Unveiling Stakeholder Perspectives on Privacy in the Metaverse: Case Study of a German Car Company

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

Sophie Riethmüller
LMU Munich School of Management
sophieriethmueller@web.de

Thomas Hess
LMU Munich School of Management
thess@lmu.de

Abstract

Companies have turned their attention to becoming part of the metaverse, a persistent, multi-user, three-dimensional environment characterized by the fusion of virtual and physical elements. While the metaverse offers new ways to create value, related software and hardware components require massive amounts of user data, which can raise privacy concerns. In addition, privacy regulation is in its infancy, creating uncertainty about how to operate in a compliant manner. Building on the multi-stakeholder privacy framework, we explored the privacy stakeholders' (user, management, policymakers) perspectives on the metaverse, analyzed their relationships, and identified measures to align their interests within a single case study of a German car company. The contribution is twofold. First, we demonstrate the importance of involving privacy stakeholders in the design of products and services in new online environments. Second, we propose privacy measures to reconcile the stakeholders' interests in the metaverse, providing implications for managers and policymakers.

Keywords: Metaverse, privacy, automotive industry

1. Introduction

The metaverse describes the merging of physical and virtual worlds, encompassing a persistent, three-dimensional (3D) virtual environment that is perceived as real (Stephenson, 1992). By employing cutting-edge immersive technologies, such as virtual reality (VR), the metaverse allows users to interact with each other and their environments, which opens up a digital space to live, work, and play (Peukert et al., 2022). Due to its ability to create unprecedented user experiences, the metaverse is predicted with great economic value, up to five trillion US dollars by 2030, as evidenced by the large investments made by numerous companies that have begun to move their products and services into the metaverse (McKinsey, 2022).

An industry that recognized the potential of the metaverse early is the automotive sector, which is undergoing a major transformation from traditional manufacturing to data-driven and software-based business models. In order to remain competitive, car companies must deliver more than just high-quality products, as customers increasingly expect great experiences throughout the entire user journey (Heineke et al., 2023). An example of an early entrant into the metaverse market is Skoda, which has created the 3D metaverse platform "Škodaverse" where users can interact as avatars, play games, take virtual test drives, and attend events (Škoda, 2023). Overall, an increasing number of car companies launch metaverse services with the expectation of brand enhancement, new customer outreach, and product information (Heineke et al., 2023).

While the metaverse can be leveraged to add value by creating immersive experiences, it also brings the potential to invade users' privacy (Bao et al., 2022). In order to provide metaverse services, companies need to collect new forms of user-generated data, such as hand and head movements, which are required to represent digital avatars through VR (Nair et al., 2022). On the one hand, these data offer detailed insights into users' behaviors and preferences, which can be used by companies to improve products and services (Peukert et al., 2022). On the other hand, more extensive data collection can raise privacy concerns, which negatively affects behavior-related outcomes, such as use intentions (Bao et al., 2022). In addition to this trade-off, another driver of complexity is compliance with existing regulatory requirements, which have yet to be defined for the metaverse (Dwivedi et al., 2022). As a result, companies must consider the interests of multiple stakeholders, including their own management, users, and policymakers (Kallemeyn & Chipidza, 2021).

Previous Information Systems (IS) literature has pointed to the importance of broadening the perspective of privacy from the individual level to an integrative view that includes the key privacy stakeholders (Kallemeyn & Chipidza, 2021). We use this theoretical lens to explore the three main stakeholders' (user, management, policymakers) views on privacy in the metaverse and derive implications for decision-makers. We conducted a single case study of a German car

URI: https://hdl.handle.net/10125/106973
978-0-9981331-7-1

company, *CarCo*, using 13 semi-structured interviews and archival data to address the following research questions (RQs):

RQ1*: What are the privacy stakeholders' perspectives on privacy in the metaverse?*

RQ2*: What are the stakeholder relationships and measures for balancing stakeholder interests for privacy in the metaverse?*

The paper is structured as follows. In section 2, we introduce the main concepts, including the metaverse and the multi-stakeholder privacy framework. After presenting the methodological approach in section 3, we demonstrate the results of the case study in section 4, outlining the three stakeholder perspectives on privacy. This includes their perceptions and evaluations on the current implementation of privacy in the metaverse. Next, in section 5, we discuss the relationships between the stakeholders and propose measures, which include actions that companies and regulators can take to harmonize stakeholders' interests and improve overall privacy. In section 6, we outline contributions and implications. Lastly, in section 7, we provide limitations and recommendations for future research.

Our study represents one of the first empirical works to investigate multi-stakeholder privacy in the context of the metaverse. By shedding light on the perspectives of stakeholders and revealing their perceptions and evaluations, we provide a comprehensive assessment of the current implementation of privacy in the metaverse. We add to previous work by illuminating the relationships between stakeholders, thus linking to the multi-stakeholder privacy framework. Furthermore, we present a range of measures that help aligning the stakeholders' interests, which offer meaningful implications for managers.

