TOWARDS AN ETHICAL METAVERSE: A SYSTEMATIC LITERATURE REVIEW ON PRIVACY CHALLENGES

Completed Research Paper

Runjie Xie, Friedrich-Alexander-Universität Erlangen-Nürnberg, Nürnberg, Germany, runjie.xie@fau.de

Jeanine Kirchner-Krath, Friedrich-Alexander-Universität Erlangen-Nürnberg, Nürnberg, Germany, jeanine.kirchner-krath@fau.de

Benedikt Morschheuser, Friedrich-Alexander-Universität Erlangen-Nürnberg, Nürnberg, Germany, benedikt.morschheuser@fau.de

Abstract

Along with the increasing interest in the metaverse as a new space for social interaction, privacy challenges that arise from new forms of data collection and usage have received notable research interest. Still, researchers and practitioners lack a structured overview of these privacy challenges as a foundation to explore measures that allow for safe and protected interaction in an ethical metaverse. To bridge this gap, we conducted a systematic literature review. We find that interaction in the metaverse carries the risk of revealing more sensitive personal data than in the traditional Internet. Moreover, we identify metaverse privacy challenges on different stakeholder levels, which often mirror those from the traditional Internet. Nevertheless, the metaverse also introduces novel facets to existing challenges due to its unique characteristics. These facets are discussed across six essential dimensions of privacy. Based on our findings, we provide recommendations for building a safe and secure metaverse environment.

Keywords: Metaverse, Extended Reality, Virtual World, Avatar, Privacy, Security, Literature Review.

1 Introduction

The term "***metaverse***", initially coined by Neal Stephenson in his science fiction novel "Snow Crash" in 1992, is a portmanteau of 'meta' (Greek for "beyond"), serving as a prefix to signify transcendence, and the suffix 'verse', derived from "universe" (Wang et al., 2023). This concept envisions a seamless fusion of physical reality and digital virtuality, transcending time and space (Kang et al., 2023). A key aspect of the metaverse involves the merging of our real-world representation and identity with a digital counterpart in the virtual world (Smith et al., 2023). Users access the metaverse through avatars and engage in interactions with each other, as well as with items, applications and services (Dwivedi et al., 2022). The foundation for the metaverse was laid by open-world multiplayer games (Chen et al., 2022), but the growing integration of cyber-physical elements has paved the way for the metaverse to extend to sports, education, work, business, and commerce (Di Pietro and Cresci, 2021). In line with Falchuk et al. (2018), we view the metaverse as inclusive of virtual worlds, whether they involve augmented reality (AR) and virtual reality (VR) technologies or exist purely as virtual environments. These spaces collectively enable immersive interactions, a defining feature of the metaverse (Wang et al., 2023).

The metaverse is envisioned as the forthcoming evolution of the Internet (Gupta et al., 2023). Consequently, it is attracting growing interest from technology giants, such as Meta, Microsoft, NVIDIA, Roblox, and Unity (Venugopal et al., 2023), and transitions from science fiction to imminent reality (Vadlamudi, 2022). However, the rapid advancement in technological capabilities for data collection, storage, and processing exceeds the pace at which regulations can keep up (Harborth, 2022).

Therefore, ensuring and protecting user privacy emerges as a prominent concern in the ongoing development and adoption of the metaverse (Venugopal et al., 2023; Wang et al., 2023).

Privacy is a multidimensional concept that is shaped by cultural and individual values (Smith et al., 2011; Tifferet, 2019). The history underscores a profound connection between privacy and technological progress (Westin, 2003). As the metaverse intertwines reality and virtuality, it is vital to include privacy definitions for both realms. While physical privacy has historically received less attention in information systems (Bélanger and Crossler, 2011; Smith et al., 2011), its importance is growing with the rise of the metaverse. Therefore, our definition of privacy in the metaverse encompasses the right to be left alone (Warren and Brandeis, 1890), the protection of personal space, the control of access to oneself (Altman, 1975), personal information (Westin, 1967), transactions between oneself and others (Margulis, 1977), and aspects concerning the freedom of dignity and autonomy (Schoeman, 1992). Drawing from literature (Kokolakis, 2017; Zhang et al., 2022), we can identify six essential privacy dimensions (PD): (1) ***information privacy*** (IP): controlling the collection, storage, processing, and distribution of personal data, (2) ***bodily privacy*** (BP): protecting individuals from unauthorized intrusion, (3) ***territorial privacy*** (TP): safeguarding the physical area surrounding a person, (4) ***social privacy*** (SP): controlling the timing, channels, and participants of interactions, (5) ***psychological privacy*** (PP): governing external influence on an individual's thoughts, feelings, and values, and (6) ***virtual territorial privacy*** (VP): regulating others' interactions with an individual's virtual properties.

The European Union recognized privacy as a fundamental human right in 2000 under Article 8 of the EU Charter (Harborth, 2022). The enactment of the General Data Protection Regulation (GDPR) in 2018 aims to protect personal data by requiring user consent for data collection by organizations. Despite the significance attached to regulations, there is a notable gap in enforcement (Custers et al., 2018).

As a particular obstacle to regulate and ensure privacy in the metaverse, a new space for virtual interaction, it is still unclear what new data and privacy challenges the metaverse may pose. Given the extensive social interactions within the metaverse, it is expected to elicit at least comparable privacy concerns to online social networks (OSN) (Benrimoh et al., 2022). While there has been significant progress and growing interest in metaverse, there remains a notable lack of an overview regarding its privacy aspects (Awadallah et al., 2023; Kang et al., 2023).

Recent surveys conducted by Chen et al. (2022), Di Pietro and Cresci (2021), Huang et al. (2023), Kang et al. (2023), and Wang et al. (2023) are of noteworthy significance, as they represent pioneering works providing an analysis of security and privacy concerns in the metaverse. However, they tend to focus on the privacy aspects of underlying technologies and consider privacy issues as a consequence of security breaches. Even though privacy and security are closely related, the concept of privacy extends beyond cyberattacks (Farahmand et al., 2013) and includes, for example, protection from unconsented data collection (Kokolakis, 2017), regulation of data usage (Custers et al., 2018), and safeguarding of personal space (Tifferet, 2019) in interactions between different legal stakeholders in the virtual space.

In this respect, we lack a systematic understanding of how the emerging metaverse, as a potential successor of today's Internet, may allow for new ways of collecting personal data and invoke novel privacy challenges in different stakeholder interactions. Therefore, we conduct a systematic literature review with the aim to synthesize insights on data, privacy challenges, and stakeholders mentioned in the ongoing scientific discourse on privacy issues in the metaverse and discuss unique differences compared to the current Internet. Thus, this research is guided by the following research questions (RQ):

RQ1*: What types of data can be exposed within the metaverse?*

RQ2*: What privacy challenges can be posed by which stakeholders within the metaverse?*

Our work offers a threefold contribution. (1) First, we present a synthesized overview of data types and privacy challenges in existing metaverse research. (2) Second, based on identified data types and privacy challenges, we discuss the unique differences in the six essential privacy dimensions between the metaverse and the current Internet landscape, with a particular focus on OSNs. (3) Third, drawing on our findings and discussion, we derive recommendations for both scholars and practitioners to guide efforts in building a safe and secure metaverse. As a result, our study serves as an informed foundation for future research and practice endeavors to ensure development towards an ethical metaverse.

