies, such as identifiers, tags, and cookies [9, 10]. Additionally, many games seek permission to access data from other applications on the same device or from a user’s social media profile, such as documents, personal details, emails, or contact lists [9, 23]. An overview of all these data categories, along with specific examples, is provided in Fig. 1.

For storage and analysis, video games typically transmit their collected data to remote servers over the Internet – a process that is not traceable for the ordinary user and commonly referred to as “telemetry” [24] or “ex situ data

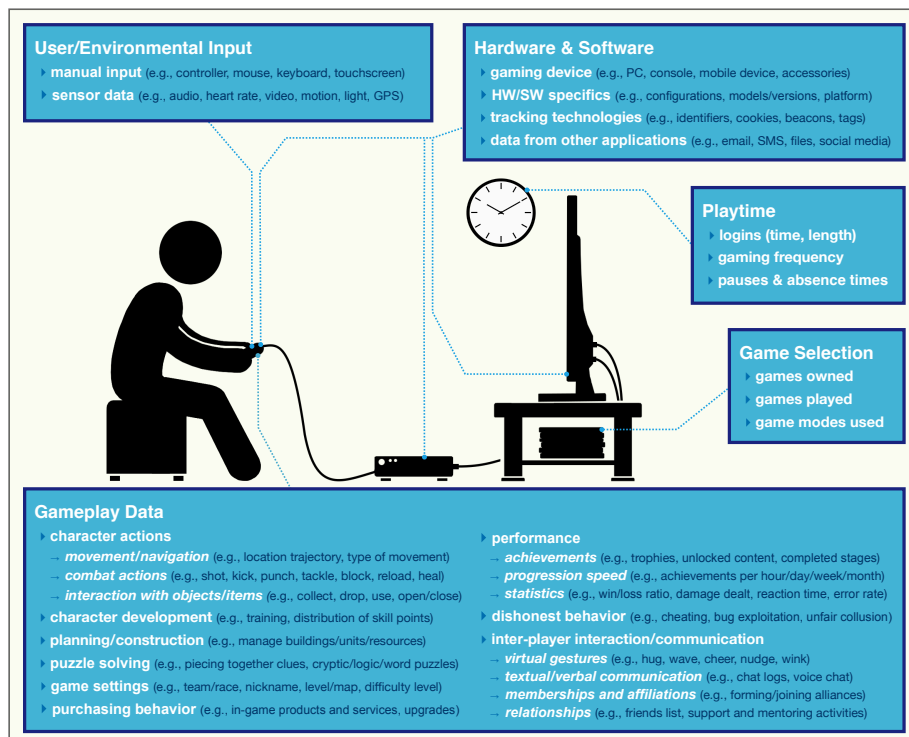


Figure 1: A classification of data types commonly collected by video games.

collection” [25]. Regarding the level of detail and granularity, it can be differentiated between shallow telemetry (i.e., collection of data on only a few behavioral variables) and deep telemetry (i.e., collection of data on all or a substantial fraction of the possible player behaviors) [26].

The specific metrics that are and can be captured naturally depend on the type of game and its underlying business model [7], but there is an overall trend towards more sophisticated video games which increases the variety of the data collected [27]. In many modern video games, “the level of granularity and completeness with which information is collected is unmatched by any real life experimental setup” [28]. One can distinguish between game-specific metrics (e.g., number of glowing bloatflies killed in *Fallout 4*), genre-specific metrics (e.g., character progression in a role-playing game), and generic metrics which can be applied across game genres (e.g., total playtime) [7].

3. Inference of Personal Information from Gameplay Data

Apart from the information that is manually entered by the user or directly recorded (e.g., real name, birthdate, GPS location, chat logs), the data collected by video games can be mined for patterns and statistical relationships to

infer additional personal information. For this purpose, advanced data analysis methods are being applied in ways that may not be easily understood or anticipated by the user. With reference to published experimental research, this section presents and categorizes personal information that can be derived from gaming data – particularly from gameplay data, i.e., the player’s in-game behavior. In view of the vast variety of existing inference methods and the pace of technological progress, this overview is designed to be illustrative rather than comprehensive. Where available, relevant patents are referenced to exemplify corporate intentions and potential real-world applications.

3.1. User Identification

While even the tracking and profiling of anonymous users can be exploited for questionable purposes (e.g., invasive targeted advertising, price discrimination), a company’s ability to link gameplay behavior to a user’s real identity increases the potential for data misuse [21].

A user’s full name, email address, social media profile, postal address, credit card details, and other pieces of identity-related information are often entered during sign-up to a video game or gaming platform [7, 10]. Additionally, online game providers commonly employ tracking technologies, including web beacons, tags, browser fingerprinting, and cookies, enabling them to re-identify individual users and track their activities across different games, even when they are not logged in [9].

Users can also be identified based on characteristics of their individual playing style, such as their specific course of action in strategy games [21] or driving profile in racing games [29]. Besides, researchers found that cross-game tracking is often possible based solely on the analysis of player nicknames [30].

Apart from conventional tracking technologies and gameplay data, modern gaming devices increasingly capture potential biometric identifiers (e.g., voice, facial features, iris patterns, physical movements, body dimensions), as will be discussed in Sect. 4. Even typing rhythms and motion patterns recorded through basic input modalities like smartphone touchscreens [31], controller touch pads [32], computer mice [33], and physical keyboards [34] may be sufficient for user identification.

Due to the variety of existing user identification methods, it is extremely difficult, if not impossible, to guarantee for any gaming data that it is and will remain truly anonymous. Even in cases where the inference of a user’s real identity is not possible (e.g., due to limitations of the applied algorithm or because the target person is not registered in the recognition system database), other attributes derived from gaming data, such as age and gender (cf. Sect. 3.2), interests (cf. Sect. 3.5), socioeconomic status (cf. Sect. 3.6), and health condition (cf. Sect. 4) can still help to classify the target person into a specific demographic group and thereby approximate the identity.

3.2. Age and Gender Recognition

Just as name and address, video game players are often asked to provide their birthdate and gender during account registration [21]. Apart from that,

there are numerous approaches to infer such demographic attributes from playing behavior. For example, Likarish et al. [35] predicted the age of *World of Warcraft* players using 435 in-game features (e.g., character race, class, guild, level, faction, skills, achievements, and combat statistics), achieving a mean absolute error of ± 5 years for 53% of players. Using a similar set of features, Symborski et al. [36] inferred the self-reported gender identity of *Guild Wars* players with an accuracy of 83%.