2. Theoretical background

2.1 Metaverse

The metaverse describes a massively scaled, multi-user, 3D, computer-generated world in which users as avatars can interact with each other and software agents (Stephenson, 1992). The concept was coined in Neil Stephenson's novel "Snow Crash" and has been used to describe different multi-user online environments (Dwivedi et al., 2022). While the first manifestation of the metaverse was introduced in the 2000's with the virtual world "Second Life", the metaverse has been shaped by recent technological advancements (Peukert et al., 2022). In 2021, the metaverse experienced its resurgence with the rebranding of the company Meta (Dwivedi et al., 2022), resulting in a new wave of academic and white paper publications (Ning et al., 2021). Since then, scholars, practitioners, and policymakers have been intensely concerned with exploring its potential and risks and drive its development and diffusion (Peukert et al., 2022). It is predicted that in 2026 a quarter of people will spend at least an hour a day in the metaverse (Gartner, 2022). These numbers suggest that the metaverse changes the way people interact, use services, and do business (Di Pietro & Cresci, 2021).

In comparison to previous applications, the metaverse is characterized by a shift from 2D to 3D media, which is achieved by using immersive technology (Dincelli & Yayla, 2022). Related head-mounted displays (HMD) create advanced experiences by offering 3D visual imagery, spatialized sound, and the opportunity to map natural movements into a virtual representation (Wohlgenannt et al., 2020). These features allow users to interact with their surroundings, creating a sense of presence that ultimately leads to immersion, the mental state of becoming absorbed by a virtual activity (Witmer & Singer, 1998).

Although the metaverse is not a "radical departure" but rather an "incremental evolution" of previous virtual environments, scholars have concluded that the metaverse is different (Richter & Richter, 2023): "In fact, the metaverse is significantly different from any other technological predecessor, being a combinational innovation of multiple emerging digital technologies such as 6G, artificial intelligence, VR, and blockchain" (Mancuso et al., 2023, p. 4). For example, while the metaverse and virtual worlds share some similarities, they differ primarily in terms of access technology (i.e., extended reality (XR) vs. web-based) and interoperability (Richter & Richter, 2023). Furthermore, the metaverse should not be confused with standalone XR applications. While XR is an important gateway to the metaverse, it does not necessarily include a multi-user virtual environment where people interact as avatars (Peukert et al., 2022). Although studies on earlier applications make a meaningful contribution, they cannot account comprehensively for challenges and opportunities posed by state-of-the-art metaverse applications, such as privacy (Dwivedi et al., 2023).

The metaverse represents a new context of data sharing (Dwivedi et al., 2023). While some types of data have already been collected by previous virtual worlds (e.g., personal identifiers such as usernames), combining new and improved technologies allows for collecting new types of data (Dwivedi et al. 2023). For example, HMDs require various user-generated data to map behaviors to the metaverse, such as eye-tracking and room camera data (Nair et al. 2022). These forms of data offer unprecedented possibilities for generating insights about users (Nair et al., 2023). Moreover, while traditional online environments track users' online behavior through cookies, the metaverse goes beyond as

it allows to observe avatars' digital traces in a 3D spatially accessible virtual world – not only by providers but also by a large number of users (Falchuk et al., 2018). This poses new privacy threats, such as devious behaviors like spying or stalking (Falchuk et al., 2018). Furthermore, data traces in the metaverse are more sensitive, as they can be represented by natural body movements, increasing the vulnerability of users (Dwivedi et al., 2023). Combining different data streams gives providers enhanced capabilities to profile users (Wang et al., 2022). Therefore, the metaverse has "potentially broader and deeper impacts" in terms of privacy (Dwivedi et al., 2023), so scholars point to the relevance of studying privacy risks in this new environment (Park & Kim, 2022). To date, the investigation of metaverse privacy is understudied and empirical studies are scarce (Bao et al., 2022).

2.2 Information privacy and multi-stakeholder privacy framework

Historically, the concept of privacy has been defined as an individual's "right to be left alone", following a value-based notion of privacy (Warren & Brandeis, 1890). A later definition described it as a state of limited access to the self (Altman, 1975; Westin, 1968). A few years later, a further notion was introduced by Margulis (1977) who described privacy as the control of the transactions that take place between a person and others. While each of these definitions refers to an individual's physical access, the concept has been reshaped with the upcoming of the information age, which brought up a new understanding of privacy, defining it as the ability to manage and influence information about one's own person (Bélanger & Crossler, 2011). In recent years, scholars have mainly referred to this definition of "information privacy" (used synonymously with privacy) (Xu & Dinev, 2022). When individuals become aware of organizational data-handling practices, privacy concerns unfold, which influence different behavioral outcomes, such as use intentions and disclosure behavior (Smith et al., 2011).