2 Methodology

To answer the proposed research questions, we conducted a systematic literature review according to the guidelines proposed by vom Brocke et al. (2009) and Webster and Watson (2002). After an initial phase of reading key studies of the fields (vom Brocke et al., 2009), we identified two sets of keywords covering the two key components of our research questions, which are metaverse and privacy. Subsequently, we constructed and refined the search string through an iterative process, primarily by excluding subparts of the keywords to narrow down the solution space. For instance, "cyberspace" was omitted due to its broad inclusion of studies related to the general digital environment, while "security" was excluded as it predominantly led to research on cybersecurity concepts. Moreover, we deliberately omitted terms like AR and VR from our search criteria to focus on the interactive dimension of the metaverse rather than the underlying technologies. However, we included the term extended reality (XR) as some researchers use it to refer to the metaverse. The final search string looked as follows:

("extended reality" OR "metaverse" OR "virtual world" OR "virtual space*" OR "virtual environment*" OR "immersive world*" OR "immersive environment*" OR "immersive space*" OR "3D world*" OR "3D environment*") AND ("privacy" OR "disclosure" OR "governance" OR "data protection" OR "personal information" OR "phishing" OR "surveillance")*

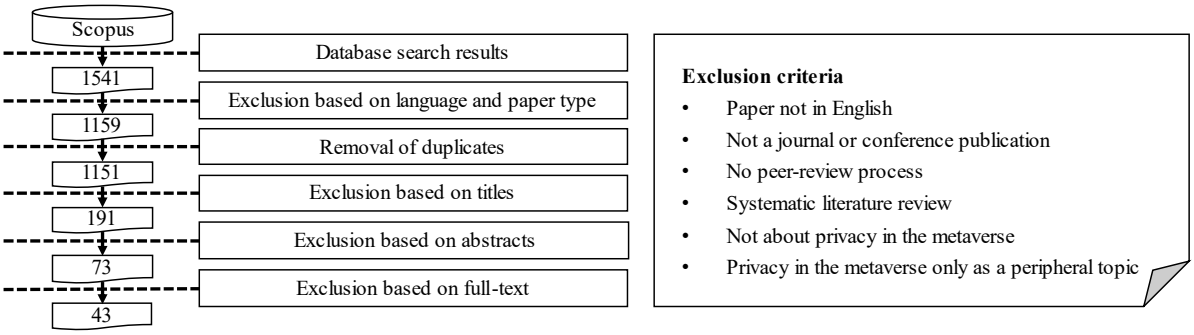

Figure 1. Search strategy and screening process.

The query was performed in July 2023 by title, abstract, and keywords in Scopus, one of the most extensive multidisciplinary databases (Baas et al., 2020). Figure 1 illustrates the search strategy and screening process. The initial search yielded 1541 papers. We then applied specific exclusion criteria to validate the studies (see Figure 1). With regard to types of studies, in line with recommendations for descriptive systematic review (Paré et al., 2015), we focused on conceptual and empirical studies published in peer-reviewed journals and conferences. In terms of content, we excluded studies that did not address privacy in the metaverse at all or barely, such as studies on blockchain, Internet of Things, OSNs, traffic surveillance, Industry 4.0, cybersecurity education, e-commerce, and avatar customization. As a result of the selection process, 43 publications were included in the final review.

Following the recommendations provided by Webster and Watson (2002), we adopted an author-centric qualitative data extraction approach. This involves coding the research method and study context as well as data types and privacy challenges mentioned in the paper. Initially, data types and challenges were coded inductively, following the data analysis approach outlined by Thomas (2006). For instance, in the article by Fernandez and Hui (2022), privacy challenges such as cyber spying and stalking, hacking, and cyber bullying and harassment were mentioned. These challenges, along with the identified data types, were coded separately to comprehensively capture all privacy challenges relevant to our research question. Subsequently, in the concept-centric phase, the inductively coded data types and challenges were analyzed and deductively categorized. We drew inspiration from Kayes and Iamnitchi's (2017) stakeholder approach to categorize these challenges. Moreover, the data types and challenges were deductively mapped to the six privacy dimensions. The first author initially coded them and the second author subsequently conducted an intercoder agreement check. The agreement rate reached 89%, indicating strong concordance (Neuendorf, 2017). Any discrepancies were resolved in joint discussion.

3 Results

3.1 Bibliometric information

The first article exploring privacy in the metaverse was published in 2009, when Second Life, one of the first metaverse platforms, became widespread (Deng and Ruan, 2009) (see Figure 2). In 2022, there has been a rapid increase in publications, largely due to raised industry attention to the metaverse (mentioned by 19 of 30 papers published after 2021) and the Covid pandemic (18 of 30), as new ways of virtual interaction were gaining interest. In terms of research context, 28 studies kept the context general, 6 studies had a focus on education, 3 on leisure, 3 on virtual workspaces, and 3 on healthcare. Regarding research methods, 28 wrote conceptual articles, 4 conducted laboratory experiments, 3 used interviews, 3 applied case studies, 2 adopted surveys, 2 carried out mixed-methods studies and 1 presented a prototype. Table 3 in the Appendix provides an overview of the included studies.

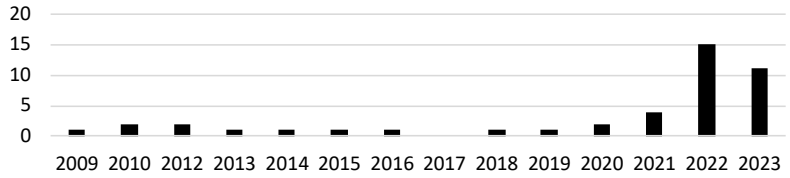

Figure 2. Studies per year.

3.2 Exposed data types in the metaverse

Regarding the exposure of personal data in the metaverse, we identified 20 different types from analyzed studies that are subject to privacy protection. These data types were then inductively classified into six distinct categories: personally identifiable information (P), on-platform data (O), physical body data (B), physical territorial data (T), habitus data (H), and context-specific data (S). Afterwards, these data types were deductively mapped to the six key privacy dimensions. Table 1 provides an aggregated overview.

First, in terms ***personally identifiable information***, which refers to information privacy, studies note that users may have to provide details about their metaverse accounts, demographics, finances, contacts, and IP addresses to access the metaverse, typically at the registration process (Deng and Ruan, 2009). This information is then stored within user accounts (Jaber, 2022). Moreover, personally identifiable information may also be collected during transactions (Venugopal et al., 2023). In addition, users may disclose this data to other users, as discussed by Maloney et al. (2020) and Sykownik et al. (2022).

The second data category is ***on-platform data***, another form of data that can potentially intrude information privacy, generated during interactions within virtual environments. Central to these interactions are avatars, which may reflect users' real or fictional looks (Awadallah et al., 2023; Venugopal et al., 2023). In addition, users may engage with various digital assets, including virtual goods, currencies, and real estates (Falchuk et al., 2018; Huang et al., 2023). Data about users' online activities and conversations can be recorded (Fernandez and Hui, 2022). Moreover, social connections such as friendships and group affiliations can be revealed (Martin, 2012; Wang et al., 2023).

The third category is ***physical body data***, entailing characteristics of an individual's body and thus refers to bodily privacy. Avatars replicating users may convey height, appearance, race, and gender (Maloney et al., 2020; Wang et al., 2021). A significant difference to the current Internet is the real-time tracking of movement and physiology, facilitated by XR technologies (Di Pietro and Cresci 2021; Marloth et al., 2020). Sensors can track gait as well as eye, head, and hand movements (Fernandez and Hui, 2022; Happa et al., 2021). This tracking is crucial for avatar animation (Venugopal et al., 2023), enabling the mimicry of users' gestures and facial expressions. In addition, attributes like gender, age, and abilities can be discerned through voice chat interactions (Maloney et al., 2020). Moreover, data collection may extend to biometric data, including voice prints, face geometry, eye scans, handprints, fingerprints, and

heart signals (Awadallah et al., 2023; Chen et al., 2022). Advanced sensors and brain-computer interfaces (BCI) may even capture neurophysiological data (Marloth et al., 2020; Smith et al., 2023).

Furthermore, the collection of ***physical territorial data*** may potentially jeopardize territorial privacy. XR devices equipped with cameras and sensors can capture real-time physical surroundings, including nearby objects and individuals (Dwivedi et al., 2023; Fernandez and Hui, 2022).