Other game metrics that were identified as cues to age and/or gender include the tendency to play alone vs. joining multiplayer games [36, 37], the frequency of certain in-game activities (e.g., jumping, harvesting items, helping other players) [36, 37, 38], primary character gender and the number of selected male and female characters [21, 38], virtual-world language use (e.g., chat logs, character names) [36, 39, 40], the time spent playing certain game genres [21], and general play style (e.g., strategic player vs. social player) [36]. In addition to numerous approaches in the scientific literature, the inference of physical properties like gender and age from gameplay data has been incorporated in patents for over 15 years [41].

3.3. Emotion Recognition

Existing approaches for automatic emotion recognition are predominantly based on voice data [42], facial expressions or body language [43], or physiological data, such as heart rate and skin conductance [15], all of which are increasingly being captured by modern gaming technology (cf. Sect. 4). At the same time, however, there are many methods for deriving a person’s affective state without using microphones, cameras, or biofeedback sensors. For example, it has long been proven possible to detect certain cognitive states of computer users, such as stress, by analyzing keyboard typing behavior [44] or cursor movements [45, 46]. Information about the emotions of a video game player can also be derived from playing characteristics, such as manner and direction of an avatar’s movement, the types of weapons fired, objects destroyed, enemies killed, and items collected [47], or from a player’s interaction with game dialogues, the frequency of game drop-outs, and overall performance metrics [46].

Behavioral patterns in interaction with a game can reflect a user’s degree of engagement [46], level of motivation [45], emotional arousal and the valence of emotions (positive, negative, and neutral) [16] as well as more specific affective states such as fun, frustration, and the feeling of being challenged [47], distress, pride, shame, admiration, and reproach [48], anticipatory joy, hope, anxiety, anticipatory relief, and hopelessness [49], focus, curiosity and confusion [50], disappointment, boredom, interest, confidence, and satisfaction [46]. The affect detection model by Conati et al. in [48] even distinguishes between a player’s emotions for the current state of the game, towards him/herself, and towards other characters in the game.

Emotion detection can be enhanced by incorporating information about the target’s personality type [48, 50], some of which is inferable from gaming data as well (cf. Sect. 3.7). Attempts at analyzing the affective state of users based

on in-game behavior have been made by various game companies, including publishers of major commercial titles [15].

3.4. Skill Assessment

Video games are “problem solving spaces” [21] which usually require specific skills and abilities, such as strategic thinking, quick reflexes, aiming accuracy, multitasking, or eye-hand coordination [7, 24]. Two elements commonly found in video games are the repeated exposure of users to similar problems and the aspect of inter-player competition, which allow for multiple observations of a target behavior [51] and direct performance comparison between different players [24].

Extensive research efforts, including whole volumes dedicated to this topic, have established that the success of players in dealing with in-game tasks, puzzles, opponents, and other obstacles can be analyzed to assess their level of competence across a range of knowledge and skills [52, 53, 54]. In a widely used approach called “stealth assessment”, evaluation mechanisms are invisibly woven into a game’s environment to avoid the user being aware of the ongoing analysis [51, 55].

Some of the skills that can be assessed based on gameplay data are teamwork ability [19, 21, 54], language proficiency [19, 54, 56], financial investment skills [19], math fluency [24, 51, 54, 56], ICT skills [54, 57], creative problem solving [45, 51], spatial navigation [58], fine motor skills [51], metacognition and systems thinking [51], memory retention [10, 45, 59], cultural knowledge [41], and the understanding of specific science concepts, such as Newtonian mechanics [11, 60]. Approaches for game-based assessment can also allow to track a user’s cognitive development and learning trajectories over time [51, 61, 62, 63] and to examine specific gaps in knowledge [46, 63] or learning difficulties, such as reading problems and dyscalculia [61, 64].

With the technological and psychological foundations having long been in place, forms of stealth assessment are built into many of today’s commercial games [15, 51]. Patents in this field have existed for over ten years [19, 41].

3.5. Inference of Interests and Preferences

Since video gaming is a voluntary activity based on personal preferences, playing characteristics can allow insights into a player’s interests, likes, and dislikes [5, 37, 65]. Such inferences can not only be drawn from the type of gaming device used and the distribution of playtime across different games, but also from in-game behavior, such as the user’s allocation of budget to certain purposes (e.g., equipment, clothing, transportation), specific items collected and sold, targets of aggression, objectives pursued, modes of transportation used, team member selection, decisions made regarding character development, and patterns in social interaction with other players [19, 41, 66].

Among the user attributes that have been derived from gaming data are the proclivity for video gaming itself and the preference for certain games and game genres [15, 66, 67], game features (e.g., multiplayer vs. singleplayer mode) [67],

game design elements [65], and in-game activities (e.g., optimization, planning, trading, improvisation, imagining, co-operation) [68] as well as, for example, the preference for certain colors [41], car models [5, 19, 41], social relationships [69], sport and leisure activities [41], and types of financial investments [19]. Playing behavior may even reflect a user’s underlying basic desires or “life motives”, such as honor (i.e., the desire to obey traditional moral code), romance (i.e., the desire for courting and sex), acceptance (i.e., the desire for approval and to avoid criticism), independence (i.e., the desire for autonomy and self-reliance) [37], or the desire for social interaction and social achievement [65].

Emotion detection from gaming data, which includes the affective valence of a user’s reactions to specific stimuli inside the game (positive vs. negative) [16] and may thus assist in analyzing preferences and aversions, was discussed in Sect. 3.7 and will be addressed again – with a focus on sensor data – in Sect. 4.

3.6. Inferences about Financial Status and Consumption Behavior

Research has shown that economic behaviors of users in virtual worlds (e.g., collection and spending of in-game currency, trading of virtual goods and services, financial planning within a video game) resemble their real-world counterparts [21, 39], including even clandestine black-market activities [39]. Based on such correlations, game metrics can be indicative of a player’s financial status and consumption habits.

For example, a recently patented profiling method uses play traces to determine whether a user is frugal (e.g., indicated by saving in-game money even in the face of attractive spending options), fiscally responsible (e.g., indicated by investing carefully and focusing on strategically important purchases), or wasteful (e.g., indicated by taking financial risks, spending money quickly, and buying items not relevant to the goals of the game) [19]. The method also aims to evaluate whether a player is “trading-conscious”, i.e., fit for certain financial trading products, and to detect an “eagerness to go after new products or services” based on how players develop their in-game character.

