7-8-2023

Guardians of the Metaverse: Expert Assessment of Emerging Privacy Challenges and Mitigation Strategies

Julia Schulmeyer
LMU Munich School of Management, schulmeyer@lmu.de

Guardians of the Metaverse: Expert Assessment of Emerging Privacy Challenges and Mitigation Strategies

Completed Research Paper

Julia Schulmeyer
LMU Munich School of Management
Ludwigstr. 28, 80539 Munich
schulmeyer@lmu.de

Abstract

The metaverse describes persistent and interconnected 3D multi-user environments that are characterized by the fusion of physical and virtual worlds. Fueled by the rebranding of Meta, the metaverse is experiencing a resurgence and has attracted the attention of practitioners and scholars, resulting in a new wave of publications. While cutting-edge technologies offer unprecedented immersive experiences, users face new privacy situations as metaverse technologies require extensive data collection. Additionally, the spatial nature of the metaverse allows for the observation of digital footprints. This changing context of data disclosure necessitates a re-evaluation of privacy. Building on the Multidimensional Development Theory as an overarching framework, I conducted 35 expert interviews, resulting in 16 emerging privacy challenges and corresponding privacy protection measures. With these findings, this paper contributes to research on today's metaverse by empirically investigating privacy as a crucial aspect and providing practical recommendations for organizations to mitigate negative user reactions.

Keywords: Metaverse, privacy, multidimensional development theory, expert interviews

Introduction

The *metaverse* is currently experiencing a renaissance. Internet searches on the term increased by 7,200 percent in 2021 (McKinsey 2022a) and publications have risen rapidly (Polyviou and Pappas 2022). In the first half of 2022, the word "metaverse" appeared more than 1,100 times in U.S. regulatory filings compared to 260 mentions in 2021 and less than twelve in the previous two decades (Ball 2022). The metaverse describes the idea of a three-dimensional (3D) virtual world in which people interact, work, and consume as avatars, which is the digital representation of a human body in a virtual space (Dionisio et al. 2013). The metaverse is characterized by an increasing fusion of physical and virtual environments, accompanied by a shift from two-dimensional media to 3D and more immersive virtual spaces that extend the real world (Boughzala et al. 2012; Wang et al. 2022). Immersion is a central characteristic of the metaverse (Ball 2020) and relates to the mental state of being completely absorbed by the activities in a virtual environment (Witmer and Singer 1998). Therefore, instead of being mere spectators, users experience a sense of social presence in the metaverse (Peukert et al. 2022).

Numerous reports predict the great economic impact of the metaverse. A McKinsey (2022b) study estimates the potential value of the metaverse market up to five trillion US dollars by 2030. According to Citibank and KPMG, the metaverse could account for 13 trillion US dollars in revenue annually by 2030 (Ball 2022). Large companies are investing millions in building the metaverse or preparing for it. Besides the economic impact, experts assume that the metaverse will change how people socialize, do business, and entertain. Moreover, the metaverse has the potential to influence users' perceptions and behaviors (Dwivedi et al. 2022). Despite its outstanding possibilities for interaction and behaviors, the metaverse also represents a

new and unexplored context of data sharing. Contemporary metaverse applications collect new forms of sensitive data such as facial features, eye movements, haptics, and surroundings. Using machine learning algorithms, these data can reveal intimate information, such as health statuses or personality traits (Bao et al. 2022; Di Pietro and Cresci 2021). Further, online behavior is not only observable by metaverse providers but also by other users which paves the way for social attacks such as harassment or stalking (Falchuk et al. 2018). Due to these changed contextual conditions, *privacy* challenges must be reassessed and privacy decisions reevaluated (Acquisti 2015). In a study, privacy was named 86 percent as the top risk of the metaverse, which shows its priority for organizations (McKinsey 2022b).

While metaverse and virtual worlds have been common themes in the information systems (IS) literature (Boughzala et al. 2012; Mennecke et al. 2008), recent papers point to the relevance of identifying privacy risks that arise in the current understanding of the metaverse to mitigate their negative consequences (Dincelli and Yayla 2022). While regulatory institutions have a natural role in enabling privacy protection, companies are interested in protecting users' privacy as studies show that privacy intrusion reduces use intentions and data disclosure, thus leading to negative economic outcomes (Smith et al. 2011). Further, the degree of data disclosure influences users' emotions, thoughts, and behaviors, which has an impact on users experiences (Acquisti 2015). Due to the relevance of privacy for creating metaverse services, this study explores privacy challenges and potential mitigation strategies in this new environment. By conducting qualitative expert interviews, I aim to answer the following research questions (RQ):

RQ1: *What are the privacy challenges that arise from the emergence of the metaverse?*

RQ2: *What are privacy protection measures that can be applied to mitigate the privacy challenges in the metaverse?*

To answer the RQ, the paper is structured as follows. In section two, the theoretical foundations on privacy and the metaverse are introduced. In section three, I present the methodological approach, which includes a comprehensive description on the procedure of the expert interviews. Next, I demonstrate the results in section four which includes 16 identified privacy challenges clustered along the multidimensional development theory (MDT). I discuss the results and their implications for privacy behavior in section five. Lastly, in section six, I present a conclusion, limitations and make recommendations for future research.

The paper contributes to the IS literature in several ways. First, by empirically conducting 35 interviews with metaverse experts on the topic of privacy, it enriches existing metaverse studies by focusing on privacy as an important pillar of the emergence of the current metaverse, which is reflected in numerous calls for research (Dincelli and Yayla 2022). By clustering the results along the MDT as a common privacy framework in the IS, the new context metaverse is applied in a systematic way to existing privacy literature. Furthermore, by reviewing previous literature on privacy in the metaverse, the paper ties in with the current state of knowledge and thus offers a timely documentation of previous works. Lastly, besides scholars, also practitioners are highly interested in the metaverse as a new business opportunity to create innovative user experiences and enable front-edge interactions. As privacy plays an important role for use intentions and data disclosure (Smith et al. 2011), the paper offers relevant practical implications by identifying the privacy challenges and recommending tangible privacy protection measures.

Theoretical foundations

Information privacy and multidimensional development theory

Privacy is a concept that has been researched comprehensively in the IS domain. The first definition dates back to 1890 when Warren and Brandeis (1890) described privacy as "the general right of the individual to be left alone" (p. 205). Rather than describing privacy value-based as an absolute right, Westin (1968) and Altman (1975) define privacy as a state of limited access and thereby follow a cognate-based understanding. Based on these definitions, Margulis (1977) explains privacy as the control of transactions with the goal of increasing autonomy and minimizing vulnerability. While the historical definition of privacy is oriented towards the physical access to an individual and its surroundings, a new definition has emerged with the advent of digital technologies. The recent and widespread understanding of privacy as "information privacy" describes an individual's desire to control personal data and influence its dissemination (Bélanger and Crossler 2011; Smith et al. 2011). It represents an umbrella term for the disadvantages emerging from information collection, processing, and dissemination (Solove 2007). In many rigorous empirical studies,

mainly based on the positivist domain, privacy is operationalized by the construct of "privacy concerns", which is defined as an individual's concerns regarding the data-handling practices of organizations (Smith et al. 1996). Information privacy, as an ever-evolving concept in IS, has been explored in many contexts and from different perspectives (Smith et al. 2011). Scholars continually point out that privacy is a concept that changes in fields, over time, and in contexts. Acquisti (2004) emphasizes that it should rather be seen as a class of multifaceted interests than as a single, unambiguous concept. This implies that privacy highly depends on the context, for example, to the purpose or type of data collection (Smith et al. 2011). A relevant driver of new privacy risks is technological advancements. The pace of the development of new digital solutions for data collection and processing has continued to fasten, leading to new determinants of concern (Kallemeyn and Chipidza 2021). Kallemeyn and Chipidza (2021) state that "privacy will continue to change and be affected by new modes and frontiers of information accumulation." (p. 3). This demonstrates that technological innovation is a primary trigger for the emergence of new privacy concerns and thus constantly causes privacy studies (Cichy et al. 2021).