ID	Data types	PD	#	Reference Examples
	Personally identifiable information			
P1	Metaverse account (username, password, profile)	IP	16	Abraham et al., 2022; Cruz et al., 2015
P2	Demographic information (name, age, gender)	IP	12	Awadallah et al., 2023; Martin, 2012
P3	Financial information (credit card, bank account)	IP	8	Venugopal et al., 2023; Wang et al., 2023
P4	Contact information (email, phone, address)	IP	5	Adams et al., 2018; Deng and Ruan, 2009
P5	IP address	IP	4	Chen et al., 2022; Martin 2012
	On-platform data			
O1	User avatar (real, fictional look)	IP	20	Huang et al., 2023; Maloney et al., 2020
O2	Digital assets (item, currency, NFT, real estate)	IP	15	Awadallah et al. 2023; Huang et al., 2023
O3	Online activities	IP	14	Fernandez and Hui 2022; Kang et al., 2023
O4	Conversations (text, voice chat)	IP	10	Girvan and Savage, 2012; Vilela et al., 2010
O5	Social connections (friendship, membership)	IP	8	Fernandez and Hui, 2022; Martin, 2012
	Physical body data			
B1	Physical movement (eye, head, hand movement)	BP	22	Abraham et al., 2022; Wang et al., 2023
B2	Appearance and physiology (height, race)	BP	19	Huang et al., 2023; Maloney et al., 2020
B3	Biometric data (finger, voice, face print)	BP	16	Chen et al., 2022; Jaber, 2022
B4	Neurophysiological data (brain, neural activity)	BP	9	Marloth et al., 2020; Wang et al., 2023
	Physical territorial data			
T1	Surrounding (bystander, object)	TP	10	Adams et al. 2018; Venugopal et al., 2023
	Habitus data			
H1	Behavioral data	PP	18	Abraham et al., 2022; Wang et al., 2023
H2	Preferences and interests (hobby, lifestyle)	PP	17	Abraham et al., 2022; Huang et al., 2023
H3	Emotion	PP	11	McStay, 2023; Smith et al., 2023
	Context-specific data			
S1	Health data (medical record)	IP	5	Kang et al., 2023; Mejia and Rawat, 2022
S2	Private documents (marketing report)	IP	3	Kang et al., 2023; Salimian et al., 2016

Table 1. Data types identified through the systematic review.

Another crucial category is ***habitus data***, which can be derived from analyzing and aggregating prior data categories (Fernandez and Hui, 2022; Smith et al., 2023). This category includes insights into users' behavioral patterns, habits, preferences, and interests, thus referring to an individual's psychological privacy. For example, avatar choices may convey users' desires and feelings (Dwivedi et al., 2022). Emotions can be detected via cameras, pressure sensors monitoring facial expressions (McStay, 2023), voice recognition (Smith et al., 2023), or inferred from other physical body data (Abraham et al., 2022; Happa et al., 2021). Moreover, users may decide to share aspects like sexuality, lifestyle, beliefs, and emotions with fellow users for relationship building (Sykownik et al., 2022).

Lastly, individual studies have indicated that the metaverse may contain ***context-specific data***, such as sensitive health information in healthcare applications and confidential corporate documents in office applications (Dwivedi et al., 2022; Kang et al., 2023), representing hazards for information privacy.

3.3 Privacy challenges in the metaverse

We identified 27 privacy challenges, entailing both causes and consequences of privacy invasions in the metaverse, as the distinction between these often blurs, occurring seamlessly in time and space. Based on these challenges, we determined relevant stakeholders and classified them into users themselves (U), metaverse platforms (M), interactions with other users (I), cybercriminals (C), enterprises (E), and governments (G). Similar to data types, these challenges were also mapped to the previously introduced privacy dimensions. Each challenge was linked to the most relevant dimension, with consideration for potential intersections with multiple dimensions. Table 2 provides an aggregated overview of identified challenges and Figure 3 illustrates respective stakeholder relations within the metaverse ecosystem.

Privacy challenges related to users themselves. ***A lack of individuals' awareness and knowledge about privacy issues*** is pointed out in one third of the studies. Users are often unaware of the pervasive and ongoing data collection, whether through device sensors (Adams et al., 2018; Venugopal et al., 2023) or on the platform (Martin, 2012), and the insights that can be derived from integrating data from diverse sources (Abraham et al., 2022). Due to the intricate nature of the personal data collected, it is difficult for users to provide truly informed consent (Happa et al., 2021). Moreover, specific user groups, such as teenagers, often lack general security and privacy knowledge (Kang et al., 2023).

Privacy challenges related to metaverse platforms. Several studies noted the issue of ***insufficient provision of privacy notices to users***. Visualization methods often fail to convey broader implications of user consent, particularly when presented in unreadable license agreements (Abraham et al., 2022). Information about data processing is often opaque (Happa et al., 2021). Existing privacy notices within metaverse applications often lack clarity and sufficient descriptions of VR-specific data collection (Adams et al., 2018; Smith et al., 2023) and many social VR platforms fail to clearly inform users about privacy settings, leading to unintentional sharing of sensitive data (Kang et al., 2023; Maloney, 2020).

Some studies have addressed the concern of ***background tracking***, which is especially facilitated by the inherent visibility of user activities to the platform (Falchuk et al., 2018). Notably, this tracking is often integrated into platform laws and protocols (McStay, 2023), allowing effortless monitoring and data logging (Dwivedi et al., 2022). Furthermore, XR devices equipped with cameras and sensors can track user movements, capture conversations, and even monitor private spaces (Dwivedi et al., 2022).

The most prominent concern related to metaverse platforms, as noted by one fifth of the studies, is ***data leakage***, especially referring to security issues. This can result from corporate data breaches (Di Pietro and Cresci, 2021) and vulnerabilities in XR device, both in software and hardware (Happa et al., 2021). This concern is magnified by extensive data collection for avatars and operations (Wang et al., 2023).

Concerns about ***identity linking*** was extensively addressed by Martin (2012). For example, IP addresses and financial data can be exploited to connect various avatars and tie avatars to real individuals, raising challenges for users maintaining separate avatars for different purposes (Martin, 2012).

While most of the aforementioned challenges primarily refer to information privacy, ***algorithmic discrimination*** presents a concern for psychological privacy. The use of personal data in Artificial Intelligence (AI) algorithms in the metaverse may introduce biases, leading to possible discrimination based on factors like race and region (Dwivedi et al., 2023). Moreover, users may be segregated into different filter bubbles, each experiencing very different content or information (Abraham et al., 2022).

Privacy challenges related to interactions with other users. ***Cyber bullying and harassment*** stand out as the most prominent challenge, as highlighted in half of the studies, and is related to social privacy. Incidents of such misconduct, often targeting females, have been widely documented (Dwivedi et al., 2022; Huang et al., 2023). As with the current Internet, this issue is propelled by anonymity (Benrimoh et al., 2022) and the lack of accountability (Dwivedi et al., 2022). However, the intensity is expected to rise, largely due to added vulnerability of avatars (Benrimoh et al., 2022; Said, 2023) and synchronous voice chats (Dwivedi et al., 2023). Moreover, victims using sensory devices experience abuse more intensely (Raina et al., 2022). Furthermore, haptic feedbacks can enable physical assaults, including simulated punches, kicks, or inappropriate touching (Benrimoh et al., 2022; Dwivedi et al., 2023). This immersive and realistic experience can lead to profound psychological trauma (Smith et al., 2023).

ID	Potential challenges	PD	#	Reference Examples
	Privacy challenges related to users themselves			
U1	Lack of awareness and knowledge	-	15	Abraham et al., 2022; Adams et al., 2018
	Privacy challenges related to metaverse platforms			
M1	Insufficient privacy information	-	6	Adams et al., 2018; Harborth, 2022
M2	Background tracking	IP	5	Falchuk et al., 2018; McStay, 2023
M3	Data leakage	IP	9	Kang et al., 2023; Wang et al., 2023
M4	Identity linking	IP	3	Martin, 2012
M5	Algorithmic discrimination	PP	5	Abraham et al., 2022; Dwivedi et al., 2023
	Privacy challenges related to interactions with other users			
I1	Cyber bullying and harassment	SP	20	Dwivedi et al., 2022; Falchuk et al., 2018
I2	Cyber spying and stalking	SP	14	Di Pietro and Cresci, 2021; Wang et al., 2023
I3	Damage of reputation	IP	12	Di Pietro and Cresci, 2021; Dwivedi et al., 2023
I4	Information distribution without consent	IP	7	Boothe, 2022; Wang et al., 2021
I5	Virtual vandalism	VP	2	Abraham et al., 2022; Farahmand et al., 2013
	Privacy challenges related to cybercriminals			
C1	Network interception attack	IP	10	Huang et al., 2023; Mejia and Rawat, 2022
C2	Hacking	IP	14	Adams et al., 2018; Chen et al., 2022
C3	Malware	IP	7	Dwivedi et al., 2022; Vadlamudi, 2022
C4	False data injection and data tampering	IP	5	Mejia and Rawat, 2022; Wang et al., 2023
C5	Experience manipulation	PP	4	Abraham et al., 2022; Raina et al., 2022
C6	Credential theft	IP	9	Awadallah et al., 2023; Jaber, 2022
C7	Digital asset theft	VP	7	Dwivedi et al., 2023; Kang et al., 2023
C8	Identity theft	IP	19	Raina et al., 2022; Wang et al., 2023
C9	Social engineering and phishing	PP	16	Chen et al., 2022; Kang et al., 2023
C10	Impersonation	PP	12	Abraham et al., 2022: Chen et al., 2022
	Privacy challenges related to enterprises			
E1	Business model	IP	10	Harborth, 2022, McStay, 2023
E2	Data mining	IP	8	Dwivedi et al., 2022; McStay, 2023
E3	User profiling	PP	11	Di Pietro et al., 2021; Wang et al., 2023
E4	Targeted advertisement	PP	16	Dwivedi et al., 2022; McStay, 2023
	Privacy challenges related to governments			
G1	Surveillance	IP	7	Bibri, 2022; McStay, 2023
G2	Public opinion shaping	PP	3	Bibri, 2022; Dwivedi et al., 2023

Table 2. Privacy challenges identified through the systematic review.