Even non-financial aspects of a game can allow insights into a user’s money-management style. The above patent, for instance, proposes to assesses a user’s level of frugality based on ammunition expenditure patterns in first-person shooter games (e.g., rate at which bullets are fired, percentage of hits, precision shots and controlled bursts vs. wasteful use of ammunition) or based on the user’s performance in driving games and flight simulators (e.g., aggressive driving, overspeed, crash frequency) [19].

Such links between gameplay and real-world spending behavior have also been reported in the scientific literature. Correlating the results of an online survey with log data from the popular sandbox video game *Minecraft*, for example, Canossa et al. [37] found that money-conscious players tend to build fewer sleeping accommodations for themselves and prefer to use cheap in-game materials, such as stone, sand, and iron instead of precious materials, such as diamond.

Besides in-game behavior and virtual consumption, it is common for game publishers to store actual payment information and purchase histories (e.g., when

the user buys games and upgrades online, or pays to unlock content) [9], which could increase their ability to estimate a user’s economic proclivities [10]. Finally, even a user’s set of gaming devices (e.g., cutting-edge game console, special equipment, high-end gaming PC) can be used as a cue to his or her financial standing [21].

3.7. Inference of Personality Traits

As with most aspects of human decision making and behavior (e.g., choice of literature, body language, leisure-time activities, decoration of personal space), personality traits play a central role in shaping how users respond to stimuli and experiences in virtual worlds [70, 71]. Therefore, even though players typically assume a fictional identity in video games – in terms of role (e.g., king, soldier, race driver), species (e.g., human, orc, elf), and other attributes (e.g., gender and age, body features, special abilities) – their individual playing styles often contain discernible traces of real-world personality [70, 72, 73].

By analyzing behavioral data from the multiplayer online games *Call of Duty* and *World of Warcraft*, Martinovic et al. [21] were able to assess certain character traits of players, including politeness (e.g., indicated by thanking and apologizing for in-game actions), leadership (e.g., indicated by remaining unchallenged in a leader role), defeatism (e.g., indicated by propensity to surrender early), disloyalty (e.g., indicated by tendency to betray own team mid-game), and punctuality (e.g., indicated by showing up in advance of scheduled games). A patent titled “Utilizing Gaming Behavior to Evaluate Player Traits” [19] comprises a method for inferring a player’s untrustworthiness (e.g., indicated by dishonest behavior and cheating), aggressiveness (e.g., indicated by using excessive violence), goal orientation (e.g., indicated by actively pursuing specific tasks and objectives), patience (e.g., indicated by planning ahead and going after long-term goals), and risk aversion (e.g., indicated by avoiding unnecessary risks and challenges inside the game).

Other traits that have been correlated with and assessed based on game metrics include the tendency towards addiction [21], the disposition toward maximizing power versus security [68], tenacity and determination [74], self-confidence [19, 46], work ethic [73], and overall psychological maturity [19]. Furthermore, gameplay data has been used to evaluate users along the so-called Big Five personality factors, namely openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism [70, 72, 73, 75] and to evaluate subtypes of traits, e.g., different forms of curiosity (social curiosity, sensory curiosity, novelty-seeking curiosity, and explorative curiosity) [76].

It has been recognized by experts in the field that “most psychology experiments could be construed as video games” [77]. In fact, games can be specifically designed to expose certain personality traits. The first-person shooter game *America’s Army*, for example, which was published by the U.S. Department of Defense as a platform for strategic communication and recruitment, can be used to specifically assess a player’s “army values”, such as loyalty, duty, respect, selfless service, honor, integrity, and personal courage [51].

Experimental research has established that gameplay-personality associations can be sufficient to build a valid personality profile [70, 78]. The game-based recognition of personality traits is possible not only in binary form (high vs. low) but also in the form of numerical scores. In [73], for instance, the prediction result is presented using 100 possible scores along five personality dimensions. The effect size – i.e., the degree to which player personality is expressed in game behavior – was found to be “in line with those seen for professional, medical, and psychological applications of the MMPI, Big Five personality inventory, and Beck’s Hopelessness Scale” [73], which are standardized psychometric tests of adult personality and psychopathology. Researchers have even started to consider “whether a game is more suitable to predicting behaviors in a natural setting than a [conventional] personality test is” [78].

4. Sensor-based Inference of Personal Information

Modern game devices increasingly capture data from outside the game environment through a variety of embedded sensors. Some of the sensor-based technologies and features that are currently trending in the video game industry are eye tracking [10], emotion recognition [15], location-based gaming [79], physiological sensing [45, 74], body motion tracking [10, 15], and the combination of video gaming and physical exercise (“exergaming”) [80]. Some sensors are still being tested and explored for their applicability in video gaming (e.g., EEG, heart rate, skin conductance), whereas other sensors, such as cameras, microphones, GPS chips, and inertial motion sensors are already commonplace in off-the-shelf gaming devices. While sensors fulfill important functions and enable new forms of game interaction, they can unexpectedly reveal a large variety of sensitive personal information [42, 81, 82, 83, 84] and regularly collect data without the user’s knowledge [21, 81].

The precision of sensors found in gaming gear can be remarkable. Some commercially available video game systems (e.g., Xbox Kinect, Wii Balance Board) have already been confirmed as suitable instruments for diagnostic and functional assessment tasks in medical settings [85]. And in a way, even the most basic input devices can be seen as a proxy to gauge physiological measures because they implicitly capture characteristics of a user’s hand and body movements. For example, mouse clicks, keyboard keystrokes, and touchscreen taps can be analyzed to infer information about a user’s physical dexterity [19], state of health [4], emotions (cf. Sect. 3.3), and biometric identity (cf. Sect. 3.1). Illustrating the amount of detail obtainable from seemingly benign sensor data, there is a patented method that uses input from a simple touch pad to detect not only a user’s finger orientation and finger spacing, but also finger lengths and knuckle joint locations [32].