Laufer and Wolfe (1977) developed an established framework for determining privacy concerns in specific contexts in terms of their *multidimensional development theory* (MDT). The MDT explains the emergence of individuals' privacy concerns by three determinants. These include: an individual's environment (environmental), their experiences (personal), and their interactions (interpersonal). The environmental dimension explains how privacy concerns are a result of cultural, social, and physical settings' impacts. The personal determinant describes the developmental process of an individual, including their experiences and attitudes that shape the concept of privacy (Laufer and Wolfe 1977). This dimension sets the boundaries of privacy meaning and experience and influences an individual's capability to perceive and use available privacy options (Hong et al. 2019). Lastly, interpersonal interaction refers to communication and information exchange with others (Laufer and Wolfe 1977). The interpersonal dimension includes two sub-concepts: information management and interaction management. Whereas information management refers to the balancing of benefits and risks of data disclosure, interaction management describes the management of social interaction. The framework is a suitable theoretical basis for exploring privacy concerns in a new context such as the metaverse. While the majority of theories in privacy settings are based on the privacy calculus, the MDT provides a more comprehensive understanding of antecedents of privacy concerns (Hong et al. 2019). Further, the three-dimensional angle provides an appropriate and systematic foundation to classify the privacy challenges.

Metaverse

Fundamentals

The metaverse describes a new wave of technological innovation characterized by virtual worlds that provide unprecedented ways of interaction between users and their surroundings (Bao et al. 2022). The historical definition of the metaverse was coined by Neil Stephenson (1992) in the novel "Snow Crash". Therein, the metaverse is described as a massively scaled multi-user three-dimensional computer-generated virtual world that humans can enter in the form of avatars. A plethora of definitions currently exists for the metaverse, depending on the author's perspective and purpose of the definition (Dwivedi et al. 2022). Bao et al. (2022) denote the metaverse as "a catch-all term that refers to the entire digital and virtual world" (p. 1), which demonstrates the heterogeneity of its definitions. While some practitioners regard the metaverse as an existing application, others argue that the concept has not reached its final state (Peukert et al. 2022). Subsequently, an increasing number of definitions and frameworks from practice and academia emerge that aim at providing explanations for the phenomenon (Dwivedi et al. 2022). Despite the heterogenous use, the concept is generally gaining relevance, as evidenced by a substantial increase in scientific and practice-oriented publications (Polyviou and Pappas 2022). In its fundamental concept, the recent understanding defines the metaverse as a persistent multi-user virtual environment that increasingly merges the physical and digital worlds (Mystakidis 2022). Some studies introduce metaverse applications, also called "proto-metaverses", like Horizon Workrooms, Minecraft, Roblox, or Fortnite (Peukert et al. 2022). Dolata and Schwabe (2023) differentiate between *the* metaverse which refers to the general technological trend and *a* metaverse which describes existing prototypes of the metaverse.

The metaverse has been a common theme in IS (Davis et al. 2009). In a first wave of publications, scholars have investigated early virtual worlds such as "Second Life" that share some characteristics with today's understanding, such as the possibility of creating avatars or assets, and moving through a variety of virtual

environments. The focus of these papers has been mainly on massively multiplayer online role-playing games (MMORPGs), which are seen as a predecessor of the metaverse. MMORPGs are social online environments in which millions of people communicate, collaborate, and compete as avatars (Boughzala et al. 2012). Due to technological advancements and changed framework conditions, Second Life and comparable 2000s virtual worlds have only partial similarities with today's understanding of the metaverse (Park and Kim 2022). The current metaverse combines various cutting-edge technologies that enable its characteristic properties such as high immersion and interoperability, which describes the possibility of walking seamlessly through virtual worlds. From recent studies, it becomes apparent that especially two technologies are seen as building blocks of the metaverse. The first decisive technology is extended reality (XR), including augmented reality (AR), virtual reality (VR), and mixed reality (MR) (Boughzala et al. 2012). XR is an umbrella term for immersive technologies that enable data to be projected in digital environments, enabling the shift from two-dimensional to 3D immersive experiences (Mystakidis 2022). XR hardware, such as the VR device "Meta Quest 2", experience mass adoption due to affordable pricing and good usability. The second crucial technology is "web3", including blockchain elements, such as cryptocurrencies and non-fungible tokens (NFT), that facilitate the digital representation of assets in the virtual world as well as interoperability. Web3 describes the set of blockchain-based metaverse services whereas "3" stand for the third iteration of the internet (Dolata and Schwabe 2023).

Besides higher maturity and diffusion of the crucial metaverse technologies, also the premises of use have changed. Physical and digital identities are becoming increasingly blurred. Young people, in particular, distinguish less between their physical and digital selves and more people regard technologies for virtual interaction as an alternative to real-world interaction (Bitkom 2022). The covid pandemic has acted as an accelerator. Additionally, digital ownership is perceived differently as blockchain tokens offer new forms of ownership and create interoperability between virtual worlds (Dolata and Schwabe 2023). Already today, users spend billions on virtual assets (Bitkom 2022). These developments demonstrate that the context of the current metaverse is different from previous understandings and applications.

Privacy in the metaverse

The metaverse combines state-of-the-art technologies that enable an immersive experience in the virtual environment as well as interconnectivity between virtual worlds and the physical world (Peukert et al. 2022). To enable full functionality and an outstanding user experience, related technologies require an extensive amount of data. For example, VR devices collect sensor data from visual input devices such as head-mounted displays (HMD) and haptic input devices such as hand controllers (Mystakidis 2022). Therefore, the metaverse represents a new situation for data collection and processing which potentially poses new threats in terms of privacy. While the topic of metaverse gains more attention in research, the papers to date mainly deal with the concept from a holistic angle, reviewing extant works on the metaverse and related research topics. Further, most of the studies investigate the metaverse conceptually rather than empirically (Dincelli and Yayla 2022). In addition, few metaverse studies have a single focus on privacy (Wang et al. 2022). Furthermore, although a range of studies thematize the topic, many of these papers are published in non-peer-reviewed outlets. Finally, existing papers mainly focus on immersive XR technologies rather than web3 technologies when investigating the topic of privacy (Dincelli and Yayla 2022). In summary, these findings demonstrate the novelty of the metaverse as a research field. In the following, I present previous works on privacy in the metaverse.

Extant studies on privacy in the metaverse present three overarching themes, which are (1) invasive data collection, aggregation, and inferences, (2) access management, and (3) privacy threats in social interaction within virtual worlds. The first theme relates to the intensive data collection of input devices that provide access to the metaverse. This mainly refers to XR devices that collect a range of multisensory data, such as facial expressions, eye and hand movements, surroundings, or geolocation (Bao et al. 2022). Based on these data, providers are able to infer sensitive user information, such as personalities or health statuses (Dwivedi et al. 2022). Even few digital traces are sufficient to derive sensitive inferences (Di Pietro and Cresci 2021). In their study, Nair et al. (2023) demonstrate that by training a classification model on five minutes of data per person with a sample of 50,000+ VR users, a user can be uniquely identified with more than 94 percent accuracy resulting from 100 seconds of motion. In an earlier study, Nair et al. (2022) show that by spending a few minutes in a VR escape room, 25 data attributes from anthropometrics, like height and wingspan, as well as demographics like age and gender, are collected. Combined and triangulated with other data sources, these new types of multisensory data can be used for various monetization options (Nair et al.

2022). Besides commercialization opportunities, these sensitive inferences can also become a victim of misuse or unauthorized access (Bao et al. 2022).

The second theme of existing papers on privacy in the metaverse deals with the access management of metaverse applications. In addition to sensory data, users are often requested to disclose sensitive data to participate in virtual worlds. During the registration process, users are forced to disclose a range of personal information such as name, gender, birth, or financial information (Wang et al. 2022). Besides losing anonymity, the provision of these data also offers a powerful source for data accumulation (Leenes 2008).