The second largest threat of user interaction is ***cyber spying and stalking***, cited in one third of the studies. In the metaverse, users can track others' avatars, observe, and record their digital activities (Falchuk et al., 2018). Moreover, the third-person perspective facilitating a wider view of avatars' surroundings can be exploited to intrude upon others' social privacy (Wang et al., 2023). Users may also modify rendering and camera settings to see through barriers and eavesdrop on conversations (Vilela et al., 2010).

Regarding further inferring of information privacy through other users, more than a quarter of the studies have addressed the concern of ***reputation damage***. As the metaverse involves increased sharing of user data across platforms and users, worries have emerged about doxing, i.e., the misuse of personal

information for online shaming and extortion (Di Pietro and Cresci, 2021). Moreover, shallow and deep fakes may be used to harm someone's reputation (Mitrushchenkova, 2022).

Multiple studies also highlighted the issue of ***unauthorized information distribution***. The metaverse's capacity to generate lifelike avatars sparks concerns about digital cloning (Boothe, 2022). Moreover, privacy risks emerge when avatars are created from photos of unrelated individuals (Wang et al., 2021). Furthermore, confidential data within the metaverse may be leaked for financial gain (Kang et al., 2023).

Lastly, two studies mention ***virtual vandalism***, which refers to virtual territorial privacy and can result in the destruction of virtual properties and real estate (Farahmand et al., 2013). In AR, users may place stickers onto other users' virtual representations without their permission (Abraham et al., 2022).

Privacy challenges related to cybercriminals. The majority of identified issues (10 of 27; 37%) are linked to cyber criminality and can be mostly related to both information privacy and psychological privacy. Regarding information privacy, a quarter of the studies express concerns regarding ***network interception*** as the metaverse inherits security and privacy vulnerabilities from the Internet, which serves as its backbone (Huang et al., 2023). Man-in-the-middle attacks enable espionage and control over communication, often hard to detect in such user-heavy environments (Mejia and Rawat, 2022). Attackers may intercept communications between users, devices, and avatars (Vadlamudi, 2022; Wang et al., 2023), partly due to inadequate encryption measures (Dwivedi et al., 2022). These attacks could pose serious risks in office and healthcare applications (Kang et al., 2023; Mejia and Rawat, 2022).

On top of that, one third of the studies express concerns about ***hacking***, as the abundance of personal data attracts criminals (Chen et al., 2022). These concerns are exacerbated by security vulnerabilities in metaverse applications, stemming from complex data exchanges and inadequate cybercrime protection (Dwivedi et al., 2022). Furthermore, security responsibilities are often unclear, with some developers outsourcing them to storage services (Adams et al., 2018). Thus, hackers may target servers and storage to obtain sensitive information (Huang et al., 2023; Wang et al., 2023). Additionally, web attacks like cross-site scripting may exploit platforms employing web pages (Huang et al., 2023; Vladimirov et al., 2022). Moreover, the metaverse's underlying technologies introduce new attack avenues, like hacking XR devices, which are less worrisome in the current Internet (Dwivedi et al., 2022). Hackers could track user locations (Venugopal et al., 2023), access device sensors (Wang et al., 2023), and compromise voice and video recordings (Chen et al., 2022; Dwivedi et al., 2022). Furthermore, the use of BCIs raises additional concerns about potential hacking (Huang et al., 2023; Raina et al., 2022).

Closely tied to hacking is the threat of ***malware***, as highlighted in multiple studies. Metaverse devices are susceptible to malware (Vadlamudi, 2022), which can disrupt their operations or turn them into data sources (Kang et al., 2023). Moreover, the metaverse platform itself can be targeted by malware (Dwivedi et al., 2022). For example, Roblox experienced ransomware attacks with hackers infecting the system and demanding virtual currency (Dwivedi et al., 2023).

In terms of ***false data injection and data tampering***, attackers may manipulate user data and also cover their tracks (Vadlamudi, 2022; Wang et al., 2023). This issue extends to data poisoning attacks aimed at digital twins and AI models, where hackers manipulate training data to diminish model effectiveness (Huang et al., 2023; Wang et al., 2023). Moreover, hackers can inject false data into metaverse devices, potentially endangering lives in healthcare applications (Kang et al., 2023; Mejia and Rawat, 2022).

Four studies pointed out ***experience manipulation*** as an intrusion of psychological privacy. Attackers can compromise users' virtual experiences by manipulating avatars' perceptions and actions (Raina et al., 2022). Hacked XR devices may be manipulated to cause users to collide, fall, and suffer injuries, and users may be directed into dangerous real-world situations (Dwivedi et al., 2022; Raina et al., 2022).

One fifth of the studies highlighted ***credential theft***, a significant concern in shopping applications (Jaber, 2022; Vadlamudi, 2022). Malicious actors may employ various methods to gain unauthorized access, including AI-driven replication of biometrics to bypass authentication (Awadallah et al., 2023) and targeting wearable devices for credential theft (Jaber, 2022). Finger and eye tracking may be exploited to compromise passwords (Chen et al., 2022), resulting in financial fraud and illegal activities (Jaber, 2022). This can result in ***digital asset theft***, invading users' virtual territorial privacy. Given the

metaverse's economic systems and massive commercial transactions, privacy breaches can lead to the theft of user profiles, avatars, virtual goods, and currencies (Dwivedi et al., 2022; Kang et al., 2023).

Identity-related issues are frequently emphasized, primarily due to the difficulty in determining the true identity of individuals behind avatars (Farahmand et al., 2013). ***Identity theft***, discussed in 43% of the studies, emerges as the foremost cybercriminal threat. Stolen online user data can be used to reconstruct individuals' identities (Abraham et al., 2022; Dwivedi et al., 2023), potentially impacting the physical world (Dwivedi et al., 2022). ***Social engineering***, mentioned in 37% of the studies, is closely intertwined with identity theft but primarily invades psychological privacy through psychological manipulation to extract valuable information (Falchuk et al., 2018). Given the metaverse's economic structure and heightened social interactions, such attacks will rise (Huang et al., 2023; Kang et al., 2023). Moreover, stolen personal information may be exploited to enhance phishing or scam effectiveness (Huang et al., 2023). ***Impersonation***, a concern highlighted in 28% of the studies, often results from identity theft and serves as a means for social engineering. It is expected to become more accessible (Chen et al., 2022; Vadlamudi, 2022) and harder to detect (Awadallah et al., 2023) within the metaverse. User avatars may be replicated for impersonation purposes, facilitated by fully animated bots (Abraham et al., 2022). Furthermore, deep fake technologies can significantly enhance the ability to mimic user traits (Huang et al., 2023; Jaber, 2022). Beyond impersonating individual users, cybercriminals can also imitate organizations (Chen et al., 2022; Falchuk et al., 2018). For instance, they may create fake marketplaces resembling official ones, trapping users into spending money (Dwivedi et al., 2023; Huang et al., 2023).