Naturally, this paper cannot cover in depth the whole diversity of sensors used in gaming. To exemplify the privacy implications, we decided to focus on three sensor types that are increasingly found in modern gaming devices and which we have thoroughly explored in previous work, namely accelerometers [81], microphones [42], and eye-tracking sensors [82]. Demonstrating the

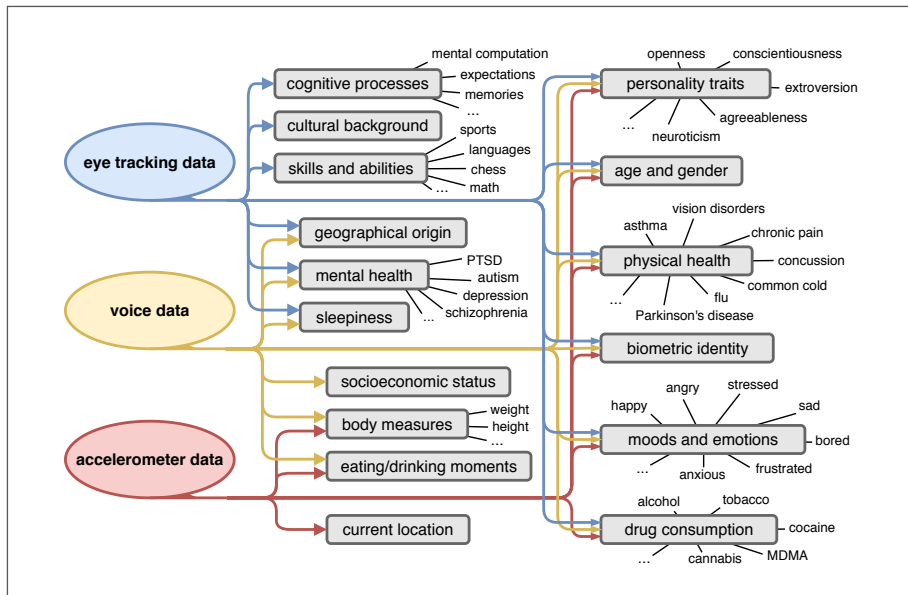


Figure 2: Overview of sensitive inferences that can be drawn from eye-tracking data [82], voice recordings [42], and accelerometer data [81].

richness and potential sensitivity of data from these sensors, Fig. 2 provides an overview of categories of personal information that can be inferred from accelerometer data, audio recordings, and eye-tracking data – representing a synthesis² of the findings from [42], [81], and [82]. For details and background information on these sensor types and inferences, please refer to the respective source. Several of the information categories shown in Fig. 2 did not yet appear in Sect. 3 (e.g., cognitive processes, cultural background, drug consumption, physical and mental health), suggesting that the growing use of sensors in entertainment electronics substantially increases the breadth of personal information discernible from video game data, going far beyond the information contained in traditional gameplay data.

5. Discussion and Implications

As we have explained and illustrated in this paper, video games can be used to collect a large variety of personal information about their users. With the help of advanced data analysis methods, patterns and correlations in gameplay and sensor data can be exploited to draw further inferences, e.g., about a user’s biometric identity, age and gender, emotions, skills, interests, socioeconomic

² From the three sources listed, we selected all inferences applicable to the context of video games.

status, consumption behavior, personality traits, physical and mental health condition, body measures, cultural and geographical background, drug habits, and cognitive processes – potentially much more information than a user wishes and expects to reveal. Considering the rapid developments in the area under investigation in recent years, as evident from the sources studied, we expect near-term discoveries of new threats and further improvements of existing inference methods in terms of speed and accuracy.

Not only the enormous volume and variety of the collected data, but also the high degree of experimental control held by the developers make game metrics so exceptionally sensitive and revealing. With respect to their unprecedented ability of placing millions of people in exactly replicated incentive environments, video games have been described by psychology and data science researchers as “rich natural laborator[ies]” [86], “ideal test bed[s] to collect and study data related to human behavior” [13], and “social engineering experiments that can generate a goldmine of behavioral data” [72]. Some forms of game-based assessment have already matched or even exceeded the accuracy of traditional psychological assessment methods, including self-reports [51, 64, 73, 87]. Above that, game mechanics can be intentionally designed to trigger the reactions and behaviors needed to analyze specific target attributes and qualities of the player [51, 88]. As a result, gaming data may allow intimate insights that are not obtainable from conventional sources of profiling information, such as a person’s browsing habits, loyalty card purchases, or credit history [19].

According to estimates, online video games may generate much more behavioral data than other Internet-based applications and services, including social media platforms [7, 77]. This seems plausible considering the typical amount and intensity of user-game interaction. Globally, gamers spend an average of over 28 hours each month playing, and around 20% of the population play more than 12 hours per week [89]. Also, unlike most other types of human-machine interaction, video gaming can be a deeply immersive experience integrating with a player’s sense of self [21, 46, 54] and may thus inhibit a rational consideration of potential risks and privacy implications.

As is clear from all the above, the video game industry urgently needs to be recognized and treated as a central issue in the discourse around consumer privacy, informational self-determination, and corporate surveillance – which is not currently the case. Users of video games deserve a high level of transparency around any collection, processing, and sharing of their personal data as well as effective protection measures against data access by unauthorized individuals or organizations.

In reality, these requirements are often far from being met. Many game publishers offer neither a sufficient explanation as to which of the data collected are really necessary for the functioning of the game, nor a simple way to opt out of non-essential data collection [7, 25]. Numerous companies in the video game industry, including market-leading players, have been involved in major data breaches [90], been criticized for being secretive about the data they collect and how this data is being used [7, 77, 91], and been accused of sharing personal data with third parties without a warrant and/or the user’s knowledge [21]. As

with many types of software, privacy policies of video games are widely written in ambiguous language and may omit important information [9].

Considering the complex plethora of data being collected by video game companies and the entertaining nature of their products, most users are likely neither motivated nor able to keep track of the ongoing data collection. Furthermore, as indicated by the persistence and prevalence of the nothing-to-hide argument [86], there still seems to be widespread ignorance about the serious risks that can arise from personal data being available to malicious or negligent parties. Thus, it can be questioned whether the doctrine of “informed consent”³ found at the core of even the most progressive data protection laws, such as EU’s GDPR [92], is appropriate and based on realistic assumptions, or whether more extensive forms of government intervention are needed to protect individuals from consequences of their own unawareness. Besides an obligation for companies to provide information on all personal data they collect *and infer*, this could mean restricting personal data usage for certain high-risk purposes irrespective of user consent [93].

In assessing the privacy impacts of video games and in the search for suitable protective measures, it should be considered that – while entertainment electronics appeal to people of all age groups – many game publishers market their products heavily towards minors who tend to be particularly unaware of privacy risks [9]. Furthermore, by putting players into a fictional environment without the immediate social context of real life, video games may give players a false sense of anonymity [10], making them “even more open to revealing their true self and thus [...] more vulnerable to prying eyes” [21].

