Virtual influencers and data privacy: Introducing the multi-privacy paradox

Gajendra Liyanaarachchi, Matthieu Mifsud, Giampaolo Viglia

Virtual influencers and data privacy: Introducing the multi-privacy paradox

Gajendra Liyanaarachchi[a], Matthieu Mifsud[b], Giampaolo Viglia [a,c,1]

[a]University of Portsmouth, Department of Strategy, Marketing and Innovation, Richmond Building, PO1 3DE, UK.

[b]Audencia Business School, Department of Marketing, 8 Route de La Jonelière, 44312 Nantes, France.

[c]University of Aosta Valley, Department of Economics and Political Science, Street Cappuccini 2, 11100 Aosta, Italy.

[1] Corresponding author: giampaolo.viglia@port.ac.uk

Virtual influencers and data privacy: Introducing the multi-privacy paradox.

Abstract

Virtual influencers have a growing presence in social media, reshaping the traditional interactions between influencers and followers. Through an interdisciplinary orientation, we assess the implications of this phenomenon for data privacy. Specifically, we argue that, given that the virtual influencer is not a human being, an unbalanced privacy risk arises from

possible data vulnerability, cybercrime, and the creation of fake profiles. We explore these risks through a qualitative exploratory study with 28 followers of virtual influencers. Our work culminates with a conceptual framework that highlights what we define as a multi-privacy paradox. We offer actionable ways for organizations to manage privacy and protect consumers dealing with virtual influencers in the metaverse.

Keywords: virtual influencer; data privacy; unbalanced privacy risk; data vulnerability, cybercrime; fake profile; multi-privacy paradox; metaverse

1. Introduction

Virtual influencers are poised to transform the business landscape, offering significant advantages for marketers and brands (Campbell et al., 2022). They outperform traditional influencers in value delivery consistency and availability (Leung et al., 2022). Controlled autonomously by AI, these virtual entities, as Sands et al. (2022) point out, enhance consumer experiences. Despite the inability to present in real life, virtual influencers can reach an unprecedented audience (Lou et al., 2022; McKenna & Chughtai, 2020). Take, for example, Lil Miquela, the fictional 19-year-old robot influencer. She has amassed a multi-platform following of millions, with high-profile collaborations including Prada, Samsung, and Calvin Klein, and is recognized by Time Magazine as one of the most influential people on the Internet (Ahn et al., 2022; Mustak et al., 2023; Robinson, 2020; Time, 2018).

The role of virtual influencers becomes increasingly critical in the context of the metaverse, defined by Mitrushchenkova (2023) as an Internet evolution into a unified, virtual space that mirrors human life with greater fidelity. Here, users interact, partake in events, and transact with cryptocurrencies. Cheng et al. (2022) view this as a new phase in the computing revolution, with Gartner (2022) forecasting that by 2026, a quarter of people will spend at

least an hour daily in the metaverse. While the metaverse offers unique societal and business opportunities, concerns arise over privacy risks, as Dwivedi et al. (2022) and Park & Kim (2022) highlight, especially given the massive data management it entails.

Despite virtual influencers' success, privacy remains a critical challenge for the future. Consumer data are vulnerable to manipulation and unauthorized access, undermining influencer credibility (Dwivedi et al., 2022; Sands et al., 2022). More research is needed to develop strategies to protect privacy and minimize consumer vulnerability in the metaverse (Zhang et al., 2023).

The spread of misinformation through virtual influencers, who manage sensitive data, raises alarms about data breaches and nefarious manipulation (Dwivedi et al., 2022). Data privacy significantly shapes public perception of digital technologies (Maseeh et al., 2021). Therefore, a comprehensive examination of the relationship between virtual influencers and data privacy is crucial.

The non-human nature of virtual influencers introduces a privacy risk asymmetry, where followers face greater privacy risks, leading to an "unbalanced privacy risk." This paper argues that such risks affect followers' well-being and their relationships with virtual influencers, creating a heightened privacy paradox, a psychological conflict where there's a discrepancy between attitudes and behaviors concerning information sharing.

While existing literature on the privacy paradox highlights inconsistencies in consumer information-sharing behaviors, the unbalanced privacy risk represents a novel challenge, underscoring the need for a broader approach to privacy management. This paper aims to bridge this gap, offering new insights into the complex privacy dynamics in the virtual influencer domain within the metaverse. Through 28 in-depth interviews with virtual influencer followers, this study provides exploratory insights into user interactions and

privacy concerns, leading to a proposed framework for managing privacy to sustain virtual influencer credibility (see Figure 1).