Privacy challenges related to enterprises. In terms of information privacy, a quarter of the studies highlighted privacy concerns arising from the ***business models*** of metaverse companies, as many of them generate profits from the use and sale of user data (Chen et al., 2022; Dwivedi et al., 2022). This practice is particularly prevalent among platforms owned by tech giants (Harborth, 2022; McStay, 2023). In exchange for data collection, companies may offer free services to users (Benrimoh et al., 2022). Moreover, the appeal of user data to advertisers further motivates companies to collect and monetize such data (Dwivedi et al., 2022). On top of that, several studies raised concerns about ***data mining***. This involves aggregating user data from various devices, often using machine learning to uncover patterns (Dwivedi et al., 2023; Vadlamudi, 2022). It enables precise analysis of user experiences and behavior modeling based on quantified data, surpassing opinion-based surveys in traditional Internet research (Dwivedi et al., 2022). Furthermore, the dynamic environment of the metaverse facilitates experimentation, such as A/B testing, to understand consumer responses, assisting marketers and companies to refine their messages and products (Dwivedi et al., 2022; McStay, 2023). Real-time user reactions to services or products can be monitored, for example, by analyzing interaction data, heart rate, head movement, and gaze data (Awadallah et al., 2023).

User profiling, noted in a quarter of the studies, is facilitated by the diverse data types available in the metaverse (Vadlamudi, 2022; Wang et al., 2023) and can critically interfere with users' psychological privacy. For instance, in metaverse offices, various aspects of workers can be monitored, enabling detailed employee profiling (McStay, 2023). Moreover, health insurance companies may use XR data to predict illnesses and estimate life expectancy (Abraham et al., 2022). In the consumer sector, user profiling often forms the basis for ***targeted advertising***, highlighted in 37% of the studies, with a particular emphasis on habitus data (Abraham et al., 2022). This data can be used to adjust the quality and pricing of advertised goods or services (Adams et al., 2018). Furthermore, the dynamic environmental changes within the metaverse can be used for advertising purposes (McStay, 2023). These may include promotional elements that subconsciously engage users, tailored billboards, and personalized marketing AI avatars (Dwivedi et al., 2022; Dwivedi et al., 2023).

Privacy challenges related to governments. While governments are the least discussed stakeholder regarding metaverse privacy challenges, some studies mention the concern of ***surveillance*** as a form of information privacy intrusion. This could be driven by governments' interest in acquiring citizens' biometrics (McStay, 2023). Moreover, authoritarian states may leverage metaverse data and AI technologies to monitor citizens (Bibri, 2022). Furthermore, individual studies raise concerns about governments exploiting the metaverse to ***shape public opinion*** and thereby invading citizens'

psychological privacy. AI techniques may also be employed to manipulate people's beliefs and spread propaganda (Dwivedi et al., 2023), posing a threat to free will and critical thinking (Bibri, 2022).

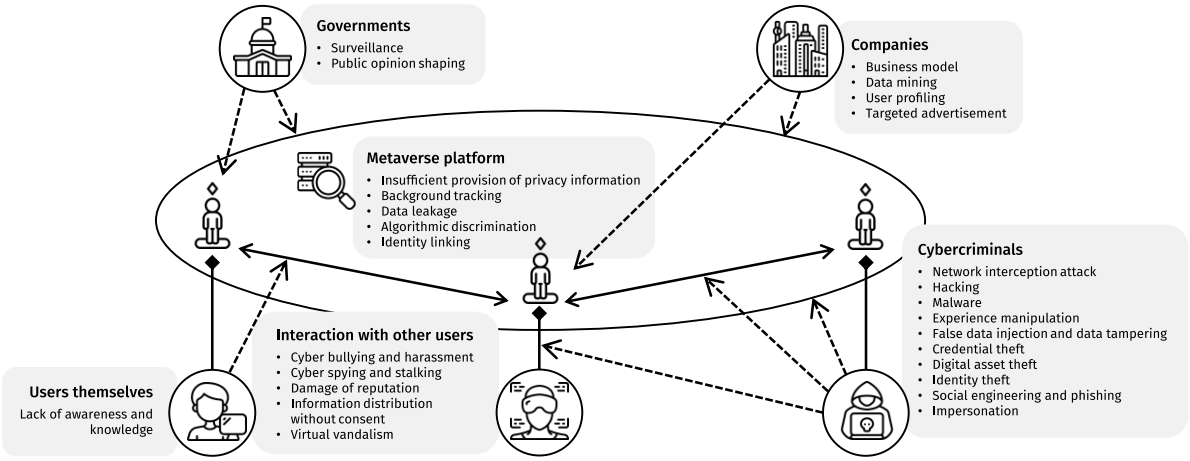

Figure 3. Overview of privacy challenges and stakeholder relations in the metaverse ecosystem.

4 Discussion and implications

This study provides an aggregated overview of the exposed data types and the associated privacy challenges within the metaverse based on a systematic synthesis of the existing literature. Overall, our review reveals that data collection and exposure in the metaverse greatly exceeds the depth and variety of the current Internet. Individuals and entities capable of compromising privacy and the majority of challenges align with those observed in OSNs (Ali et al., 2018; Jain et al., 2021; Kayes and Iamnitchi, 2017; Zhang et al., 2010). However, we observe that the metaverse introduces novel aspects across the six essential privacy dimensions, which are discussed in the following:

(1) Most data types and challenges can be associated to the dimension of ***information privacy***. While the collection of personally identifiable information is also common in OSNs (Kayes and Iamnitchi, 2017), the collection of on-platform data is forecast to be notably more extensive in the metaverse. Unlike current Internet platforms limited to tracking clicks, posts, likes, and site visits, the metaverse allows detailed tracking of avatar-based interactions with virtual objects and other users within virtual worlds (Dwivedi et al., 2022). While sensitive data in OSNs already attracts various stakeholders with adverse interests (Ali et al., 2018; Zhang et al., 2010), the growing value and volume of data in the metaverse heighten the stakeholders' interests to gain access to such data. Thus, the occurrence and severity of challenges related to information privacy are expected to escalate in the metaverse.

(2) XR devices with body-attached sensors expand ***bodily privacy*** concerns by utilizing the entire body as input, offering more detailed data than OSNs, which rely on mouse or touchscreen interactions. This is primarily attributed to the integration of the physical person and the virtual avatar. While individuals' appearances and biometrics can also be revealed in OSNs through the sharing of images and videos (Ali et al., 2018), in the metaverse, this real-time sensor tracking enhances data quantity and granularity, potentially entailing neurophysiological data. Unlike in OSNs, where users can freely decide on sharing body-related data, metaverse participation may obligate such data collection for operation and the unique experience. Furthermore, while input devices may intrude upon bodily privacy, the same applies to output devices, as haptic feedbacks may be exploited to cause inconvenient bodily contact.

(3) In terms of ***territorial privacy***, XR devices also use sensors to capture users' surroundings. While locational information may also be disclosed in OSNs through the sharing of pictures, videos, geotagged content, or GPS coordinates, leading to exposing information like where one lives and where one is traveling (Ali et al., 2018; Jain et al., 2021), XR devices' real-time tracking capabilities enable the

capture of immediate surroundings at a more granular level. Similar to bodily privacy, where users have the free choice to disclose this data in OSNs, access to the metaverse may require mandatory collection.

(4) Challenges related to ***social privacy,*** like bullying, harassment, and stalking, are also prevalent in OSNs (Tifferet, 2019). However, these challenges can be expected to intensify in the metaverse due to increased synchronous interaction opportunities. Perpetrators can exploit various channels such as text chat, voice chat, and avatar-based interactions to target victims. Despite the metaverse's ability to digitally replicate physical interactions, it lacks corresponding social norms like respectful behavior and social distance, driven by anonymity and the lack of real-world consequences for perpetrators, similar to OSNs (Chan et al., 2021; Jain et al., 2021). Moreover, the immersive nature of the metaverse may intensify the impact of intrusions on social privacy, potentially leading to psychological trauma.

(5) Regarding ***psychological privacy***, the metaverse's extensive data collection enables more natural and authentic inference of users' habitus and personas compared to OSNs. This not only raises concerns about the unauthorized analysis of users' psyches but also highlights questions about the control individuals have over their thoughts. While disinformation and sponsored content are pressing concerns in OSNs (Morrow et al., 2021), the metaverse offers even more opportunities for unwanted influences. Unlike OSNs, where user-generated contents mainly feature text, pictures, and videos, the metaverse includes 3D objects and immersive experiences. Moreover, the dynamic nature of the metaverse poses a significant threat to psychological privacy by impairing users' ability to discern reality from deception, endangering individual autonomy (Bibri, 2022; Harborth, 2022). This heightened risk also extends to social engineering and impersonation attacks, further exacerbated by the ease of replicating avatars.