6. Limitations

Being collected and applied in the service of corporate missions, gaming data and the algorithms used for data analysis are typically considered proprietary and not revealed to the public [5, 27]. Due to these confidentiality provisions, we cannot precisely assess the technological state of the art and current practices within the video game industry. Therefore, while being based on a broad range of valid empirical research, the overviews provided in Sect. 3 and 4 should be understood as an initial exploration of the respective issue, not as the upper bound of what is or may become technically feasible. It should further be noted that many of the cited inference methods were only tested on specific video game genres, individual games, or selected game components (e.g., [21, 29, 35, 36, 38, 75]), meaning that cross-game applicability of these methods remains largely unknown. Since researchers outside corporate laboratories rarely obtain direct access to large-scale user data collected by video game companies [27, 39], most of the cited studies also have relatively small sample sizes.

³In many jurisdictions, informed consent of the data subject is a legal basis for personal data processing. Under EU law, for example, a “freely given, specific, *informed* and unambiguous indication of the data subject’s wishes” is required for valid consent (Art. 4 GDPR). It can be questioned how often these legal requirements are really met in practice.

7. Conclusion

With users, developers, and the wider public being mainly focused on their features and entertainment value, it has been widely overlooked that video games constitute a substantial threat to consumer privacy. The overview provided in this paper illustrates that a wealth of potentially sensitive personal information can be collected and inferred from video game data. Our proposed data classification scheme is intended as a mutual reference point for readers of diverse backgrounds, and as a basic support tool for holistic privacy impact assessments. The example-rich sections on information inference will assist lawmakers, practitioners, and fellow researchers in further grasping the richness and potential sensitivity of gaming data.

Since the workings of data collection and data mining are completely invisible to ordinary video game users, it can be impossible for them to understand and control what information is revealed. Sophisticated surveillance and assessment mechanisms can be imperceptibly woven into the fabric of game environments and storylines. The immersive and distractive nature of video games may further impede a reasonable reflection on the staggering scope of the data harvesting taking place and on potential data misuses. Considering the immense and growing popularity of video gaming, consumer education in this field is urgently needed, along with effective technical and legal safeguards.

However, there still seems to be a long way to go. Various stakeholders of the video game industry are being criticized for a lack of transparency in data processing and have been involved in data scandals. Business models in the industry increasingly revolve around the harvesting and sharing of personal data. Under current circumstances, caution is definitely advisable. As with web browsing, users should not expect that their privacy will be protected or even respected when playing video games. At the same time, solving this problem cannot be left to the individual user. Only technology-savvy NGOs, research institutions, and governmental agencies are equipped to find sustainable solutions to this complex issue.

References

- [1] OppenheimerFunds, Investing in the Soaring Popularity of Gaming, 2018. URL: <https://www.reuters.com/sponsored/article/popularity-of-gaming>.
- [2] S. Santhosh, M. Vaden, Telemetry and Analytics Best Practices and Lessons Learned, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 85–109. URL: https://doi.org/10.1007/978-1-4471-4769-5_6.
- [3] T. V. Fields, Game Industry Metrics Terminology and Analytics Case Study, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 53–71. URL: https://doi.org/10.1007/978-1-4471-4769-5_4.

- [4] S. McCallum, J. Mackie, WebTics: A Web Based Telemetry and Metrics System for Small and Medium Games, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 169–193. URL: https://doi.org/10.1007/978-1-4471-4769-5_10.
- [5] R. Sifa, A. Drachen, C. Bauckhage, Profiling in Games: Understanding Behavior from Telemetry, in: K. Lakkaraju, G. Sukthankar, R. T. Wigand (Eds.), *Social Interactions in Virtual Worlds*, 1 ed., Cambridge University Press, 2018, pp. 337–374. URL: <https://doi.org/10.1017/9781316422823.014>.
- [6] S. Blickensderfer, N. A. Brown, Even the Games Have Eyes: Data Privacy and Gaming, 2019. URL: <https://www.natlawreview.com/article/even-games-have-eyes-data-privacy-and-gaming-podcast>.
- [7] A. Drachen, M. Seif El-Nasr, A. Canossa, Game Analytics – The Basics, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics*, Springer, London, 2013, pp. 13–40. URL: https://doi.org/10.1007/978-1-4471-4769-5_2.
- [8] List of most-played video games by player count, 2020. URL: https://en.wikipedia.org/w/index.php?title=List_of_most-played_video_games_by_player_count&oldid=976346186, page Version ID: 976346186.
- [9] N. C. Russell, J. R. Reidenberg, S. Moon, Privacy in Gaming, *Fordham Intellectual Property, Media & Entertainment Law Journal* (2020). URL: <https://doi.org/10.2139/ssrn.3147068>.
- [10] S. Moon, Privacy in Gaming and Virtual Reality Technologies: Review of Academic Literature 2012 – 2017, Technical Report, Center on Law and Information Policy (CLIP) at Fordham Law School, New York, NY, 2017. URL: https://www.fordham.edu/download/downloads/id/10331/privacy_in_gaming_and_virtual_reality_technologies_review_of_academic_literature_2012-2017.pdf.
- [11] V. J. Shute, F. Ke, Games, Learning, and Assessment, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 43–58. URL: https://doi.org/10.1007/978-1-4614-3546-4_4.
- [12] J. R. Whitson, B. Simon, Game studies meets surveillance studies at the edge of digital culture: An introduction to a special issue on surveillance, games and play, *Surveillance & Society* 12 (2014) 309–319.
- [13] J. Ball, Xbox Live among game services targeted by US and UK spy agencies, 2013. URL: <https://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life>.

- [14] M. S. El-Nasr, *Game Analytics: Maximizing the Value of Player Data*, Springer, New York, 2013.
- [15] T.-H. D. Nguyen, Z. Chen, M. S. El-Nasr, Analytics-based ai techniques for a better gaming experience, in: S. Rabin (Ed.), *Game AI Pro 2: Collected Wisdom of Game AI Professionals*, volume 2, A K Peters/CRC Press, New York, NY, 2015, pp. 481–500.
- [16] G. N. Yannakakis, A. Paiva, Emotion in games, in: R. A. Calvo, S. D’Mello, J. Gratch, A. Kappas (Eds.), *The Oxford Handbook of Affective Computing*, Oxford University Press, New York, NY, 2014, pp. 459–471. Publisher: Oxford University Press.
- [17] W. Christl, *How Companies Use Data Against People*, Technical Report, Cracked Labs, Vienna, 2017.
- [18] Federal Bureau of Investigation, 2019 Internet Crime Report, 2020. URL: https://pdf.ic3.gov/2019_IC3Report.pdf.
- [19] E. J. Landers, B. G. Chun, S. B. Martin, M. H. Chang, A. Rao, T. H. Nguyen, D. S. Pelton, Utilizing gaming behavior to evaluate player traits, 2019. URL: <https://patents.google.com/patent/US10357713B1/en>.
- [20] Scoutible, 2020. URL: <https://www.scoutible.com>.
- [21] D. Martinovic, V. Ralevich, J. McDougall, M. Perklin, “You are what you play”: Breaching privacy and identifying users in online gaming, in: 2014 Twelfth Annual International Conference on Privacy, Security and Trust, IEEE, Toronto, 2014, pp. 31–39. URL: <https://doi.org/10.1109/PST.2014.6890921>.
- [22] A. Canossa, A. Drachen, Patterns of Play: Play-Personas in User-Centred Game Development, in: *Proceedings of the 2009 DiGRA International Conference*, Digital Games Research Association, London, 2009.
- [23] Pokémon GO Caught Millions of Players and Their Data, *Information Management* 50 (2016) 12.
- [24] C. S. Loh, Information Trails: In-Process Assessment of Game-Based Learning, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 123–144. URL: https://doi.org/10.1007/978-1-4614-3546-4_8.
- [25] C. S. Loh, Y. Sheng, Measuring Expert Performance for Serious Games Analytics: From Data to Insights, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*, *Advances in Game-Based Learning*, Springer, Cham, 2015, pp. 101–134. URL: https://doi.org/10.1007/978-3-319-05834-4_5.