The third theme deals with privacy threats of social interaction within the virtual environment. As common metaverse worlds are publicly available, other users as well as providers can observe an avatar's behavior and track its digital footprints. The spatiality paves the way for devious actions such as spying or the hidden observation of communication between avatars (Lee et al. 2021). Also, platform providers have an interest in tracking users' behaviors, communications, activities, and habits in the virtual world. They can use the observed digital footprints to create rich user profiles (Zhao et al. 2021). Besides hidden observations, users are also potential victims of revealed social attacks, such as stalking, abuse, and sexual harassment. As users act through their digital representatives in a 3D world, social attacks are similar to real-world assaults. Moreover, attackers can make use of digital deception instruments such as social engineering or deep fakes (Falchuk et al. 2018). Social engineering exploits human characteristics such as helpfulness, trust, and fear to manipulate people (Salahdine and Kaabouch 2019). Deep fakes describe falsified media content based on artificial intelligence (AI), that aim at manipulating digital identities (Mirsky and Lee 2021). Although the presented privacy issues pose more severe forms of privacy intrusion, regulation has not yet reacted. Scholars emphasize governments' role in enforcing adequate privacy protection (Dincelli and Yayla 2022; Dwivedi et al. 2022). The three themes show that the framework conditions for privacy have changed in the metaverse which is evidenced by an extensive call for research (Park and Kim 2022; Peukert et al. 2022).

Methodology

Recent literature suggests that privacy is an issue that requires additional consideration in future studies (Dincelli and Yayla 2022). Due to the novelty of the current metaverse and its incorporated technologies, an exploratory qualitative approach is chosen to identify the privacy challenges emerging in the metaverse (Corbin and Strauss 2008). Qualitative inductive approaches are particularly suitable in new technological contexts of data sharing. For example, Cichy et al. (2021) examined the determinants that influence connected car users' sharing decisions. In accordance with their approach, the goal of the present study is to assess the manifestations of privacy challenges in the new context metaverse. Furthermore, the study aims at identifying how these challenges can be mitigated. Because users are often unaware of data disclosure and unable to assess its consequences, interviews were conducted with metaverse experts. Besides of being unaware about the privacy consequences, users are also exposed to an information asymmetry towards metaverse providers and do not have full information about the data collection and processing. The increasing complexity of information technology (IT) adds to this uncertainty about data disclosure (Acquisti 2015). Therefore, I interviewed experts who deal with the metaverse in their professional lives on a daily basis because they tend to have a better understanding of data collection and processing in the metaverse (Bennett 1997).

Data collection

For the identification and selection of experts, I used purposeful sampling. The advantage of this sampling strategy is the selection of information-rich cases for an in-depth study (Patton 1990). Purposeful sampling involves selecting the most productive sample, meaning the one that is best suited to answer the research questions (Marshall 1996). To assess suitability, a framework with the relevant variables of interest is sought. Furthermore, researchers incorporate previous knowledge from literature or evidence from the study itself. In the present study, subjects with specific expertise (i.e., key informant sample) on the metaverse were selected (Marshall 1996). As XR and web3 are the predominant technologies of the metaverse (Peukert et al. 2022), participants from both areas of expertise were selected. I also included experts in the sample who deal with the metaverse from a holistic business perspective, for example, by advising companies on their metaverse strategies. The interview partners (IPs) have between one and 16 years of metaverse experience. The years of experience relate to the expertise with related metaverse concepts or technologies. Therefore, some IPs have longer experience because they have expertise in

predecessor elements of the metaverse (e.g., immersive media) or technologies that are incorporated in the metaverse (e.g., VR). Other IPs have just begun work on the metaverse with the new wave of publications in 2021. This explains the broad range of experience. In addition to the metaverse expertise, it was ensured that the IPs have a professional background in IT or deal with digital technologies in their works. Thereby, I ensured that the IPs are suitable to assess privacy challenges. Because the metaverse is based on technological pillars, most of the experts had a natural connection to IT and were therefore able to make informed statements about the collection and processing of data, and ultimately arrive at an assessment of the privacy challenges and measures. Since the IPs have different backgrounds in terms of professional expertise or industry, I made sure that a heterogeneity in terms of subject areas was covered. The IPs originate from Europe, U.S., or China, which ensures a broad geographical coverage. All IPs have an academic background. The first batch of participants was contacted via common social network platforms. It was checked from profile screening that the potential participants have expertise in one of the metaverse building block technologies or deal with metaverse topics holistically. The second batch of IPs was collected through snowball sampling (Marshall 1996). Table 1 gives further details on the position, metaverse expertise, and professional expertise of the IPs.

Data collection took place between July 2022 and February 2023. The interviews were conducted face-to-face via video chat or in person, following a semi-structured interview guide (Myers and Newman 2007). This structure allows taking advantage of qualitative data that is characterized by being open-ended, concrete, vivid, rich, and nuanced (Graebner et al. 2012). The IPs had the opportunity to express their opinions, motivations, and individual understandings. The interviews were conducted in German and English and lasted on average 43 minutes. The German quotations were translated directly into English. The total interview material includes more than 25 hours of audio.

ID	Position	Metaverse Expertise	Years of Metaverse Experience	Professional Expertise
IP1	Project manager	AR	2	Electrical engineering
IP2	Owner (spatial audio services)	XR	6	VR technology
IP3	Author/journalist	Business model	1	Futurology, sociology
IP4	Owner (metaverse agency)	Business model	8	Media technology
IP5	Chief operating officer	Business model	2	Strategy, operations
IP6	University professor	VR	12	Media technology
IP7	Senior innovation manager	VR	2	Media technology
IP8	Co-founder (NFT platform)	Web3	2	Finance, IT
IP9	Senior knowledge analyst	Web3	2	Media, sales
IP10	Freelancer, events manager	VR	6	Media, content creation
IP11	Self-employed VR consultant	VR	11	Healthcare, pharmaceutics
IP12	Founder (VR platform)	VR	9	VR, AR technology
IP13	University professor	XR	10	Chemistry
IP14	Manager	Web3	3	Strategy
IP15	Manager	Web3	1	Marketing
IP16	IT and innovation manager	Business model	1	Innovation
IP17	Founder (XR training services)	XR	2	Marketing strategy
IP18	Senior consultant	Web3	2	Marketing, strategy
IP19	Co-founder (XR consulting)	XR	2	Business development
IP20	Owner (XR UX design)	XR	16	UX design
IP21	Chief executive officer	Web3	10	Strategy
IP22	Privacy program manager	Business model	3	Strategy
IP23	Senior product designer	XR	3	UX design
IP24	Senior software engineer	VR, web3	8	Project management
IP25	XR systems administrator	XR	9	IT developer, innovation
IP26	Chief creative officer	XR	7	Project management
IP27	Metaverse designer	XR	2	Graphics design
IP28	Senior AI engineer	Web3	1	Computer science
IP29	Co-founder (DAO services)	Web3	4	Strategy, innovation

IP30	Founder (privacy services)	Web3	3	IT, biomedical engineering
IP31	Principal group manager	Web3	14	Computer science
IP32	Metaverse R&D specialist	XR	1	Project management
IP33	Co-founder (metaverse services)	Business model	2	Brand strategy
IP34	Venture associate	Business model	1	Industrial engineering
IP35	Senior researcher	Web3	5	Electronic engineering
UX = User experience, DAO = Decentralized autonomous organization, R&D = Research and development				

Table 1. Expert Details: Position, Metaverse Expertise, and Professional Expertise

The interview guideline included the following elements: (1) professional background and experience with the metaverse and related technologies, (2) assessment of emerging privacy challenges in the metaverse in the respective field of expertise, and (3) privacy measures and mitigation strategies for the identified challenges. Beforehand each interview, it was ensured that interviewer and interviewee follow the same definition of the metaverse. Exemplary questions from the main part of the interview are: "*what new privacy challenges, related to your field of expertise, arise from the emergence of the metaverse?*" or "*What are potential privacy protection measures in the metaverse suitable for the identified risks?*". The interview guide was marginally adjusted during the interview process to include prior experience. After each interview, the material was iteratively reviewed by two researchers who are experts in the privacy field and do research on the metaverse for more than one year. Interviews were conducted until saturation became apparent (Gioia et al. 2013).