(6) Finally, challenges regarding ***virtual territorial privacy*** are unique in the metaverse. These concerns, rooted in the real world, have received less attention so far compared to other privacy issues. The metaverse's ability to mirror real-world attributes in virtual realms, including properties and economies, raises issues akin to those in physical environments. Moreover, the integration of digital and physical economies, with seamless currency conversion, assigns real-world monetary value to virtual objects. On top of that, virtual properties can hold unique value for their owners and fulfill purposes analogous to physical objects (Hamari and Keronen, 2017; Jung and Pawlowski, 2014). Therefore, privacy breaches can lead to real-world financial losses and consequences, demanding heightened scrutiny and response.

In summary, the emergence of the metaverse will mark a profound shift in privacy research within information systems, which has previously centered on information privacy (Bélanger and Crossler, 2011; Smith et al., 2011). As the lines between virtual and physical privacy become increasingly blurred in this evolving landscape (Smith et al., 2023), examining privacy must include both digital and physical dimensions. Moreover, with the metaverse's advent, we may embark on a new privacy era, as historical precedents suggest that the understanding of privacy is driven by the IT evolution (Westin, 2003). As a result, current regulations like the GDPR may need reevaluation to prepare for this landscape.

Based on our findings, we derive seven key recommendations for researchers and practitioners that can serve as foundations to guide the development of appropriate privacy measures to address the challenges imposed by the respective stakeholder groups in the metaverse ecosystem (Figure 2) and pave the way to establish a safe and secure environment for virtual interaction in the metaverse.

(1) ***Increase user awareness***: The lack of privacy awareness among *users* highlights the need for innovative education methods regarding privacy risk and data collection in the metaverse. Given that metaverse users are generally young, it is crucial to develop effective strategies to reach and sensitize them. Moreover, considering the potential struggles faced by technology-illiterate users to grasp privacy intricacies, it is essential to implement foolproof privacy assurances by default (Gupta et al., 2023).

(2) ***Promote ethical practices on metaverse platforms***: To address insufficient privacy information, *platform providers* must integrate clear privacy notices. Strategies from 2D platforms may lack impact in 3D worlds, as it is crucial to balance user awareness without overwhelming them (Abraham et al., 2022). To reduce background tracking, platforms must adhere to data minimization principles, capturing only essential data for operations (Abraham et al., 2022). User data collection and processing should be transparent, relying on informed consent and serving legitimate purposes (Raina et al., 2022). Users should have the option to opt out non-essential tracking. Establishing standards, regulations, and

ensuring strict compliance are vital (McStay, 2023). Additionally, data masking and security protocols must be rigorously implemented to prevent user identification and data leaks. Moreover, developers must also consider the global and diverse user base of the metaverse to mitigate algorithmic biases. Transparency is essential when leveraging personal data for AI modeling and algorithmic decisions.

(3) ***Safeguard user interactions***: To ensure safe *user interactions*, platform providers must actively engage in moderation by establishing codes of conduct and reporting systems (Benrimoh et al., 2022). Linking offline and online identities for accountability is contentious (Sykownik et al., 2022), sparking significant debate also in OSN contexts (McCarthy et al., 2023), as it may jeopardize privacy at the same time (see identity linking). This decision can pose a dilemma, as it may entail weighing privacy concerns against potential misconduct by other users or the handling of personal data by platform providers. Nonetheless, platforms should offer customizable privacy settings and features allowing users to uphold social privacy and offline social norms. This can include safety bubbles to maintain social distances and access management, allowing users to choose their interaction partners. Moreover, effectively informing users about the implemented measures is crucial for their successful adoption (Falchuk et al. 2018).

(4) ***Guard against cybercriminals***: Given the abundance of sensitive personal data, platform providers must thwart *cybercriminal* interference. The metaverse's immaturity and its underlying technologies heighten vulnerability to cyberattacks, necessitating robust encryptions and security protocols for both infrastructure and data transfers (Kang et al., 2023). Moreover, XR devices should incorporate privacy-enhancing technology and security by design strategies. For instance, processing sensitive data directly on user devices can reduce exposure, especially for biometrics that are difficult to alter (Huang et al., 2023). Innovative identity management, verification, and authentication methods are essential to address identity-related challenges. In addition, law enforcement plays a crucial role in combating cybercrimes.

(5) ***Regulate data-hungry companies***: In terms of *enterprises*, compromised consumer privacy often results from data-driven business models, particularly those of monopolistic platforms. Providing transparent information to users regarding the purpose of data processing is imperative. While future platforms may prioritize user privacy, paradoxical behaviors may arise, similar as in OSNs (Kokolakis, 2017), as privacy-conscious users may remain on privacy-unfriendly platforms due to factors like user base, switching costs, or nudges. Thus, relying solely on the market for regulation is ideal, as observed in OSNs (Benrimoh et al., 2022). Therefore, effective regulation is crucial to protect consumers in the metaverse's ongoing development, preventing a recurrence of issues seen in OSNs. Moreover, methods must be established for assessing companies' compliance with regulations and ensuring enforcement.

(6) ***Discuss government interference***: To counteract *governmental* interference, it is essential to heighten awareness of the issues and stimulate discussions and open dialogues within the general public.

(7) ***Protect psychological privacy***: To combat manipulation by diverse *stakeholders* like enterprises (advertising), governments (opinion shaping), and cybercriminals (impersonation), platform providers must assist users in navigating this complex landscape. Adopting practices from OSNs, such as content labeling and moderation (Morrow et al., 2022), is essential. Moreover, our findings reveal the pivotal role of AI in manipulation, especially avatar-based deep fakes. Alongside regulatory actions, deploying technological solutions like intelligent systems for deepfake detection is crucial (Gupta et al., 2023).

5 Limitations and Future Research

As is common in any research, our study comes with certain limitations. Although the search strategy was selected and tested to include all relevant studies on privacy in the metaverse, it is possible that some relevant studies were not included in this review (e.g., studies not available in English). In addition, despite basing our analysis on established frameworks, following a systematic data extraction and analysis as well as extensive discussions among the authors, the classification of data types and privacy challenges may still be subject to bias. Future research should attempt to address such possible biases in the data selection, extraction, and analysis. Moreover, from a methodological standpoint, we found that most research on privacy in the metaverse is conceptual. Therefore, we strongly encourage researchers to conduct empirical studies in this domain. Further, while considerable research examines interpersonal

and consumer privacy challenges, there is a lack of studies addressing citizen and employee privacy. In similar vein, our research revealed a limited focus on workplace and healthcare contexts, where privacy is notably crucial. Thus, there is a clear need for dedicated research to address these contextual gaps.