- [26] A. Canossa, Interview with Nicholas Francis and Thomas Hagen from Unity Technologies, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 137–142. URL: https://doi.org/10.1007/978-1-4471-4769-5_8.
- [27] A. Drachen, C. Thureau, A Comparison of Methods for Player Clustering via Behavioral Telemetry, in: *Proceedings of the 8th International Conference on the Foundations of Digital Games*, Society for the Advancement of the Science of Digital Games, Chania, Crete, 2013.
- [28] K. J. Shim, N. Pathak, M. A. Ahmad, C. DeLong, Z. Borbora, A. Mahapatra, J. Srivastava, Analyzing human behavior from multiplayer online game logs: A knowledge discovery approach, *IEEE Intelligent Systems* 26 (2011) 85–89.
- [29] M. Kale, M. Bedekar, Driver Profiling Using Realistic Racing Games, in: *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, IEEE, Coimbatore, 2018, pp. 13–17. URL: <https://doi.org/10.1109/ICICCT.2018.8473154>.
- [30] M. A. Ahmad, C. Shen, J. Srivastava, N. Contractor (Eds.), *Predicting real world behaviors from virtual world data*, Springer, Cham, 2014. URL: <https://doi.org/10.1007/978-3-319-07142-8>.
- [31] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, N. Nguyen, Continuous mobile authentication using touchscreen gestures, in: *2012 IEEE conference on technologies for homeland security (HST)*, IEEE, Waltham, MA, 2012, pp. 451–456.
- [32] B. Lukas, Q. Fu, S. Ranganathan, J. Karaoguz, T. W. Kwan, X. Yu, Hand-held gaming device that identifies user based upon input from touch sensitive panel, 2014. URL: <https://patents.google.com/patent/US8754746B2/en>.
- [33] B. Sayed, I. Traoré, I. Woungang, M. S. Obaidat, Biometric authentication using mouse gesture dynamics, *IEEE Systems Journal* 7 (2013) 262–274. URL: <https://doi.org/10.1109/JSYST.2012.2221932>, publisher: IEEE.
- [34] S. Maheshwary, S. Ganguly, V. Pudi, Deep secure: A fast and simple neural network based approach for user authentication and identification via keystroke dynamics, in: *IWAISE: First international workshop on artificial intelligence in security*, NUI Galway, Melbourne, 2017, pp. 59–67.
- [35] P. Likarish, O. Brdiczka, N. Yee, N. Ducheneaut, L. Nelson, Demographic Profiling from MMOG Gameplay, in: *11th Privacy Enhancing Technologies Symposium*, Springer, Waterloo, Canada, 2011, pp. 1–19.

- [36] C. Symborski, G. M. Jackson, M. Barton, G. Cranmer, B. Raines, M. M. Quinn, The Use of Social Science Methods to Predict Player Characteristics from Avatar Observations, in: M. A. Ahmad, C. Shen, J. Srivastava, N. Contractor (Eds.), *Predicting Real World Behaviors from Virtual World Data*, Springer, Cham, 2014, pp. 19–37. URL: https://doi.org/10.1007/978-3-319-07142-8_2, publisher: Springer, Cham.
- [37] A. Canossa, J. B. Martinez, J. Togelius, Give me a reason to dig Minecraft and psychology of motivation, in: *2013 IEEE Conference on Computational Intelligence in Games (CIG)*, IEEE, Niagara Falls, ON, 2013, pp. 1–8. URL: <https://doi.org/10.1109/CIG.2013.6633612>.
- [38] T. Kennedy, R. R. Ratan, K. Kapoor, N. Pathak, D. Williams, J. Srivastava, Predicting MMO Player Gender from In-Game Attributes Using Machine Learning Models, in: M. Ahmad, C. Shen, J. Srivastava, N. Contractor (Eds.), *Predicting Real World Behaviors from Virtual World Data*, Springer, Cham, 2014, pp. 69–84. URL: https://doi.org/10.1007/978-3-319-07142-8_5.
- [39] M. A. Ahmad, C. Shen, J. Srivastava, N. Contractor, On the Problem of Predicting Real World Characteristics from Virtual Worlds, in: M. A. Ahmad, C. Shen, J. Srivastava, N. Contractor (Eds.), *Predicting Real World Behaviors from Virtual World Data*, Springer Proceedings in Complexity, Springer, Cham, 2014, pp. 1–18. URL: https://doi.org/10.1007/978-3-319-07142-8_1.
- [40] A. Lawson, J. Murray, Identifying User Demographic Traits Through Virtual-World Language Use, in: M. A. Ahmad, C. Shen, J. Srivastava, N. Contractor (Eds.), *Predicting Real World Behaviors from Virtual World Data*, Springer Proceedings in Complexity, Springer, Cham, 2014, pp. 57–67. URL: https://doi.org/10.1007/978-3-319-07142-8_4.
- [41] D. Willis, Method and system for delivering advertising content to video games based on game events and gamer activity, 2006. URL: <https://patents.google.com/patent/US20060135232A1/en>.
- [42] J. L. Kröger, O. H.-M. Lutz, P. Raschke, Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference, in: M. Friedewald, M. Önen, E. Lievens, S. Krenn (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy*, Springer,, Cham, 2020, pp. 242–258. URL: https://doi.org/10.1007/978-3-030-42504-3_16.
- [43] E. Novak, T. E. Johnson, Assessment of Student’s Emotions in Game-Based Learning, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 379–399. URL: https://doi.org/10.1007/978-1-4614-3546-4_19.