Data analysis

Qualitative data analysis is characterized by the hermeneutic evaluation of non-numerical data. The approach is strongly inductive in that the material is separated into individual units of analysis which are analyzed by using different coding mechanisms. Implications for answering the research questions can thus be derived from the data itself (Bhattacherjee 2012). Similar to extant studies in privacy research, also this study uses an inductive approach for interpreting the interview material (Cichy et al. 2021). I followed the approach by Saldaña (2013) and analyzed the material in two coding cycles. After highlighting descriptive information about the participants, open coding was applied. Herein, the qualitative material is divided into discrete parts which allows comparing text passages for similarities and differences. In-vivo codes and provisional category names were used to "crystallize and condense meanings" (Charmaz 2006, p. 57). The result of the open coding procedure is a long list of privacy challenges and measures of the metaverse expressed in the experts' narratives. In the second cycle, the initial codes were iteratively refined, merged, and extended into conceptual categories. This step is characterized by moving back and forth between data, codes, and relevant literature and is accompanied by discussions between the two researchers involved (Charmaz 2006). I applied pattern coding, which groups the material into explanatory and inferential codes that helps derive assertions. Pattern coding helps "pull together a lot of material into a more meaningful and parsimonious unit of analysis" (Saldaña 2013, p. 210). The results show the final categories and themes on metaverse privacy challenges and protection measures. The categories were then deductively clustered into the MDT dimensions as an analytical frame. Since the metaverse represents a new context for privacy, it is useful to combine exploratory qualitative data with an established analytical framework (Hong et al. 2019). To ensure a rigorous approach and consensus in the interpretation of the material, the results were discussed among two researchers. As part of this triangulation, iteration was performed until a satisfactory agreement between coders was found.

Results

The identified privacy challenges and related privacy protection measures in the metaverse are classified into three dimensions in accordance with the MDT as an overarching framework (see Figure 1).

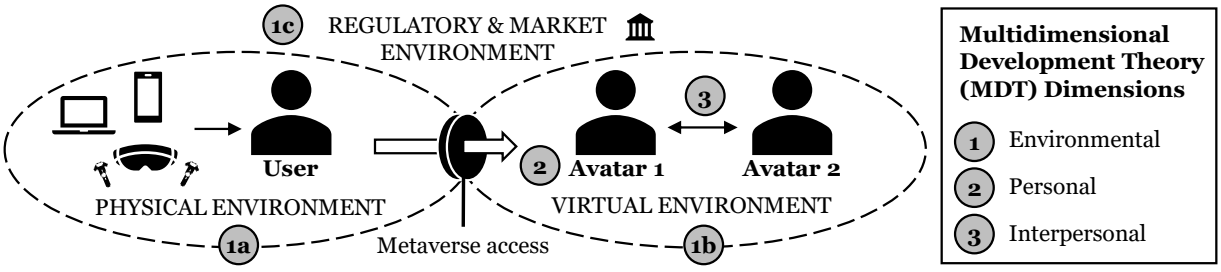

Figure 1. Three-dimensional Privacy Framework in the Metaverse

The environmental dimension includes three sub-dimensions in the context of the metaverse: **(1a)** physical environment, **(1b)** virtual environment, and **(1c)** regulatory and market environment. The physical environment includes all physical objects that provide access or are connected to the metaverse whereas the virtual environment refers to metaverse worlds that are accessible via avatars. The regulatory and market environment includes institutions and market players that set standards and define the rules of the metaverse. The personal dimension **(2)** refers to the avatar as human representation in the virtual world (Dionisio et al. 2013). The interpersonal dimension **(3)** contains all forms of communications and interactions between avatars. The metaverse privacy challenges and associated measures for privacy protection are summarized in Table 2 and described in the following.

MDT Dimension	MDT Sub-dimension	Metaverse Privacy Challenges	Measures for Privacy Protection
Environmental (1a)	*Physical environment*	• Collection of new forms of data (e.g., *multisensory data*), inferences, data aggregation	• Technical features for privacy protection (e.g., *end-to-end encryption*)
Environmental (1b)	*Virtual environment*	• Mandatory account requirements	• Access and identity management (e.g., *blockchain wallets*)
		• Transparency of blockchain	• *No measures*
Environmental (1c)	*Regulatory and market environment*	• Platforms' data monetization interests	• Transparency and control options • Incentives for data disclosure
		• Platforms as gatekeepers	• Blockchain-based infrastructure
		• Insufficient data privacy regulation	• Revision of regulations and standards
		• Know-your-customer processes	• Code as law
Personal (2)	-	• Clear names obligation	• Prohibition of clear names
		• Realistic avatar design	• Restricted avatar design options
Interpersonal (3)	-	• Observation of digital footprints	• *No measures*
		• Proof-of-attendance protocols	• *No measures*
		• Spam in wallets	• *No measures*
		• Social attacks (e.g., *harassment*)	• Sanctions (e.g., *blocking*) • Safety bubbles, private rooms • Disguise of avatars • Moderation, governance
		• Psychological consequences	
		• Social engineering	
		• Deep fakes	

Table 2. Metaverse Privacy Challenges and Measures for Privacy protection

Environmental

Physical environment

Although the metaverse is accessible via different devices, XR technologies are considered a crucial element and relevant access point (Peukert et al. 2022). To enable full functionality, XR devices require massive **collection of new forms of data** (IP22). The IPs frequently mentioned the privacy risks emerging from the collection of diverse multisensory data. Biometric data such as eye or face tracking, and haptics enable metaverse providers to make sensitive **inferences** about users: "*You find out things about yourself via eye tracking that you don't even know. You can analyze: Is a person an alcoholic? Does one have a mental*

health condition? Is it stressed?" (IP10). Moreover, XR devices are packed with cameras that scan users' room environments: "*One issue that I see as critical is the fact that you have a living camera on your head.*" (IP5). These kinds of data traces lead to user identification with a higher accuracy: "*The data that an Oculus [Quest 2] collects in five minutes can easily track you with 95.3% accuracy.*" (IP23). By means of **data aggregation** and triangulation, metaverse providers become owners of valuable data treasures: "*If paired with web2 data, for example from social media, […] you have a pretty powerful source.*" (IP15).

The IPs mentioned a range of **technical features for privacy protection**, including edge computing (IP1), virtual private networks (VPN) (IP10), end-to-end encryption (E2EE) (IP16), and access management through biometric data (IP12). Edge computing describes decentralized data processing which allows data to be processed on the device without sending it to external servers (McKinsey 2022b). VPN is a technique that ensures a secure network connection by opening a tunnel between the device and the Internet (XRSI 2020). E2EE describes the encryption of transmitted data, whereby only the communication partners can encrypt and decrypt the message (IBM 2022).

Virtual environment

Within the virtual environment, users are often forced to provide a range of personal data to access metaverse worlds (IP2). Many platforms require the creation of a user profile and set **mandatory account requirements**. Especially Meta was criticized for their requirement of having a Facebook account to use their VR devices*: "Currently, you must connect to a Facebook account to be able to use the glasses. That gives you a bad feeling because you know exactly what's happening to your data."* (IP2). Algorithms can use these data streams to create user profiles, making users more transparent: "*You can find out quite a lot about a person by using algorithms. And in the end, you're pretty much a transparent person.*" (IP13).

An integral part of many metaverse worlds is the blockchain, which allows transactions between users (Xu et al. 2022). One issue that was mentioned with regards to blockchain-based applications is **transparency of the blockchain** (IP14). In order to make transactions, users require a "wallet", which is used to store and exchange cryptocurrencies and crypto assets (Citigroup 2022). Due to the decentralized nature of the blockchain, transactions can be viewed publicly. If a wallet is mapped to a personal identity, all the person's transactions are also public: "*Nowadays, all wallets are public to a large extent, including whom they belong to […] So you would probably be able to identify all my wallets in 10 minutes just clicking through the publicly available information.*" (IP8). Further, data on the blockchain is stored immutably: "*The right to be forgotten […] there will be no such thing on blockchain.*" (IP18).