The investigation of privacy concerns and related outcomes has been researched intensively in IS literature in different contexts, whereas technological innovations constantly cause new privacy studies (Xu & Dinev, 2022). While previous works have focused on individuals' perspectives on privacy (Smith et al., 2011), Kallemeyn and Chipidza (2021) introduced a framework that incorporates companies and government as two additional stakeholders in privacy considerations. The framework is based on the well-established idea of privacy as a multilevel construct, suggesting that it manifests at several levels, i.e., individual, group, organizational, and societal (Smith et al., 2011). The multi-stakeholder privacy framework combines the previously isolated levels of analysis and transforms them into agents with different perspectives and dyadic relationships. Threats to privacy can come from any actor and their actions, which have reciprocal effects on each other. Users' privacy concerns can be interpreted as a response to specific circumstances and threats (Kallemeyn & Chipidza, 2021).

The multi-stakeholder privacy framework adds value to previous conceptualizations as it takes a broader perspective on how privacy threats are shaped and regulated by the interplay of the three actors. The framework provides a suitable theoretical lens to investigate the stakeholder's perspectives on privacy in the new context metaverse and analyze their interrelations.

3. Methodology

3.1 Case selection

Considering the emerging nature of the metaverse and its implications for privacy, the lack of substantial evidence on privacy within the metaverse, and the RQs at hand, we chose a qualitative research approach using a single case study. This case study type provides a holistic investigation of a single case and is suitable for critical or unusual cases (Yin, 2018). Due to the novelty of the metaverse, *CarCo* represents one of the first companies to formulate a metaverse strategy. *CarCo* is a German premium car company operating in more than 100 countries and employing more than 90,000 employees. Although many companies have launched metaverse services, *CarCo* has adapted its corporate strategy to exploit the potential of the metaverse on a larger scale. It is pursuing a number of initiatives, including various technologies, platforms, and applications, and is migrating a wide range of services and products into the metaverse. Using a single case study approach allows for in-depth analysis of the stakeholders' perspectives (Yin, 2018).

3.2 Metaverse activities

In 2021, *CarCo* took its first steps in the metaverse with the launch of a virtual multi-user platform designed to increase brand engagement, reach new customer groups, and provide information on their product lines. Today, use cases are manifold. One of *CarCo's* core metaverse initiatives that fundamentally changes car sales is the development of a 3D game engine, which allows customers to configure their car individually and offers the opportunity to make a car purchase. The game engine differs from previous 3D car virtual

configuration via web browser as customers can interactively have a conversation with a salesperson in real-time and access the virtual space from a first-person perspective as a configurable avatar. For the avatar design, *CarCo* cooperates with the provider "Ready Player Me" who offers the generation of interoperable avatars that are compatible with various virtual worlds. In the 3D game engine, users can choose different car styles, change them interactively, view all technical details, and have a virtual driving experience. Besides the salesperson, users can also invite third parties to join the experience. The use case is intended to be hardware agnostic and usable across all relevant media and is currently accessible on mobile, desktop and XR (VR/augmented reality). The first development phase has been completed and the solution has been tested with first customers. It is expected to be rolled out in three targeted markets by 2023.

While this metaverse use case brings new opportunities to transform user experiences, it also raises the question of how to protect users' privacy. Especially HMDs change the privacy situation as they collect a variety of data, such as head and eye movements, body height, and behaviors (Nair et al., 2022). Furthermore, the vehicle configuration provides insight into user preferences. Although *CarCo's* management ensures that vehicle designs are recorded anonymously, the company places highest priority in protecting user privacy. Therefore, personally identifiable information is only collected if the user proceeds with purchasing a vehicle. The only data point currently collected and stored is the user's email address.

3.3 Data collection and analysis

Within our approach, we collected and analyzed interview material and archival data of *CarCo* in order to gain comprehensive insights on the stakeholders' perspectives and understand their relations. During the data collection phase, a close exchange took place with the company between October 2022 and April 2023. Empirical data was gathered by conducting semi-structured interviews. The interviewee sample selection followed the approach of purposeful sampling, which is suitable for investigating information-rich cases (Patton, 2014). This sampling strategy was adjusted to the stakeholder role. For the user group, we interviewed selected customers and employees who had the opportunity to test *CarCo's* metaverse solution via VR. With regards to the manager and policymaker groups, we selected experts, who are employed internally or externally by *CarCo* and have experience in the field of virtual experiences and the metaverse. Their metaverse expertise spanned multiple areas, from immersive technologies to blockchain technology with an average experience of 3,5 years on a range from 2 to 9 years. While the policymaker group provides a legal perspective on privacy in the metaverse, the management group's expertise is related to product or strategic decisions and their implementation. Contact was made via one author's professional network.