Appendix

Study	Context	Method	Data types	Privacy challenges
Abraham et al., 2022	General	Interview	P1, P2, O1, O3, B1, B2, T1, H1, H2, H3	U1, M1, M5, I5, C5, C6, C8, C10, E4
Adams et al., 2018	General	Mixed	P1, P4, B1, B3, T1, H3	U1, M1, M3, I1, C2, C6, C8, E1, E4
Awadallah et al., 2023	General	Conceptual	P1, P2, P3, O1, O2, O3, B1, B2, B3, B4, H1, H2	I3, C1, C3, C6, C8, C9, C10, E2, E4, R17
Benrimoh et al., 2022	Healthcare	Conceptual	S1	I1, E1, E3, E4
Bibri, 2022	General	Conceptual	B2, B4, H1, H3	E1, E2, E3, G1, G2
Boothe, 2022	Leisure	Case study	B2	I1, I3, I4, C8
Chen et al., 2022	General	Conceptual	P1, P5, B1, B3	I1, C2, C3, C6, C8, C9, C10, E1
Cruz et al., 2015	Education	Conceptual	P1, P5	M4, C6, C10
Deng and Ruan, 2009	General	Conceptual	P1, P2, P3, P4, P5, O1, O2, O3, H1, H2	I1, I3, C8
Di Pietro and Cresci, 2021	General	Conceptual	P2, O1, O3, B1, B2, B4, H1, H2	U1, M3, M5, I1, I2, I3, I4, C9, E3, E4
Dwivedi et al., 2022	General	Conceptual	P1, P2, P3, P4, O1, O2, O3, O4, O5, B1, B2, B3, T1, H1, H2, H3	M2, M3, I1, I2, C1, C2, C3, C5, C7, C8, C9, C10, E1, E2, E3, E4
Dwivedi et al., 2023	General	Conceptual	P1, P2, O1, O2, B1, B3, T1, H1, H3, S1	M2, M3, M5, I1, I2, I3, C2, C3, C7, C8, C9, C10, E2, E3, E4, G2
Falchuk et al., 2018	General	Conceptual	O1, O2, O3, O5, H1, H2	U1, M2, I1, I2, C8, C9, C10, E4, G1
Farahmand et al., 2013	Education	Survey	P1, O2	I1, I2, I3, I5, C6, C7, C8
Fernandez and Hui, 2022	General	Conceptual	O1, O2, O3, O4, O5, B1, B3, H2	I1, I2, C2, C5
Girvan and Savage, 2012	Education	Conceptual	P1, O1, O4	U1, M4, I2, G1
Gupta et al., 2023	General	Conceptual		I1, I2, I3, C2, C8, C10
Happa et al., 2021	General	Conceptual	B1, B2, B3, H3	U1, M1, M3, I3, C8, E1, E3
Harborth, 2022	General	Conceptual	T1, H1	U1, M1, E1
Heider and Massanari, 2010	General	Mixed	P1, O2, O4, O5, H1, H2	
Huang et al., 2023	General	Conceptual	O1, O2, O3, O5, B1, B2, B3, T1, H2, S1	U1, M3, I1, C1, C2, C4, C6, C7, C8, C9, E1, E3, E4
Jaber, 2022	General	Conceptual	P1, P2, P3, B3	I1, C1, C2, C3, C6, C8, C9
Kang et al., 2023	General	Conceptual	O2, O3, B2, B3, H1, H2, S1, S2	U1, M2, M3, I4, C1, C2, C3, C4, C7, C8, C9, E4, G1
Maloney et al., 2020	Leisure	Interview	P1, P2, O1, O4, B1, B2, B3, H3	U1, I2
Marloth et al., 2020	Healthcare	Conceptual	B1, B2, B4, H1	E2, E4
Martin, 2012	General	Case study	P1, P2, P3, P4, P5, O1, O2, O3, O4, O5, H2	U1, M4, I2, I3, G1
McStay, 2023	General	Conceptual	O1, O2, O3, B1, B2, B3, B4, H2, H3	M2, C1, C9, E1, E2, E3, E4, G1
Mejia and Rawat, 2022	Healthcare	Conceptual	B2, S1	C1, C4, C9, C10
Men and Zhao, 2021	Workspace	Experiment	B1	
Mitrushchenkova, 2022	General	Conceptual		I1, I2, I3, I4, G1, G2
Raina et al., 2022	General	Conceptual	O1, O2, O5, B1, B2, B3, B4, H1, H2	I1, I3, C2, C5, C8, C9, C10, E1
Reilly et al., 2014	Workspace	Prototype	S2	
Said, 2023	Education	Interview	B1	U1, I1
Salimian et al., 2016	Workspace	Experiment	S2	U1, M1
Smith et al., 2023	Education	Case study	O1, O3, O4, B1, B2, B3, B4, H2, H3	M1, I1, I4, C8
Sykownik et al., 2022	Leisure	Survey	P1, P2, P4, O1, O4, B1, B2, H1, H2, H3	I1
Tricomi et al., 2023	General	Experiment	P2, B1, H1	I1, E3, E4
Vadlamudi, 2022	General	Conceptual	P3, O1, O2, O3, B1, B2, T1, H1, H2	U1, M5, I2, C1, C2, C3, C4, C6, C7, C8, C9, C10, E2, E3, E4
Venugopal et al., 2023	General	Conceptual	P3, B1, B2, B3, B4, T1, H1	U1, M3, C2, E2, E4
Vilela et al., 2010	Education	Conceptual	O1, O4	I2, C9
Vladimirov et al., 2022	General	Conceptual	O1, B2	I3, C1, C2, C9
Wang et al., 2021	General	Experiment	T1	I4
Wang et al., 2023	General	Conceptual	P1, P2, P3, O1, O2, O3, O4, O5, B1, B3, B4, T1, H1, H2, H3	M3, M5, I2, I4, C1, C2, C4, C7, C8, C9, C10, E3, E4

Table 3. Literature overview and mapping to identified data types and privacy challenges.

Acknowledgments

The research project PRIME (www.privacy-metaverse.de) underlying this paper was funded by the German Federal Ministry of Education and Research (BMBF) under funding code 16KIS1894K. Responsibility for the content of this publication lies with the authors.

References

Abraham, M., Saeghe, P., McGill, M., and Khamis, M. (2022). "Implications of XR on Privacy, Security and Behaviour: Insights from Experts," *Nordic Human-Computer Interaction Conference*, 1-12.

Adams, D., Bah, A., Barwulor, C., Musabay, N., Pitkin, K., and Redmiles, E. M. (2018). "Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality," *USENIX Symposium on Usable Privacy and Security*, Baltimore, MD, USA, 443-458.

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., Rodrigues, J. J. P. C. (2018). "Privacy and Security Issues in Online Social Networks," *Future Internet* 10 (12), 114, 1-12.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole.

Awadallah, A. M., Damiani, E., Zemerly, J., and Yeun, C. Y. (2023). "Identity Threats in the Metaverse and Future Research Opportunities," *International Conference on Business Analytics for Technology and Security*, Dubai, United Arab Emirates, 1-6.

Baas, J., Schotten, M., Plume, A., Côté, G., and Karimi, R. (2020). "Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies," *Quantitative Science Studies* 1 (1), 377-386.

Bélanger, F., and Crossler, R. E. (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* 35 (4), 1017-1041.

Benrimoh, D., Chheda, F. D., and Margolese, H. C. (2022). "The Best Predictor of the Future – the Metaverse, Mental Health, and Lessons Learned From Current Technologies," *JMIR Mental Health* 9 (10), e40410.

Bibri, S. E. (2022). "The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society," *Smart Cities* 5 (3), 832-874.

Boothe, A. (2022). "The death and life of Jang Nayeon: A case for personality rights in the digital layers of reality," *International Journal of Law and Information Technology* 30 (4), 398-422.

Chan, T. K. H., Cheung, C. M. K., and Lee, Z. W. Y. (2021). "Cyberbullying on social networking sites: A literature review and future research directions," *Information & Management* 58 (2), 103411.

Chen, Z., Wu, J., Gan, W., and Qi, Z. (2022). "Metaverse Security and Privacy: An Overview," *IEEE International Conference on Big Data*, Osaka, Japan, 2950-2959.

Cruz, G., Costa, A., Martins, P., Gonçalves, R., and Barroso, J. (2015). "Toward educational virtual worlds: Should identity federation be a concern?" *Educational Technology & Society* 18 (1), 27-36.

Custers, N., Dechesne, F., Sears, A. M., Tani, T., and van der Hof, S. (2018). "A comparison of data protection legislation and policies across the EU," *Computer Law & Security Review* 34, 234-243.

Deng, X., and Ruan, J. (2009). "Users' privacy in the second life library," *IEEE International Symposium on IT in Medicine and Education*, Jinan, China, 337-340.

Di Pietro, R., and Cresci, S. (2021). "Metaverse: Security and Privacy Issues," *IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*, 281-288.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... Wamba, S. F. (2022). "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International Journal of Information Management* 66, 102542, 1-55.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... Yan, M. (2023). "Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse," *Information Systems Frontiers* 25, 2071-2114.

Falchuk, B., Loeb, S., and Neff, R. (2018). "The Social Metaverse: Battle for Privacy," *IEEE Technology and Society Magazine* 37 (2), 52-61.

Farahmand, F., Yadav, A., and Spafford, E. H. (2013). "Risks and uncertainties in virtual worlds: An educators' perspective," *Journal of Computing in Higher Education* 25, 49-67.

Fernandez, C. B., and Hui, P. (2022). "Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse," *IEEE International Conference on Distributed Computing Systems Workshops*, Bologna, Italy, 272-277.