The IPs have not mentioned any measures that resolve the issue of the blockchains' transparency. Although some measures exist to protect the privacy of blockchain transactions, such as "ring signatures" or "mixing" (Berghoff et al. 2019), these are largely unsuitable for NFT transactions (Chen and Omote 2022). However, one measure mentioned was zero-knowledge (zk) proofs, which is a form of verification based on the blockchain (IP16). The verifier can check for the information of interest without revealing other sensitive information (Nofer et al. 2017). Although zk proofs are already being applied in areas such as digital payments, online authentication and access control, they do not provide a general solution for the transparency of blockchains (Berghoff et al. 2019).

While the blockchain was criticized for increasing users' transparency, wallets were also named as a solution to manage data disclosure. The advantage is that a wallet is interoperable, which means that it is not dependent on a specific application or party as it runs on the blockchain. Wallet owners can manage and control personal data by means of a wallet: *"[The wallet] keeps your address, driver's license, and other data. But <u>you</u> decide which data to disclose.*" (IP8). This decentralized **access and identity management** would be an alternative for centralized platform accounts (IP21).

Regulatory and market environment

The regulatory and market environment plays a crucial role in setting the standards of the metaverse usage. Many participants called **platforms' data monetization interests** a remarkable threat: "*Meta has a vested interest in finding out all the data about me and tracking my condition to the last wink.*" (IP1). The business model of these platforms, whose services are often offered free of charge, is based on data monetization: "*Facebook always had the customer as the product because there is no such thing as a free social VR or whatever experience.*" (IP10). Therefore, these companies have no intention to protect privacy

that goes beyond minimum standards: "*Meta, Google, and Co's. […] business model is based on collecting as much data as possible and turning them into money.*" (IP16). This can also be seen in low investments in privacy: "*So they are investing billions in Metaverse and have targeted 50 million [Us dollars] for privacy. That is shocking, because the issue is still not given any priority.*" (IP16). Due to the high market shares of technology companies and the tendency toward market consolidation, they are in the position to set their own rules and act as **platform gatekeepers**: "*There are large areas of the digital world that are in the hands of a few corporations, which then actually set the rules.*" (IP3).

IP6 remarks the **insufficient data privacy regulation** of the metaverse as a major privacy threat. However, the IPs emphasized the difficulty of regulating the metaverse as it is spread across different geographical and regulatory areas. Therefore, a threat exists that rules in the metaverse are not made by users but enforced by market players: "*Then we have a space that is completely controlled by the corporations. […] The rules in the virtual space will no longer be made democratically by political parties, but by economic interests.*" (IP6). Also, regulation for web3 technologies is criticized and described as "wild west" (IP4, IP8, IP18): "*This decentralized idea […] has led to the fact that it is a wild west. Because there is still little focus on privacy.*" (IP8). The IPs often mentioned the General Data Protection Regulation (GDPR) when it came to privacy protection from a regulatory standpoint. GDPR is an EU regulation that unifies the rules regarding the processing of personal data across the EU. The IPs argue that the GDPR needs to be revised for the metaverse: "*GDPR is woefully out of date. Because the technology industry always moves faster than the regulators.*" (IP21).

With regards to blockchain-based applications, the IPs called **know-your-customer** (KYC) **processes** a privacy issue. KYC describes a legitimation check for new customers to prevent money laundering, which is mandatory for credit institutions and insurance companies (Citigroup 2022). Beyond ensuring safety, users are also forced to provide personal data, such as their passports: "*[The KYC process] is pretty tough. It's also the case that people have to photograph their passports.*" (IP15). Besides KYC processes, IP35 criticizes the data hunger of governmental agencies, that set regulations in a way that forces users to provide personal information: "*There are many constraints with regulators that make things hard to regulate. They don't want this to happen. They want all your behaviors, transactions, and your daily activities being handled in their way so that they have control. They can tax you. […] And they can find you.*" (IP35).

In conclusion, the IPs suggested that privacy threats are currently not adequately addressed: "*We need to take a closer look at privacy risks, because today we're running towards them at 100 km/h and no one cares about this issue.*" (IP16). As privacy protection measures, the IPs suggested different directions. Although criticized for the transparency of wallets, IP8 regards **blockchain-based infrastructures** as an alternative to a centralized concept. By using blockchain as an "underlying layer", users would be independent of metaverse providers: "*Blockchain technology […] would offer an economy, in which users are not dependent on a large corporation - on a large data octopus.*" (IP8).

The IPs further claimed that metaverse platforms should provide more **transparency** (IP1) **and control options**, such as cookie management (IP9). The IPs stated that the platforms should be transparent about their business models and offer **incentives for data disclosure**: "*It would be a measure for the platforms to say: You get a privacy-protected, anonymized basic service for free. But if you want […] premium features, you can pay either with money or with your user data. Or they offer a premium version saying: Here is the catalog of user data you can choose, to disclose. And for each body tracking you get one meta coin a month.*" (IP10). In this suggestion, users would pay for a higher level of privacy or earn money by providing their data, which comes with a lower level of privacy.

The second direction to enforce privacy protection is through governments and regulatory institutions. According to the IPs, the regulatory body has the responsibility to enforce the **revision of regulations and standards** to include the novelties of the metaverse: "*It is necessary to establish some criteria at the international level for a basic data protection regulation that specifies the standards to which the companies that build [the metaverse] must adhere.*" (IP3). This could be obtained, for example, by more investments in privacy (IP12). However, the IPs acknowledged that it is a challenging task to set rules for the metaverse, which spans across the world: "*Globally it's a challenge anyway because of the different jurisdictions, as it's still very fragmented.*" (IP4). IP35 proposed the concept of "**code as law**" as a substitute to data intensive identity verification processes such as KYC. The concept connects a program code running on the blockchain to existing law and thus replaces governmental controls: "*You need to build*

your identity from scratch with the law embedded in it, which we call "code as law". […] Anything that breaks the law can be easily justified and stopped because the law is in the code." (IP35).

Personal

The personal dimension refers to the user's identity in the virtual environment. The creation of avatars enables users to express their identities in a digital format (Dionisio et al. 2013). Thus, privacy threats emerge by disclosing real-world identities. An example are **clear name obligations**, that are currently enforced by different platforms such as Facebook. According to IP10, privacy is only protected when clear names are prohibited: "*As long as I don't have to give my real name, privacy is considered quite well.*" (IP10). Also, IP4 mentions that clear names should be disabled or replaced by nicknames. Especially for the protection of children, the avoidance of clear names is relevant: "*I tell my kids that they can do anything on the Internet, have fun with Roblox avatars and Animal Crossing, but never ever tell your real name*." (IP10). However, while being a determinant of privacy concerns, clear names are also an instrument to ensure safety and prevent crime (IP4). Another privacy risk is **avatar design**. Users tend to design their avatars according to their real looks: "*If you consider avatar creation, people tend to create an image of themselves that is as identical as possible […] which provides even more data*." (IP16). In combination with clear names, platforms and users can make accurate inferences about users' identities. Both presented avatar features force platforms to make trade-offs between two overarching goals of virtual worlds. Either they enforce privacy-intrusive identity disclosure, or they allow anonymity for the sake of privacy, which could lead to less credibility and trust among users: "*On the one hand, there is protection of privacy and anonymity. On the other hand, there is less authenticity, less credibility, and also less trust among users, due to the anonymity. So, it's a trade-off.*" (IP16). IP16 and IP12 describe it as a challenge for companies to find a balance of this trade-off: "*What outfits do we offer? Should we nudge users to want to look like they do in real life? Or do we design it so that anyone can be any person? Those are the relevant questions*." (IP12). IP12 further mentions that the variety of options has an impact on users' privacy decisions: "*The design decisions that we have in our app, can define whether you want to look more like yourself or be a panda bear in a meeting*."