A total of thirteen interviews, which lasted 36 minutes on average, were conducted. **Table 1** provides an overview of the positions of the interview partners (IP) and indicates their stakeholder category. The interviews were conducted in German and quotations were translated directly into English. Interviews were conducted either in person or on video conference platforms and were structured by an interview guideline, which was developed based on the RQs and literature. Before each interview, we provided a definition of the metaverse to ensure that the IPs follow the same understanding. Questions were asked according to stakeholder category. In general, the interviews were structured into three parts. First, we asked the IPs about their backgrounds, occupation, and experiences with the metaverse and related technologies. Second, we asked questions about their perception and evaluation of the current implementation of privacy in the metaverse. Finally, we wanted to know about their privacy demands, expectations, and suggestions for the future implementation of privacy.

Table 1. Interview partner details.

Stakeholder category	ID	Position
User	IP7	Independent consultant
	IP8	Business student
	IP12	Junior digital consultant
Management	IP3	Head of digital content creation
	IP4	Business development manager
	IP5	IT product owner
	IP6	Marketing strategist
	IP9	Senior manager innovation and strategy
	IP10	Innovation manager
	IP11	Innovation associate
	IP13	Software engineer
Policymaker	IP1	Digital policy lawyer
	IP2	Corporate data protection

All interviews were recorded, transcribed verbatim, and analyzed within two rounds using qualitative data analysis software. Data was coded inductively in the first round. We applied two coding cycles to the material (Saldaña, 2013). In the first cycle, we used descriptive coding to condense the meaning of the data segments, followed by attribute coding, which helped us extracting

basic information from larger segments of data (e.g., attitude towards metaverse). The second coding cycle includes "classifying, prioritizing, integrating, synthesizing, abstracting and conceptualizing, and theory building" (Saldaña, 2013, p. 58). We applied pattern coding, which groups the material into explanatory and inferential codes. The resulting categories represent the stakeholders' perceptions, evaluations, and demands on privacy in the metaverse. In the second round of data analysis, the resulting code set was clustered deductively along the multi-stakeholder privacy framework to relate our findings to the theoretical framework. To draw conclusions from the final coding set, the inferential codes were mapped for each three stakeholder groups to analyze the dyadic relationships. We further synthesized the proposed privacy measures and enriched them with results from the literature and examples of real-world applications. Because of the novelty of the metaverse, we follow guidelines for building theory from case studies (Eisenhardt, 1989).

A team of two researchers, performed data analysis independently, whereas outstanding differences were discussed until a consensus was reached (Miles et al., 2014). This approach ensured reliability and increased objectivity. To prepare for the interviews and to understand the relevance of the use case for *CarCo*, archival data (e.g., internal documents and privacy-related reports) was analyzed.

4. Results

4.1 User's privacy perspective

The interviewed users are generally equally open to the metaverse, appear interested, and name several benefits: "*I do think that that's definitely going to be a part of the future*" (IP8). In terms of data sharing, the IPs are willing to disclose some data in order to have full user experiences. When users were given the choice for full privacy or the unrestricted virtual experience, they all chose the latter and would accept the piecemeal loss of their privacy: "*I would do the full user experience, for the price of my data*" (IP8). Thus, users are aware that a range of data is collected, but this does not prevent them from using these services.

However, the interviews indicate that data collection is generally an important issue for users and that personal data collection is a relevant factor in their use decision (IP12). Although users are comfortable with collecting data in exchange for advanced experiences, they reported concerns about which data is collected and how it is used (IP7). Currently, users do not feel sufficiently informed about the gathered data types: "*I do think there is a lot of data being disclosed, but I don't know to what extent or what is being collected - the companies don't really explain what exactly is being done*" (IP8). This lack of information leads to a lack of trust in companies regarding data analysis: "*The problem a user has is, two years after the industry pulls data from me, you read in the press what they have pulled from you*" (IP7). In general, trust in providers plays a crucial role in the decision to use a metaverse service and disclose data (IP12).

Due to this perceived information asymmetry, users emphasized that they want to know the consequences of their data sharing in the metaverse at the outset. Although privacy statements are provided, users agreed that privacy statements and consent notices are overly complicated (IP7). As a result, many are overwhelmed by these statements and simply click "agree" instead of fully and consciously agreeing to the policies (IP7). In sum, users care about their privacy, but when it comes to privacy statements, they often behave in counterproductive ways. Therefore, users demand more transparency on data collection and processing practices (IP12), clarity about the consequences of their data sharing (IP8), and simplicity in privacy policies (IP7).

4.2 Management's privacy perspective

Interviewees from the management category agreed that the metaverse will affect the way companies do business in unpredictable ways (IP3, IP5). With respect to privacy, the IPs said that handling data is becoming a differentiating competitive factor, not only because data is becoming more valuable as an asset (IP3), but also because of how user data is handled by a company: "*Privacy and information protection will become a differentiating feature. They can also generate a positive brand value, which I don't think has been the case before*" (IP11). According to the IPs, users nowadays have a strong preference for maximizing privacy in the digital space (IP9, IP13). Also, trust in the brand is reported as a crucial aspect that determines concerns about sharing personal data (IP6, IP9).