- [44] L. M. Vizer, L. Zhou, A. Sears, Automated stress detection using keystroke and linguistic features: An exploratory study, *International Journal of Human-Computer Studies* 67 (2009) 870–886. URL: <https://doi.org/10.1016/j.ijhcs.2009.07.005>.
- [45] I. Ghergulescu, C. H. Muntean, Measurement and Analysis of Learner’s Motivation in Game-Based E-Learning, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 355–378. URL: https://doi.org/10.1007/978-1-4614-3546-4_18.
- [46] E. E. Mattheiss, M. D. Kickmeier-Rust, C. M. Steiner, D. Albert, Approaches to Detect Discouraged Learners: Assessment of Motivation in Educational Computer Games, in: *Proceedings of eLearning Baltics (eLBa)*, Rostock, 2010, pp. 1–10.
- [47] N. Shaker, G. Yannakakis, J. Togelius, Towards Automatic Personalized Content Generation for Platform Games, in: *6th AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, AIIDE*, Stanford, CA, 2010, pp. 63–68.
- [48] C. Conati, H. Maclaren, Empirically Building and Evaluating a Probabilistic Model of User Affect, *User Modeling and User-Adapted Interaction* 19 (2009) 267–303. URL: <https://doi.org/10.1007/s11257-009-9062-8>.
- [49] K. Muñoz, P. M. Kevitt, T. Lunney, J. Noguez, L. Neri, An emotional student model for game-play adaptation, *Entertainment Computing* 2 (2011) 133–141. URL: <https://doi.org/10.1016/j.entcom.2010.12.006>.
- [50] J. Sabourin, B. Mott, J. C. Lester, Modeling Learner Affect with Theoretically Grounded Dynamic Bayesian Networks, in: S. D’Mello, A. Graesser, B. Schuller, J.-C. Martin (Eds.), *Affective Computing and Intelligent Interaction*, volume 6974, Springer, Berlin, 2011, pp. 286–295. URL: https://doi.org/10.1007/978-3-642-24600-5_32, series Title: *Lecture Notes in Computer Science*.
- [51] J. L. Plass, B. D. Homer, C. K. Kinzer, Y. K. Chang, J. Frye, W. Kaczetow, K. Isbister, K. Perlin, Metrics in Simulations and Games for Learning, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 697–729. URL: https://doi.org/10.1007/978-1-4471-4769-5_31.
- [52] D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012. URL: <https://doi.org/10.1007/978-1-4614-3546-4>.
- [53] C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious games analytics: methodologies for performance measurement, assessment, and improvement*, *Advances in Game-Based Learning*, Springer, Cham, 2015. URL: <https://doi.org/10.1007/978-3-319-05834-4>.

- [54] M. C. Mayrath, J. Clarke-Midura, D. H. Robinson (Eds.), *Technology-Based Assessments for 21st Century Skills: Theoretical and Practical Implications from Modern Research*, Information Age Publishing, Charlotte, NC, 2012.
- [55] V. J. Shute, *Stealth Assessment in Computer-Based Games to Support Learning*, *Computer Games and Instruction* 55 (2011) 503–524.
- [56] A. Canossa, *Interview with Simon Egenfeldt Nielsen from Serious Games Interactive*, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 763–766. URL: https://doi.org/10.1007/978-1-4471-4769-5_33.
- [57] R. J. Mislevy, J. T. Behrens, K. E. Dicerbo, D. C. Frezzo, P. West, *Three Things Game Designers Need to Know About Assessment*, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 59–81. URL: https://doi.org/10.1007/978-1-4614-3546-4_5.
- [58] F. Ke, V. Shute, *Design of Game-Based Stealth Assessment and Learning Support*, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics*, Springer, Cham, 2015, pp. 301–318. URL: https://doi.org/10.1007/978-3-319-05834-4_13.
- [59] K. E. DiCerbo, M. Bertling, S. Stephenson, Y. Jia, R. J. Mislevy, M. Bauer, G. T. Jackson, *An Application of Exploratory Data Analysis in the Development of Game-Based Assessments*, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*, *Advances in Game-Based Learning*, Springer, Cham, 2015, pp. 319–342. URL: https://doi.org/10.1007/978-3-319-05834-4_14.
- [60] E. Rowe, J. Asbell-Clarke, R. S. Baker, *Serious Games Analytics to Measure Implicit Science Learning*, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*, *Advances in Game-Based Learning*, Springer, Cham, 2015, pp. 343–360. URL: https://doi.org/10.1007/978-3-319-05834-4_15.
- [61] B. Csapó, A. Lőrincz, G. Molnár, *Innovative Assessment Technologies in Educational Games Designed for Young Students*, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 235–254. URL: https://doi.org/10.1007/978-1-4614-3546-4_13.
- [62] D. Ifenthaler, D. Eseryel, X. Ge, *Assessment for Game-Based Learning*, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, New York, NY, 2012, pp. 1–8. URL: https://doi.org/10.1007/978-1-4614-3546-4_1.