Interpersonal

The third dimension refers to the interpersonal interaction between avatars within the virtual world. Due to the spatiality and accessibility of the virtual environment, the **observation of digital footprints**, communications, and behaviors is possible (IP14). Privacy risks emerge by the possibility of spying activities: "*There's many new ways we can spy on you.*" (IP24). One user can follow another and take record of its digital footprints or listen to private conversations (IP14). Further, other users can make recordings without being recognized which can't be technically prevented (IP1). Blockchain-based **proof-of-attendance protocols** (POAP) offer a way to keep track of users' digital footprints. POAP prove the attendance of a virtual or physical event in the form of an NFT. A user's privacy is threatened when an unauthorized person can map the wallet, in which the POAP is stored, with the users' identity. The attacker would have access to the user's digital and real-world footprints that are documented through the POAP (IP15). Further, as wallets have no technical possibility of filtering, malicious attackers can send **spam to wallets**: "*A huge privacy problem there is spam. Technically, I can't prevent anyone from sending me anything to my wallet*." (IP8).

Another privacy risk in interaction with other avatars is **social attacks**, such as bullying, stalking, or sexual harassment: "*Bullying is an issue on different platforms. The other thing that is a problem is the haptics in terms of sexual harassment. That is something new in the metaverse*." (IP13). IP5 calls the protection of minors in the metaverse a major issue: "*A huge problem in [VRChat] is that minors constantly meet pedophiles in terms of social interaction*." (IP5). Even without malicious intentions, users can overstep avatars' personal spaces and intrude on their privacy: "*In social communication in VR, it's the case that when people invade this space, it is quickly perceived as a border crossing and thus entry into private space and privacy*." (IP4). According to IP12 and IP19, the feeling of anonymity in the virtual environment also leads to a higher willingness to harass and more severe forms of harassment: "*As a harasser, you somehow think you have less consequences. This abstraction to the digital world sometimes tempts you to bring out even more extreme or severe harassment*." (IP12). Furthermore, the degree of immersion leads to the fact that privacy attacks feel more realistic which leads to more severe **psychological**

consequences: "*This whole bullying issue that you've always had in Twitter as well, but it's much more critical here because of avatars' interaction. […] someone is coming physically close to you, or even rape insinuations that the avatars have among each other.*" (IP6). This perception is triggered by higher immersion and spatial presence, enabled by VR: "*For the person receiving [harassment], it's extremely realistic and authentic. It's also much worse to get a sexist comment in VR than reading it in 2D.*" (IP12). IP12 further mentions that negative emotions are perceived *"a hundred times more intense in VR compared to 2D.*" Malicious users can leverage this immersion to influence users by means of **social engineering**: "*People feel frightened by avatars, feel influenced by the behavior, how close other people get to them.*" (IP6). In addition, when malicious users pretend to be someone else's avatar, they can damage the person's reputation or conduct identity theft. Leveraged by AI, **deep fakes** are also possible (IP18).

To prevent social attacks in the metaverse, the IPs suggest different **sanction** mechanisms which mainly refer to technical features within the virtual environment. One option is blocking of users, meaning that they cannot interact with or are invisible to the harassed avatar (IP6). Another measure is the blurring of attackers' voices (IP4). A feature that in some applications is already implemented is **safety bubbles** that limit an avatar's radius: "*Meta has introduced certain functions, such as a social bubble, which automatically hides people when someone gets too close.*" (IP4). Another suggestion includes **private rooms** or "safety spaces" (IP4), that ensure that communication cannot be observed by other users: "*To avoid that one can hear sensitive conversations, you can pull yourself in self-zones. These can be physically recreated rooms, but also simply like a soap bubble, invisible around you.*" (IP4). Instead of blending out attackers, the harassed user can also **disguise** its avatar's look (IP6). According to IP6, these measures are technically feasible and could be easily implemented.

The IPs also mentioned organizational privacy features as countermeasures for social attacks such as the **moderation** of virtual worlds (IP2) and forms of **governance**, such as codes of conduct (IP4). Both measures relate to the regulation and sanctioning of behavior within virtual communities: "*It's about code of conduct or netiquette or social regulations that are also supported by the community.*" (IP4). Moderators can punish violations of the virtual world's rules. However, it was also mentioned that moderation does not come without privacy risks. In many virtual worlds, moderators can remain invisible and observe other people's behavior without being detected (IP4).

The IPs did not identify any measures for observing avatar footprints. While previous work has suggested a number of privacy features, such as avatar cloning or invisibility (Falchuk et al. 2018), these features are not yet implemented in current metaverse worlds (Lee et al. 2021). The IPs also did not mention measures for blockchain-related privacy challenges, namely POAP and spam. According to IP8, spam in wallets cannot be technically prevented. However, some vendors have started to offer first solutions (Alchemy 2023). For POAP, no measures were mentioned either, which is due to the fact that POAP inherently contains information about digital footprints (Binance 2023).

Discussion

The results present 16 privacy challenges and corresponding privacy protection measures of the metaverse that act as mitigation strategies for policymakers and organizations (see Table 2). While previous studies are mainly conceptual in nature (Dwivedi et al. 2022), this study complements existing works with comprehensive empirical results. Further, the focus of previous articles on investigating privacy in the metaverse had been mainly on XR as a constituent technology of the metaverse, neglecting the challenges posed by web3 technologies (Dincelli and Yayla 2022). Although the concepts of metaverse and virtual worlds have been an established part of the IS literature for several years (Boughzala et al. 2012), it appears that technological improvements as well as the renaming of the company Meta in 2021 have unleashed a new wave of publications. Therefore, it seems necessary to reassess the opportunities and risks of today's understanding of the metaverse. This paper intends to make a first contribution to the examination of the challenges and potential solutions to privacy conditions. In the following, the results are discussed and put into a broader context. For this, the framework by Acquisti (2015) is applied, which is established to evaluate new contexts of data sharing and the associated changes in privacy conditions (see Figure 2).

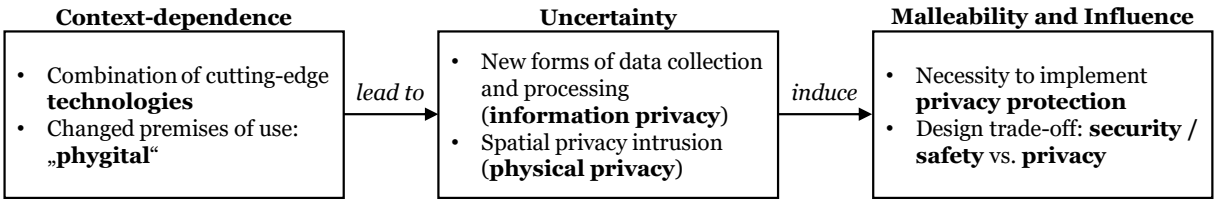

Figure 2. Changing Contextual Factors in the Metaverse Lead to Privacy Challenges, Inducing the Necessity to Implement Privacy Protection Measures

Context-dependence

Numerous studies demonstrate that new contexts of data sharing lead to different privacy decisions and behaviors (Acquisti 2015). In the information age, technologies become more data intensive and require more extensive data collection and processing. Therefore, technological advancements constantly trigger new privacy studies in the IS discipline (Cichy et al. 2021). The metaverse represents a new context that is driven by two changes of contextual factors. First, improvements of metaverse technologies are a major driver for the generation of new privacy challenges (Kallemeyn and Chipidza 2021). The metaverse combines various contemporary **technologies** whereas XR and web3 are considered as fundamental elements (Peukert et al. 2022). XR technologies play a crucial role in enabling immersion and improving user experiences (Zhao et al. 2021). With increasing maturity, XR is experiencing mass adoption (Dincelli and Yayla 2022). Corresponding hardware becomes lighter, cheaper, and more comfortable and shows enormous technological improvements for view, display of images, and software. However, to enable full functionality they need to collect new forms of data such as haptics and surroundings (Dincelli and Yayla 2022). The results of this study show that the scope of data collection in the metaverse differs from previous applications. Metaverse providers can collect completely new forms of multisensory data, which can be used to generate targeted insights about users. Moreover, as the metaverse becomes more prevalent, hardware vendors like Meta are taking on a gatekeeper role. Another fundamental metaverse technology is web3. In contrast to standalone XR applications, the metaverse pursues the idea of interconnected virtual worlds that span a parallel reality to the physical world (Peukert et al. 2022). The interconnection and the representation of assets in the virtual world is enabled by web3 technologies (Dolata and Schwabe 2023). The second driver for changing context is new premises of use which is characterized by an increasing fusion of digital and physical worlds (Wang et al. 2022). Studies demonstrate that people distinguish less between their digital and physical identities. Further, the idea of ownership changes which is shown by the increasing popularity of NFTs (Bitkom 2022). The blurring of virtual and physical worlds is called "**phygital**" (Forbes 2022). As physical properties continue to migrate to the digital environment, more data trails emerge, creating the potential to invade privacy.