Overall, the IPs from the management group noted that *CarCo* faces several competing privacy objectives. On the one hand, business objectives drive how data is handled (IP5). Therefore, *CarCo* has a strong demand to control platforms and related data flows: "*When we talk about our own platforms, we want to be the owner of the data and the controller of the data*" (IP3). On the other hand, users' demands for privacy have changed, but so have their expectations for user experience, which in turn requires more data: "*In the future, there will be a lot more work with data. And of course, this will have an impact on the customer experience*" (IP10). Therefore, the IPs mentioned that metaverse solutions

need to be designed in a way that makes data collection comprehensible to users (IP5, IP11).

CarCo's awareness of privacy aspects is also reflected in their data minimization policy (IP4). The IPs ensured that *CarCo* prioritizes user privacy and report that they have no need to generate value from selling customer data: "*We try to collect as little data as possible*" (IP4). No tracking or selling of user data is conducted (IP5). Only through double opt-in consent, personal data may be further processed, and advertising offers sent to users (IP6, IP9). *CarCo* thus relies on transparency and user self-control: "*Transparency is provided when the customer can actually decide on his own responsibility and autonomously. It's about protecting the personal rights*" (IP10).

Also, in the virtual world, *CarCo* is concerned with privacy protection related to avatar appearance and behavior. According to the IPs, the creation of avatars in a virtual world should not be restricted in principle (IP3, IP5). Users should be able to create a second identity according to their individual needs (IP4). However, following IP3, the anonymity of avatars in the metaverse also creates options for devious behaviors in open metaverse worlds: "*I see a reverse problem here. Any avatar can be anonymous at any time, which unfortunately carries a high risk that people will abuse this for their own benefit*" (IP3). Users could exploit this freedom and associated anonymity in the metaverse. Therefore, *CarCo* is working to develop governance mechanisms to balance freedom and anonymity based on user preferences (IP5).

Another challenge for *CarCo* is missing guidance from regulatory institutions on the implementation of privacy in the metaverse: "*The current legal situation is not yet sufficient at this point*" (IP4). In addition, IPs reported uncertainty about who is responsible for ensuring privacy: "*The question is, do I have a responsibility? Or does the metaverse have to provide the privacy basis? This is incredibly difficult to clarify but clearly, we need legal advice here*" (IP6). Furthermore, the demarcation between legal borders is not given (IP5). Due to these regulatory uncertainties, IP6 sees qualified legal advice as overdue. The IPs advocate for technical standards that are mandated by legislation and accepted worldwide (IP5, IP6).

4.3 Policymaker's privacy perspective

From the interviews, it appears that there is no universally applicable regulatory framework for user privacy in the metaverse and there is a lack of guidance from regulatory institutions. IP2 believes that the European General Data Protection Regulation (GDPR) does not currently and will not in the future apply to the metaverse due to the generic formulation of rules: "*GDPR cannot cover the metaverse - the data protection laws are not clearly interpretable […]. They are so generic that a lot must be interpreted*" (IP2). Therefore, IP2 complains about the great deal of interpretation to be done in this area of law and especially for the automotive sector. According to IP1, the current legal framework in the digital space is not conclusive due to its technology neutrality: "*The GDPR suffers from the fact that it sees itself as technology-neutral*". Hence, companies face a great challenge in complying with legal regulations and that this compliance appears to be "*almost impossible*" in the metaverse context (IP1).

Respondents agree that there is a need for regulation of the metaverse, however, current legal provisions, such as the requirement of data minimization, contradict the idea of the metaverse (IP1, IP2). Therefore, they mention a need to revise rules and laws in regular and short intervals. IP2 believes that this will require the creation of new laws for the metaverse, which should be applied and accepted uniformly around the world: "*As the metaverse has no geographical border, this issue will intensify in the metaverse. The virtual world is not based in any country, here the question is whether to make new laws that are then uniform worldwide*".

Besides high requirements to comply with regulatory standards, the IPs also reported on challenges resulting from high demands of users. IP2 emphasizes that customers sometimes use small privacy violations to blackmail companies: "*Customers use the data protection, to a large extent, for extortion*" (IP2). IP2 sees a shared responsibility from user and companies to inform about privacy: "*Everyone knows how to write privacy, but very few know what it means or why you should do it*". One issue that is currently causing great uncertainty among policymakers is the question of accountability (IP1).

5. Discussion

In an in-depth case study of a German car company that has achieved a leading position in providing metaverse products and services, we explored the perspectives of the three privacy stakeholders (user, management, policymakers) on the metaverse. Although some types of data were collected in previous virtual applications (e.g., usernames), the metaverse represents a new context for data sharing, as advanced technologies collect a range of new sensitive data, and the exposure of public online spaces makes digital traces easier to track (Nair et al., 2022). Therefore, the rules for privacy in the online space must be renegotiated (Kallemeyn & Chipidza, 2021).