Girvan, C., and Savage, T. (2012). "Ethical considerations for educational research in a virtual world," *Interactive Learning Environments* 20 (3), 239-251.
Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., and Shabaz, M. (2023). "Metaverse Security: Issues, Challenges and a Viable ZTA Model," *Electronics* 12 (2), 391, 1-13.
Hamari, J., and Keronen, L. (2017). "Why do people buy virtual goods: A meta-analysis," *Computers in Human Behavior* 71, 59-69.
Happa, J., Steed, A., and Glencross, M. (2021). "Privacy-certification standards for extended-reality devices and services," *IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops*, Lisbon, Portugal, 397-398.
Harborth, D. (2022). "Human Autonomy in the Era of Augmented Reality – A Roadmap for Future Work," *Information* 13 (6), 289, 1-10.
Heider, D., and Massanari, A. L. (2010). "Friendship, Closeness and Disclosure in Second Life," *International Journal of Gaming and Computer-Mediated Simulations* 2 (3), 61-74.
Huang, Y., Li, Y. J., and Cai, Z. (2023). "Security and Privacy in Metaverse: A Comprehensive Survey," *Big Data Mining and Analytics* 6 (2), 234-247.
Jaber, T. A. (2022). "Security Risks of the Metaverse World," *International Journal of Interactive Mobile Technologies* 16 (13), 4-14.
Jain, A. K., Sahoo, S. R., and Kaubiyal, J. (2021). "Online social networks security and privacy: comprehensive review and analysis," *Complex & Intelligent Systems* 7, 2157-2177.
Jung, Y., and Pawlowski, S. D. (2014). "Virtual goods, real goals: Exploring means-end goal structures of consumers in social virtual worlds," *Information & Management* 51 (5), 520-531.
Kang, G., Koo, J., and Kim, Y.-G. (2023). "Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective," *IEEE Communications Magazine* 62 (1), 1-7.
Kayes, I., and Iamnitchi, A. (2017). "Privacy and security in online social networks: A survey," *Online Social Networks and Media* 3-4, 1-21.
Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* 64, 122-134.
Maloney, D., Zamanifard, S., and Freeman, G. (2020). "Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality," *ACM Symposium on Virtual Reality Software and Technology*.
Margulis, S. T. (1977). "Conceptions of privacy: Current status and next steps," *Journal of Social Issues* 33 (3), 5-21.
Marloth, M., Chandler, J., and Vogeley, K. (2020). "Psychiatric Interventions in Virtual Reality: Why We Need an Ethical Framework," *Cambridge Quarterly of Healthcare Ethics* 29 (4), 574-584.
Martin, J. (2012). "Second Life Surveillance: Power to the People or Virtual Surveillance Society?" *Surveillance & Society* 9 (4), 408-423.
McCarthy, S., Rowan, W., Mahony, C., and Vergne, A. (2023). "The dark side of digitalization and social media platform governance: a citizen engagement study," *Internet Research* 33 (6), 1-33.
McStay, A. (2023). "The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons," *Philosophy and Technology* 36, 13, 1-26.
Mejia, J. M. R., and Rawat, D. B. (2022). "Recent Advances in a Medical Domain Metaverse: Status, Challenges, and Perspective," *International Conference on Ubiquitous and Future Networks*.
Men, L., and Zhao, D. (2021). "Designing privacy for collaborative music making in virtual reality," *International Audio Mostly Conference*, 93-100.
Mitrushchenkova, A. N. (2022). "Personal Identity in the Metaverse: Challenges and Risks," *Kutafin Law Review* 9 (4), 793-817.
Morrow, G., Swire-Thompson, B., Polny, J. M., Kopec, M., and Wihbey, J. P. (2022). "The emerging science of content labeling: Contextualizing social media content moderation," *Journal of the Associations for Information Science and Technology* 73 (10), 1365-1386.
Neuendorf, K. A. (2017). *The content analysis guidebook*. SAGE Publications, Inc.
Paré, G., Trudel, M.-C., Jaana, M., and Kitsiou, S. (2015). "Synthesizing information systems knowledge: A typology of literature reviews," *Information and Management* 52 (2), 183-199.
Raina, V., Srinivas, J., and Shilpa, M. S. (2022). "Metaverse - The New Age Empire : Relinquishing Our Identity to Acquire Digital Immortality," *International Conference on Futuristic Technologies*.

Reilly, D., Salimian, M., MacKay, B., Mathiasen, N., Edwards, W. K., and Franz, J. (2014). "SecSpace: Prototyping Usable Privacy and Security for Mixed Reality Collaborative Environments," *ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, 273-282.

Said, G. R. E. (2023). "Metaverse-Based Learning Opportunities and Challenges: A Phenomenological Metaverse Human–Computer Interaction Study," *Electronics* 12 (6), 1379, 1-13.

Salimian, M., Reilly, D., Brooks, S., and MacKay, B. (2016). "Physical-digital privacy for mixed reality collaboration: An exploratory study," *ACM International Conference on Interactive Surfaces and Spaces: Nature Meets Interactive Surfaces*, 261-270.

Schoeman, F. D. (1992). *Privacy and Social Freedom*. Cambridge University Press.

Smith, H. J., Dinev, T., and Xu, H. (2011). "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* 35 (4), 989-1015.

Smith, C. H., Molka-Danielsen, J., Rasool, J., and Webb-Benjamin, J.-B. (2023). "The World as an Interface: Exploring the Ethical Challenges of the Emerging Metaverse," *Hawaii International Conference on System Sciences*, 6045-6054.

Sykownik, P., Maloney, D., Freeman, G., and Masuch, M. (2022). "Something Personal from the Metaverse: Goals, Topics, and Contextual Factors of Self-Disclosure in Commercial Social VR," *CHI Conference on Human Factors in Computing Systems*, 632, 1-17.

Thomas, D. R. (2006). "A General Inductive Approach for Analyzing Qualitative Evaluation Data," *American Journal of Evaluation* 27 (2), 237-246.

Tifferet, S. (2019). "Gender differences in privacy tendencies on social network sites: A meta-analysis," *Computers in Human Behavior* 93, 1-12.

Tricomi, P. P., Nenna, F., Pajola, L., Conti, M., and Gamberini, L. (2023). "You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality," *IEEE Access* 11, 9859-9875.

Vadlamudi, S. (2022). "The Taxonomy of Security issues and Countermeasures in the Metaverse World," *International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems*, Hyderabad, India, 553-558.

Venugopal, J. P., Subramanian, A. A. V., and Peatchimuthu, J. (2023). "The realm of metaverse: A survey," *Computer Animation and Virtual Worlds* 34 (5), e2150, 1-28.

Vilela, A., Cardoso, M., Martins, D., Santos, A., Moreira, L., Paredes, H., ... Morgado, L. (2010). "Privacy Challenges and Methods for Virtual Classrooms in Second Life Grid and OpenSimulator," *International Conference on Games and Virtual Worlds for Serious Applications*, 167-174.

Vladimirov, I., Nenova, M., Nikolova, D., and Terneva, Z. (2022). "Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey," *International Scientific Conference on Information, Communication and Energy Systems and Technologies*, Ohrid, North Macedonia, 1-4.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Pattfaut, R., and Cleven, A. (2009). "Reconstructing the Giant. On the Importance of Rigour in Documenting the Literature Search Process," *European Conference on Information Systems*, 1-14.

Wang, C. Y., Sriram, S., and Won, A. S. (2021). "Shared realities: Avatar identification and privacy concerns in reconstructed experiences," *ACM on Human-Computer Interaction* 5, 337, 1-25.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., and Shen, X. (2023). "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Communications Surveys and Tutorials* 25 (1), 319-352.

Webster, J., and Watson, R. T. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* 26 (2), xiii-xxiii.

Warren, S., and Brandeis, L. (1890). "The Right to Privacy," *Harvard Law Review* 4 (5), 193-220.

Westin, A. F. (1967). *Privacy & Freedom*. London: The Bodley Head.

Westin, A. F. (2003). "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59 (2), 431-453.

Zhang, C., Sun, J., Zhu, X., and Fang, Y. (2010). "Privacy and security for online social networks: challenges and opportunities," *IEEE Network* 24 (4), 13-18.

Zhang, N. A., Wang, C. A., Karahanna, E., and Xu, Y. (2022). "Peer Privacy Concern: Conceptualization and Measurement", *MIS Quarterly* 46 (1), 491-529.