Uncertainty

Individuals make boundaries between private and public spheres in the physical and virtual environment (Acquisti 2015). Privacy in the physical environment relates to the intrusion into people's personal spheres. When a stranger oversteps an individual's boundaries, physical privacy concerns arise (Warren and Brandeis 1890). In contrast, the intrusion of privacy in virtual environments refers to the collection and processing of data and is therefore called "information privacy" (Smith et al. 2011). In their work, Lin and Armstrong (2019) draw on Altman (1975) definition of privacy as access to the self and introduce the concept of "private virtual territory". In doing so, they apply the metaphor of spatial territories to a digital context, linking both understandings of privacy. This also applies to the metaverse, which is characterized by the fusion of physical and virtual worlds (Wang et al. 2022).

In terms of **information privacy**, new forms of data are being collected by metaverse technologies that allow information to be inferred about intimate behaviors and perceptions. Biometrically derived data, such as facial attributes, can be used to make sensitive inferences about preferences, personality traits, or physical health. This data is linked to digital identities and can be observed by the virtual community and platforms (Bao et al. 2022). The results of the study show that users are increasingly being observed in the metaverse. Movements, reactions, and preferences can be observed in real time by other users and collected as records by providers. In addition, the transparency of the blockchain offers the possibility of inference

about users, who now conduct a wide range of transactions via tokens, some of which contain sensitive data. Metaverse companies, who play a crucial role in setting the standards for metaverse access and usage, were criticized for their extensive commercialization interest in the metaverse. Furthermore, the results of this study show that providers have a direct impact on users' privacy by defining the requirements for creating profiles and making profile information available to other users. As a result, existing privacy policies and standards should be revised. Due to the spatiality, three-dimensionality, and accessibility of the metaverse, **physical privacy** must also be considered in the configuration of metaverse services. Thus, invasion of privacy also refers to the crossing of physical privacy boundaries (Falchuk et al. 2018). Avatars can be victims of social attacks, such as stalking, spying, or harassment. Attacks are already happening today. Instead of policing and punishing, platforms like Meta focus on providing controls for users to protect themselves. This differs from Facebook and Instagram, which use bots and humans to filter hate speech (Nix 2023). Due to the immersion, psychological consequences are more severe than in previous applications. The results also show that social engineering and deep faking are increasingly becoming issues in the metaverse. Early works call for investigating "secure zones" in virtual worlds that adapt security and privacy models from web browsers, such as the Secure Sockets Layer (SSL) security protocol (Mennecke et al. 2008). Such protocols would add a privacy measure and ensure secure transactions in the metaverse.

Malleability and influence

With changing contextual factors and the potential for physical and information privacy intrusion, metaverse creators and stakeholders, such as platforms, regulators, and users, must find a balance between diverging interests. On the one hand, companies have a natural interest in collecting and aggregating user data. On the other hand, protecting privacy is important to prevent adverse user reactions such as reduced use intentions (Smith et al., 2011). The results of this study reveal that the development of **privacy protection** depends on a negotiation process between metaverse organizations and users. Since user privacy concerns are a predictor of economic outcomes such as use intentions, organizations must find appropriate mitigation strategies to address the emerging privacy challenges. The results present several privacy protection measures that act as guidelines for metaverse providers and regulatory institutions. Another implication was that the decision to provide a certain level of user anonymity, and thus privacy in the metaverse, forces metaverse designers to make **trade-offs between privacy** and **safety/security** aspects. Due to the accessibility of virtual worlds, the metaverse enables the formation of virtual communities (Mennecke et al. 2008). To ensure safety and security, metaverse platforms and regulators develop codes of conduct and rules to control users' behavior. For example, many platforms are forced to conduct authentication processes such as KYC to prevent crime. These processes force the disclosure of identity information, which presents an intrusion into users' privacy. However, verification processes can also increase safety. When users can be linked to their real-world identities, metaverse guards can penalize inappropriate behavior. Therefore, metaverse designers are confronted with the decision of giving away users' privacy to enable a safe virtual world and create trust and credibility amongst users.

Conclusion, limitations, and future research

The metaverse is a timely topic that currently graces headlines of scientific and practitioner literature which is evident from a sharp increase in publications (Polyviou and Pappas 2022). The metaverse describes a massively scaled multi-user three-dimensional computer-generated virtual world that humans can access as avatars. While the concept has been researched in the IS discipline for a while (Boughzala et al. 2012), a new wave of studies has emerged, fueled by increasing technological advancements, such as the readiness and diffusion of state-of-the-art immersive XR technologies and the increasing popularity of web3 applications (Peukert et al. 2022). While these technologies offer unprecedented options for experience and interaction, related devices and applications require huge amounts of data to provide full functionality and advanced user experiences (Wang et al. 2022). This data intensity potentially leads to privacy concerns and therefore lower use intention and decreased willingness to provide data (Smith et al. 2011). Thus, it is crucial for metaverse companies to anticipate potential pitfalls and respond with sufficient mitigation strategies.

This paper responds to the numerous calls for research to investigate privacy as an important pillar of the metaverse (Dincelli and Yayla 2022). In doing so, I conducted 35 qualitative empirical interviews with metaverse experts to explore privacy challenges and recommend corresponding privacy measures for the metaverse. In my research approach, I was guided by the MDT that explains how an individual's privacy

concerns develop in a specific context. The theory states that privacy concerns emerge by means of three dimensions: environmental factors, personal experiences, and interpersonal exchange (Laufer and Wolfe 1977). Based on the expert interviews, I identified 16 privacy challenges and proposed associated privacy protection measures. The results indicate that due to changing contextual factors, new forms of intrusion in information and physical privacy spaces emerged. This leads to the necessity for companies and policymakers to implement appropriate privacy protection measures for the novel context metaverse.

The results of this paper hold implications for research and practice. From a research perspective, the paper contributes to the IS literature by enriching existing metaverse studies with comprehensive empirical results on the focus topic of privacy. The interviewed metaverse experts cover a broad spectrum of professional knowledge and come from different geographical regions. Further, the paper provides an extensive documentation on extant works and thus offers scholars a point of reference for future studies. From a practical point of view, the results offer implications on privacy challenges that metaverse providers need to consider when implementing metaverse services. Further, the paper provides tangible recommendations for action to prevent adverse user reactions. Finally, the results also offer implications for regulatory institutions who protect user privacy by setting standards and laws.