To identify the stakeholder perspectives and propose measures to align their interests, we conducted

13 interviews and analyzed archival data collected over a three-month period as part of a case study. While some aspects mentioned by the IPs were known from previous virtual applications, our results show that all three stakeholders face new uncertainties and report several privacy challenges. In the following, we describe the relationships among the stakeholders (5.1) and discuss measures that contribute to aligning their interests (5.2). An overview of the stakeholder relationships is provided in **Figure 1**.

5.1 Relationships between stakeholders

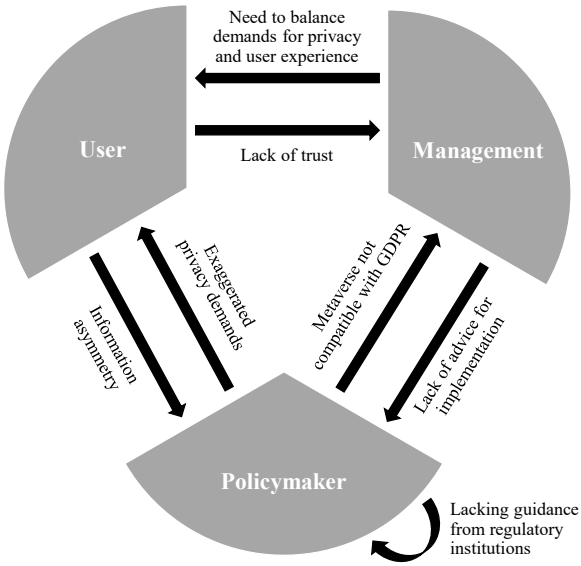

Figure 1. Relationships between privacy stakeholders.

(1) User / Management. Our results demonstrate that users are willing to provide data in exchange for advanced metaverse experiences. However, they showed some skepticism about *CarCo's* practices on data processing and analysis. Although users do not know exactly which data is concerned, they perceive that more and more sensitive data is involved in metaverse services, compared to previous virtual environments. Thus, they have low trust in companies to handle their data responsively. These results are in line with Adjerid et al. (2018) who show that although individuals may not be fully informed about data handling, they raise privacy concerns when they perceive a relative change of privacy. *CarCo*, on the other side, knows about the importance of protecting their users' privacy and has implemented a range of privacy protection measures. The company regards privacy as a competitive advantage and dispense from tracking techniques or selling users' data. However, to create advanced user experiences, it is necessary to collect a certain amount of data. The example of *CarCo* shows that there is a gap between company's efforts to protect privacy and what users actually perceive.

(2) User / Policymaker. Users do not feel sufficiently informed about *CarCo's* data practices and perceive an information asymmetry. Although privacy policies are provided, users complain about their complexity. The lack of understandability and accessibility of privacy policies was investigated in numerous studies, which showed that traditional privacy policies are ineffective in creating transparency and trust as users do not read or understand them (Gerlach et al., 2015). On the other side, *CarCo's* legal staff reports that users are not interested in privacy, which is why they make zero efforts in reading any privacy statements. Moreover, they argue that some users even use small violations of privacy as a form of blackmail to get advantages from the company.

(3) Management / Policymaker. *CarCo's* legal staff reported that they cannot adequately advise the management because they do not receive sufficient guidance from regulatory institutions who pass laws, such as the GDPR. According to them, GDPR, which regulates data collection and processing in the European Union, does not provide guidance on technology implementation and its terminology is perceived as too generic. Therefore, they note that it is not possible to be 100 percent compliant with it, especially with the new privacy circumstances brought by the metaverse. Due to this uncertainty, also the management does not feel sufficiently advised for their implementation and product decisions. For example, it is not clear who is responsible for monitoring and controlling adherence to privacy standards of metaverse worlds. Another area of tension is the differing interests of management and policymakers. While management has economic and business interests in collecting user data, the primary goal of the legal department is to implement existing regulations. As a result, legal professionals must simultaneously meet the goals of two interest groups and balance their requirements.

5.2 Privacy measures

Potential measures to align the stakeholders' interests are outlined in **Table 2** and described in the following. The identification of the measures is based on the expressed needs and suggestions of the participants, the analysis of their relationships, and is enriched by existing literature.

(1) User / Management. Although both stakeholders have the same priorities and goals in terms of privacy, users have another perception of what is actually provided by companies. Therefore, companies should proactively communicate their efforts. An

example of a brand that strongly communicates privacy is Apple who even focused on privacy rather than their products in commercials (Apple, 2023). In order to reach their privacy-sensitive target group, *CarCo* should integrate privacy aspects into their brand promise or make a binding commitment, for example, in the form of a code of ethics to clearly position itself with regard to privacy. This should be communicated to users in a comprehensible way to reinforce users' trust. Another solution is to segment target group into active customers and potential customers and vary data collection according to this segmentation (Gerlach et al., 2019).