- [63] R. D. Myers, T. W. Frick, Using Pattern Matching to Assess Gameplay, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*, *Advances in Game-Based Learning*, Springer, Cham, 2015, pp. 435–458. URL: https://doi.org/10.1007/978-3-319-05834-4_19.
- [64] S. Klingler, T. Käser, A.-G. Busetto, B. Solenthaler, J. Kohn, M. von Aster, M. Gross, Stealth Assessment in ITS - A Study for Developmental Dyscalculia, in: A. Micarelli, J. Stamper, K. Panourgia (Eds.), *Intelligent Tutoring Systems*, volume 9684, Springer, Cham, 2016, pp. 79–89.
- [65] X. Li, C. Lu, J. Peltonen, Z. Zhang, A statistical analysis of Steam user profiles towards personalized gamification, in: *Proceedings of the 3rd International GamiFIN Conference*, CEUR-WS, Levi, 2019.
- [66] R. Sifa, C. Bauckhage, A. Drachen, Archetypal Game Recommender Systems, in: *Learning, Knowledge, Adaption (LMA) Conference*, CEUR-WS, Aachen, 2014, pp. 45–56.
- [67] J. Hamari, J. Tuunanen, Player Types: A Meta-synthesis, *Transactions of the Digital Games Research Association* 1 (2014) 29–53. URL: <https://doi.org/10.26503/todigra.v1i2.13>.
- [68] B. Cowley, D. Charles, Behavlets: a method for practical player modelling using psychology-based player traits and domain specific features, *User Modeling and User-Adapted Interaction* 26 (2016) 257–306. URL: <https://doi.org/10.1007/s11257-016-9170-1>.
- [69] P. P. Lai, S. Bai, D. Baack, K. Lee, Systems and methods for determining game level attributes based on player skill level prior to game play in the level, 2019. URL: <https://patents.google.com/patent/US10363487/en>.
- [70] P. Spronck, I. Balemans, Player Profiling with Fallout 3, in: *Proceedings of the AIIDE 2012 Conference*, AAAI Press, Palo Alto, CA, 2012, pp. 179–184.
- [71] V. Zeigler-Hill, S. Monica, The HEXACO model of personality and video game preferences, *Entertainment Computing* 11 (2015) 21–26. URL: <https://doi.org/10.1016/j.entcom.2015.08.001>.
- [72] N. Ducheneaut, N. Yee, Data Collection in Massively Multiplayer Online Games: Methods, Analytic Obstacles, and Case Studies, in: M. S. El-Nasr, A. Drachen, A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data*, Springer, London, 2013, pp. 641–664. URL: https://doi.org/10.1007/978-1-4471-4769-5_28.
- [73] S. Tekofsky, J. V. D. Herik, P. Spronck, A. Plaat, Psyops: Personality assessment through gaming behavior, in: *In Proceedings of the International*

Conference on the Foundations of Digital Games, ACM, Chania, Crete, 2013, pp. 166–173.

- [74] J. R. Stafford, S. Osman, Automated video game rating, 2015. URL: <https://patents.google.com/patent/US9044675B2/en>.
- [75] N. Yee, N. Ducheneaut, L. Nelson, P. Likarish, Introverted Elves & Conscientious Gnomes: The Expression of Personality in World of Warcraft, in: Proceedings of the SIGCHI conference on human factors in computing systems, ACM, New York, NY, 2011, pp. 753–762.
- [76] M. Schaekermann, G. Ribeiro, G. Wallner, S. Kriglstein, D. Johnson, A. Drachen, R. Sifa, L. E. Nacke, Curiously Motivated: Profiling Curiosity with Self-Reports and Behaviour Metrics in the Game "Destiny", in: Proceedings of the Annual Symposium on Computer-Human Interaction in Play - CHI PLAY '17, ACM, Amsterdam, 2017, pp. 143–156.
- [77] T. Upchurch, Google Stadia has kicked off a new age of gaming data harvesting, Wired UK (2019). URL: <https://www.wired.co.uk/article/google-stadia-data-harvesting>.
- [78] G. van Lankveld, P. Spronck, J. van den Herik, A. Arntz, Games as personality profiling tools, in: 2011 IEEE Conference on Computational Intelligence and Games (CIG'11), IEEE, Seoul, 2011, pp. 197–202. URL: <https://doi.org/10.1109/CIG.2011.6032007>.
- [79] D. Leorke, Location-Based Gaming: Play in Public Space, Palgrave Macmillan, Singapore, 2018. URL: <https://doi.org/10.1007/978-981-13-0683-9>.
- [80] E. Loos, Exergaming: Meaningful Play for Older Adults?, in: J. Zhou, G. Salvendy (Eds.), Human Aspects of IT for the Aged Population. Applications, Services and Contexts, Lecture Notes in Computer Science, Springer, Cham, 2017, pp. 254–265.
- [81] J. L. Kröger, P. Raschke, T. R. Bhuiyan, Privacy Implications of Accelerometer Data: A Review of Possible Inferences, in: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP), ACM, New York, NY, 2019, pp. 81–87. doi:<https://doi.org/10.1145/3309074.3309076>.
- [82] J. L. Kröger, O. H.-M. Lutz, F. Müller, What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking, in: S. Fricker, M. Friedewald, S. Krenn, E. Lievens, M. Önen (Eds.), Privacy and Identity Management. Data for Better Living: AI and Privacy, IFIP Advances in Information and Communication Technology, Springer, Cham, 2019, pp. 226–241. URL: https://doi.org/10.1007/978-3-030-42504-3_15.

- [83] J. Kröger, Unexpected inferences from sensor data: a hidden privacy threat in the internet of things, in: IFIP International Internet of Things Conference, Springer, 2018, pp. 147–159. URL: https://doi.org/10.1007/978-3-030-15651-0_13.
- [84] J. L. Kröger, P. Raschke, Is my phone listening in? on the feasibility and detectability of mobile eavesdropping, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2019, pp. 102–120. URL: https://doi.org/10.1007/978-3-030-22479-0_6.
- [85] J. Ruff, T. L. Wang, C. C. Quatman-Yates, L. S. Phieffer, C. E. Quatman, Commercially available gaming systems as clinical assessment tools to improve value in the orthopaedic setting: A systematic review, *Injury* 46 (2015) 178–183.
- [86] T. Casey, The Value of Deviance: Understanding Contextual Privacy, *Loyola University Chicago Law Journal* 51 (2019) 65–105.
- [87] D. J. Cornforth, M. T. P. Adam, Cluster Evaluation, Description, and Interpretation for Serious Games, in: C. S. Loh, Y. Sheng, D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*, Advances in Game-Based Learning, Springer, Cham, 2015, pp. 135–155.
- [88] J. T. Behrens, R. J. Mисlevy, K. E. DiCerbo, R. Levy, An evidence centered design for learning and assessment in the digital world, Technical Report, National Center for Research on Evaluation, Standards, and Student Testing (CREST), Los Angeles, CA, 2010.
- [89] Limelight Networks, The State of Online Gaming - 2019, 2019. URL: <https://www.limelight.com/resources/white-paper/state-of-online-gaming-2019/>.
- [90] List of data breaches, 2020. URL: https://en.wikipedia.org/w/index.php?title=List_of_data_breaches&oldid=980849764, page Version ID: 980849764.
- [91] J. L. Kröger, J. Lindemann, D. Herrmann, How do app vendors respond to subject access requests? a longitudinal privacy study on ios and android apps, in: International Conference on Availability, Reliability and Security, 2020, pp. 1–10. URL: <https://doi.org/10.1145/3407023.3407057>.
- [92] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, (Un)informed Consent: Studying GDPR Consent Notices in the Field, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, London, 2019, pp. 973–990.
- [93] J. L. Kröger, O. H.-M. Lutz, S. Ullrich, The myth of individual control: Mapping the limitations of privacy self-management, *Social Science Research Network (SSRN)* (2021). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776.