Despite the contribution of this study, there are some limitations and starting points for future research. First, there is no uniform definition of the metaverse. Rather, it is an ever-changing concept that encompasses a wide range of ideas and technologies (Peukert et al. 2022). This study refers to the current understanding of the metaverse that incorporates XR and web3 as building blocks. For the interviews, I ensured the IPs follow the same definition of the metaverse and have expertise in one of those fields. However, different technologies may also play a role in the metaverse which points to the inclusion of a wider range of professions and technological expertise. Although it was ensured that the IPs have a basic understanding of IT, they may work on metaverse topics from other perspectives than privacy. The results could therefore be enriched by the assessment of pure privacy experts. It is also important that the challenges for which no actions were identified in this study are further investigated. While this study identified the major areas where privacy challenges could arise, future studies should further elaborate on policies and guidelines to resolve the privacy issues and analyze their real-world effectiveness. Lastly, in this study, I conducted interviews with experts as they usually have a better understanding of actual privacy threats. Nevertheless, future studies could also include users into the exploration of privacy. User perceptions and behaviors are relevant to design issues and therefore of interest to platform providers and participating companies. Since physical privacy is an issue of growing importance in the metaverse, it could be investigated to what extent previous privacy constructs are suitable for the measurement of users' privacy concerns. I hope that the results of this paper will motivate further research on privacy in the metaverse.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce*, 21-29.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347* (6221), 509-514.

Alchemy (2023). *How to filter out spam nfts*. https://docs.alchemy.com/docs/how-to-filter-out-spam-nfts.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding* Monterey, CA: Brooks/Cole Publishing.

Ball, M. (2020). *The metaverse: What it is, where to find it, and who will build it*. https://www.matthewball.vc/all/themetaverse.

Ball, M. (2022). *The metaverse will reshape our lives. Let's make sure it's for the better*. https://time.com/6197849/metaverse-future-matthew-ball/.

Bao, X., Shou, M., & Yu, J. J. (2022). Exploring metaverse: Affordances and risks for potential users. *Proceedings of the Forty-Third International Conference on Information Systems (ICIS 2022)*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35* (4), 1017-1041.

Bennett, C. J. (1997). Policy for the protection of personal data? *Technology and privacy: The new landscape*, 99.

Berghoff, C., Gebhardt, U., Lochter, M., & Maßberg, S. (2019) Blockchain sicher gestalten. Bundesamt für Sicherheit in der Informationstechnik, Bonn.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices. *Textbook Collections*, *3*.

Binance (2023). *Proof of attendance protocol (poap).* https://academy.binance.com/en/glossary/proof-of-attendance-protocol-poap.

Bitkom (2022). *A guidebook to the metaverse*. https://www.bitkom.org/sites/main/files/2023-01/230105LFMetaverseEN.pdf.

Boughzala, I., de Vreede, G.-J., & Limayem, M. (2012). Team collaboration in virtual worlds: Introduction to the special issue. *Journal of the Association for Information Systems*, *13*.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis* London, Thousand Oaks, New Delhi: SAGE Publications.

Chen, Z., & Omote, K. (2022). Toward achieving anonymous nft trading. *IEEE Access*, *10*, 130166-130176.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars. *MIS Quarterly*, *45* (4), 1863-1892.

Citigroup (2022). *Metaverse and money - decripting the future.* https://www.citifirst.com.hk/home/upload/citi_research/AZRC7.pdf.

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3 ed.). Los Angeles, CA: SAGE Publications.

Davis, A., Murphy, J., Owens, D., Khazanchi, D., & Zigurs, I. (2009). Avatars, people, and virtual worlds: Foundations for research in metaverses. *Journal of the Association for Information Systems*, *10* (2), 90-117.

Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and privacy issues. *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA).*

Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the metaverse: A hybrid-narrative review based on the technology affordance perspective. *Journal of Strategic Information Systems*, *31* (101717), 1-22.

Dionisio, J. D. N., Burns, W. G., & Gilbert, R. (2013). 3d virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys (CSUR)*, *45* (3), 1-38.

Dolata, M., & Schwabe, G. (2023). What is the metaverse and who seeks to define it? Mapping the site of social construction. *Journal of Information Technology*.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., ..., & 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).

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, *37* (2), 52-61.

Forbes (2022). *A 'phygital' perspective on the 21st century: Welcome to the metaverse.* https://www.forbes.com/sites/forbestechcouncil/2022/04/18/a-phygital-perspective-on-the-21st-century-welcome-to-the-metaverse/?sh=6df5ae2f2254.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational Research Methods*, *16* (1), 15-31.

Graebner, M. E., Martin, J. A., & Roundy, P. T. (2012). Qualitative data: Cooking without a recipe. *Strategic Organization*, *10* (3), 276-284.

Hong, W., Chan, F. K., & Thong, J. Y. (2019). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, *168* (3).

IBM (2022). *What is end-to-end encryption?* https://www.ibm.com/topics/end-to-end-encryption.

Kallemeyn, D., & Chipidza, W. (2021). Towards a forward-looking conceptualization of privacy. *Proceedings of the Forty-Second International Conference on Information Systems (ICIS 2021).*

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33* (3), 22-42.

Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint*, *2302.08927*.

Leenes, R. (2008). Privacy in the metaverse: Regulating a complex social construct in a virtual world. In S. Fischer-Hubner, P. Duquenoy, A. Zuccato and L. Martucci (Eds.), *Ipip international federation for information processing* (pp. 95-112), Boston: Springer.

Lin, S., & Armstrong, D. (2019). Beyond information: The role of territory in privacy management behavior on social networking sites. *Journal of the Association for Information Systems*, *20* (4), 434-475.
Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33* (3), 5-21.
Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, *13* (6), 522-526.
McKinsey (2022a). *Value creation in the metaverse - the real business of the virtual world.*
McKinsey (2022b). *Marketing in the metaverse: An opportunity for innovation and experimentation.* https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/marketing-in-the-metaverse-an-opportunity-for-innovation-and-experimentation.
Mennecke, B., McNeill, D., Ganis, M., Roche, E. M., Bray, D. A., Konsynski, B., Townsend, A. M., & Lester, J. (2008). Second life and other virtual worlds: A roadmap for research. *Communications of the Association for Information Systems*, *18* (28), 371-388.
Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR)*, *54* (1), 1-41.
Myers, M. D., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and Organization*, *17* (1), 2-26.
Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2* (1), 486-497.
Nair, V., Garrido, G. M., & Song, D. (2022). Exploring the unprecedented privacy risks of the metaverse. *arXiv preprint 2302.08927*.
Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J. F., Rosenberg, L., & Song, D. (2023). Unique identification of 50,000+ virtual reality users from head & hand motion data. *arXiv preprint 2302.08927*.
Nix, N. (2023). *Meta doesn't want to police the metaverse. Kids are paying the price.* https://www.washingtonpost.com/technology/2023/03/08/metaverse-horizon-worlds-kids-harassment/.
Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*, 183-187.
Park, S.-M., & Kim, Y.-G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, *10*, 4209-4251.
Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2 ed.). SAGE Publications.
Peukert, C., Weinhardt, C., Hinz, O., & van der Aalst, W. M. P. (2022). Metaverse: How to approach its challenges from a bise perspective. *Business & Information Systems Engineering*, *64* (4), 401-406.
Polyviou, A., & Pappas, I. O. (2022). Chasing metaverses: Reflecting on existing literature to understand the business value of metaverses. *Information Systems Frontiers*, 1-22.
Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11* (4), 89.
Saldaña, J. (2013). The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, 1-440.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35* (4), 989-1015.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.
Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745-772.
Stephenson, N. (1992). *Snow crash* New York: Bantam Book.
Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *arXiv preprint 2203.02662*.
Warren, S. D., & Brandeis, D. L. (1890). The right to privacy. *Harvard Law Review*, *4* (5), 193-220.
Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25* (1).
Witmer, B. G., & Singer, M. J. (1998). Measuring presence in virtual environments: A presence questionnaire. *Presence*, *7* (3), 225-240.
XRSI (2020). *Extend reality with awareness! Xr safety and privacy guide for artists.* https://xrsi.org/wp-content/uploads/2020/12/Artizen-XR-Safety-and-Privacy-Guide-for-Artists-v002.pdf.
Xu, H., Li, Z., Li, Z., Zhang, X., Sun, Y., & Zhang, L. (2022). Metaverse native communication: A blockchain and spectrum prospective. *IEEE International Conference on Communications Workshops (ICC Workshops)*.
Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2021). Metaverse: Security and privacy concerns. *arXiv preprint arXiv:2203.03854*.