Table 2. Measures for balancing privacy stakeholders' interests.

Stakeholder relationship	Measures
(1)	**Communication** of privacy efforts
	Segmentation of customers according to privacy preference
(2)	Accessible **privacy policies**
	Surveys for privacy preferences
	Transparency & **control** features
	Privacy **seals**
(3)	**Collaboration** with firms, regulatory institutions, and standards agencies
	Revision of **regulation** and **laws**

(2) User / Policymaker. Results show that there are strong tensions between users and policymakers resulting from diverging understanding of what is sufficient transparency on data-handling practices. Previous studies have demonstrated that in order to build trust, privacy policies should be more accessible (Gerlach et al., 2015). Also, the interview partner gave some indications on possible approaches. IP2 proposes to involve users in the process of data collection, in the form of customer surveys, studies, or recommendation systems. This helps understanding customers' privacy preferences and demands. Another option is providing transparency and control mechanisms like privacy settings or opt-out features that gives users the ability to decide which data they want to provide. This can be advantageous for companies as it reduces privacy concerns and enhances trust (Xu et al., 2012). Control features and privacy settings are already a common feature in many metaverse worlds, such as VRChat (2023). Another option is to pursue privacy signaling. IP2 recommended to include third parties who verify compliance with data protection at regular intervals. The effect of privacy seals on creating trust was also shown by previous studies (Xu et al., 2012).

(3) Management / Policymaker. While the metaverse is at the beginning of its development, it can be seen that standards are not yet conclusively regulated (Di Pietro & Cresci, 2021). Due to the different requirements, companies and policymakers should collaborate to negotiate the rules and standards underlying the metaverse collectively (Kallemeyn & Chipidza, 2021). An example is provided by the "Metaverse Standard Forum", which brings together companies, certification agencies, and scientists to discuss and formulate uniform standards for the metaverse (Metaverse Standards Forum, 2023). Besides legal issues, also technical standards are discussed. Moreover, also regulatory institutions should participate in the definition of binding regulations. An example provides the German government that organized an open panel discussion to which they invited metaverse experts, policymakers, and citizens (Deutscher Bundestag, 2022).

6. Contribution and implications

With the emergence of the metaverse, privacy conditions have changed due to more invasive forms of data collection and processing (Nair et al., 2022). However, despite numerous calls for research (Dincelli & Yayla, 2022; Dwivedi et al., 2022), empirical studies on privacy in this new environment are scarce in IS research (Bao et al., 2022). This study contributes by investigating privacy in a large-scale, market-ready metaverse application of an automotive company from different stakeholder perspectives. By building on a rich set of data from a real case, it adds to existing studies who treat privacy only as a side issue. Moreover, the study considers the metaverse within a real-world business case, going beyond hypothetical privacy considerations.

Within the privacy field, the study ties in with the multi-stakeholder privacy framework, which we apply to the metaverse context and thereby add to the so far rare investigation of privacy as a multilevel concept. Our study sheds light on the privacy stakeholder's perspectives, their relationships, and proposing adequate measures to align their interests. Thereby, we demonstrate the frameworks' applicability to explore changed privacy circumstances in new online environments and show that decision-makers must take all perspectives into account to successfully launch new products and services.

Our findings indicate that the introduction of the metaverse as a new digital innovation that is more data-intensive than previous applications, brings uncertainties for all stakeholder groups and causes tensions between them. While previous studies have demonstrated the effect of uncertainty on users' behavioral outcomes (Pavlou et al., 2007), literature has neglected uncertainties for companies' and

policymakers' decision-making. For example, Dinev and Hart (2006) used uncertainty as an index to investigate cultural differences in individual privacy decisions. Our results suggest that uncertainty is also a determinant of business and policy decisions. In addition, the results show that the uncertainties of the stakeholders influence each other, which makes it necessary to renegotiate agreements collectively.

An alignment between the stakeholders' privacy interests can be achieved through a range of measures, some of which we present in this study. Previous studies have largely demonstrated the effectiveness of privacy assurances on privacy decisions (Xu et al., 2012). However, these studies have focused on changes in user behavior and have neglected the preferences and consequences of businesses and policymakers. Our findings present some measures that integrate the interests of all stakeholders in the context of the metaverse. The findings are transferable to other contexts in which organizations face new privacy challenges, as it shows that in situations of privacy uncertainty, stakeholders must reconcile their privacy interests until certain guidelines are established.

From a practical point of view, our results demonstrate that managers must balance different interests when implementing digital products and services in new online environments. Previous research has shown that firms face trade-offs when making privacy decisions (Gerlach et al., 2019). Our findings suggest that uncertainty in new online environments exacerbates these trade-offs, as firms have little transparency about customer preferences and legal frameworks are not yet established. However, especially in new markets, speed is important to achieve a good market position. Therefore, companies have two options. Either they launch services early and risk violating privacy laws and suffering reputation loss, or they wait until regulations and standards are defined but may lose the opportunity to build a good market position. Our findings suggest that in competitive markets that are driven by digital innovations, companies are eager on being a leader and not miss business opportunities like the metaverse. *CarCo* has achieved this market leadership position, while at the same time implemented a range of privacy measures.

7. Limitations and future research

This study includes limitations, which provide starting points for future research. First, while the interviews provide comprehensive and rich insights into the views of the three privacy stakeholders, the study is focused on providing a broad rather than a deep picture of the current implementation of privacy in the metaverse. Therefore, the results should be strengthened by further interviews and follow-up studies.

Second, while the case study highlights a certain industry, it is possible that perspectives and relationships between the stakeholders and the proposed privacy measures differ for other contexts. Although many industries engage in similar metaverse activities, their regulatory and business settings may deviate (e.g., financial industry). Future studies can include further industries to increase generalizability. Further, while this study had a focus on data collection in immersive environments, future studies could complement the findings by including additional metaverse technologies, such as blockchain (Xu et al., 2022).

Finally, as *CarCo* is operating in the European Union (EU), we referred to this legal area in our considerations. Future studies could integrate other legal areas. Yet, the development of the metaverse is in an early stage, leaving room for a comprehensive consideration of potentials and risks. We shed light on privacy risks from a multi-stakeholder perspective and hope that our results motivate future studies researching privacy in the metaverse.

8. References

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly 42*(2), 465-488.

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

Apple. (2023). *Privacy. That's Apple.* Retrieved 10.06.2023 from https://www.apple.com/privacy/

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 (ECIS), Copenhagen, Denmark.

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.

Deutscher Bundestag. (2022). *Metaverse: Zwischen großen Chancen und Hype*. Retrieved 10.06.2023 from https://www.bundestag.de/dokumente/textarchiv/2022/kw50-pa-digitales-925124

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,

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*(2), 1-22.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Dwivedi, Y., Kshetri, N., Hughes, L., Rana, N., Baabdullah, A., Kar, A., Koohang, A., Ribeiro-Navarrete, S., Bele, N.,

Balakrishnan, J., Basu, S., Behl, A., Davies, G. H., Dutot, V., Dwivedi, R., Evans, L., Felix, R., Foster-Fletcher, R., Giannakis, M., . . . Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*.

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).

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

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

Gartner. (2022). *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026* https://gtnr.it/42pIiJo

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The journal of strategic Information Systems*, *24*(1), 33-43.

Gerlach, J. P., Eling, N., Wessels, N., & Buxmann, P. (2019). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal*, *29*(2), 548-575.

Heineke, K., Khan, H., Möller T., Schedhelm, D., & Srivastava, S. (2023). *The metaverse: Driving value in the mobility sector*. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-metaverse-driving-value-in-the-mobility-sector

Kallemeyn, D., & Chipidza, W. (2021). Towards a Forward-Looking Conceptualization of Privacy. Proceedings of the Forty-Second International Conference on Information Systems (ICIS) Austin, Texas.

Mancuso, I., Petruzzelli, A. M., & Panniello, U. (2023). Digital business model innovation in metaverse: How to approach virtual economy opportunities. *Information Processing & Management*, *60*(2023), 1-28.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues 33*(3), 5-21.

McKinsey. (2022). *Value creation in the metaverse - The real business of the virtual world*.

Metaverse Standards Forum. (2023). *Metaverse Standards Forum: Fostering interoperability standards for an open metaverse*. https://metaverse-standards.org/

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis. A Methods Sourcebook* (3 ed.). SAGE Publications.

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*.

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2021). A survey on metaverse: The state-of-the-art, technologies, applications, and challenges. *arXiv preprint 2111.09673*.

Park, S.-M., & Kim, Y.-G. (2022). A Metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, *10*, 4209-4251.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice* (4 ed.). SAGE Publications.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly 31*(1), 105-136.

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.

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*(2023), 1-11.

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2 ed.). SAGE Publications.

Škoda. (2023). *Škodaverse*. https://www.skoda-auto.com/world/skodaverse

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly 35*(4), 989-1015.

Stephenson, N. (1992). *Snow Crash*. Bantam Book.

VRChat. (2023). *VRChat Safety and Trust System*. Retrieved 10.06.2023 from https://docs.vrchat.com/docs/vrchat-safety-and-trust-system

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319-352.

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.

Wohlgenannt, I., Simons, A., & Stieglitz, S. (2020). Virtual reality. *Business & Information Systems Engineering*, *62*(5), 455-461.

Xu, H., & Dinev, T. (2022). Why Privacy Still Matters. *MIS Quarterly 46*(4), xx-xxxii.

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, Rome, Italy.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, *23*(4), 1342-1363.

Yin, R. K. (2018). *Case study research: Design and methods*. SAGE Publications.