The article introduces the "multi-privacy paradox," expanding the traditional privacy paradox to encapsulate the transfer of privacy impact from virtual entities to their legal stakeholders. It advocates for a collective strategy to combat cybercrime and misinformation, thus safeguarding consumer privacy and fostering healthier engagement with virtual influencers in the metaverse.

2. Literature Review

2.1. Privacy paradox

The privacy paradox depicts the discrepancy between attitudes and behaviors in disclosure (Barnes, 2006; Norberg et al., 2007), where consumers share information, ignoring their privacy concerns (Awad & Krishnan, 2006; Jorstad, 2000). Scholars have explained the paradox from normative and behavioral perspectives, yet a resolution remains elusive due to contextual complexities (Acquisti et al., 2023). Research adopting the normative perspective (Dienlin & Trepte, 2015; Dienlin et al., 2023; Solove, 2021; Smith et al., 2011) defines the privacy paradox rationally, often overlooking situational influences on disclosure behavior. For example, followers of virtual influencers divulge information due to social pressure, irrespective of their privacy concerns. Amid rising cybercrime, fake profiles, and data vulnerability, the behavioral perspective (Acquisti et al., 2015; Adjerid et al., 2018; Colnago et al., 2023; Norberg et al., 2007) gains significance, exemplified by consumers sharing data despite knowing the apparent risks.

The idea of the paradox arises with an attitude reflecting the intention and behavior depicting the actual disclosure decision. Dienlin and Trepte (2015) employed two separate methodological approaches to investigate the privacy paradox with the same sample, resulting in disparate outcomes; one acknowledged the privacy paradox's existence, while the

other failed to recognize it. However, despite the incongruity in results, the study ultimately suggests that the privacy paradox may no longer hold validity, stating it is a relic of the past. Likewise, Solove (2021) contends that the privacy paradox is a myth, asserting that behavior pertains to context-specific disclosure decisions and attitudes encompass a generic privacy concern. As a result, the two concepts are incomparable to consider a paradox. In a longitudinal study, Dienlin et al. (2023) discovered incongruous results while examining the validity of the privacy paradox, highlighting the need for additional research to understand the concept comprehensively.

The primary basis for rejecting the concept arises from studies frequently misconstruing attitudes and behavior in isolation as separate entities. As highlighted by Alashoor et al. (2022), these studies have treated attitude as an outcome, neglecting actual behavior and approaching behavior as decisions without incorporating the influence of attitude. In contrast, Adorjan and Ricciardelli (2019) identified a reversal of the attitude-behavior gap, where individuals share more information than intended, extending the original idea of the paradox where behavior overrides attitude. In line with this thinking, Colnago et al. (2023) introduce the reverse privacy paradox, which reveals that individuals displaying minimal privacy concerns exhibit behaviors safeguarding privacy. However, despite their reciprocal differences, both original and reverse privacy paradoxes substantiate the doctrine's existence, highlighting the prevalent divergence between attitudes and actual behavior. Also, Flender and Müller (2012) identified similarities between the privacy paradox and quantum theory. They outline that privacy paradox manifests quantum phenomena like indeterminacy, where decisions are determined according to the situation rather than intended, aligning with behavior-dominant privacy decisions.

Conducting systematic literature reviews of the privacy paradox, scholars Barth & De Jong (2017), Gerber et al. (2018), Gotsch & Schögel (2021), and Kokolakis (2017)

emphasize that while certain studies have raised questions about the validity of the privacy paradox, a substantial majority of research recognize its existence. Furthermore, these reviews demonstrate that the privacy paradox has often been examined within specific contexts, and future research should focus on developing a comprehensive and universally applicable definition. Further, Liyanaarachchi (2021) points out that research on the paradox frequently has a confined scope, primarily focusing on specific industries or customer segments.

Acknowledging the scholarly discourse, this study explores the privacy paradox within the metaverse, a comprehensive ecosystem interconnecting consumers, organizations, industries, and global regulatory governance with a broader stakeholder perspective. In the metaverse, data collection encompassing users' online experiences has given rise to instances exemplifying the privacy paradox (Hilken et al., 2022). This paradox ingrains itself within the metaverse due to the progressively mounting value of consumer data over time, prompting organizations, consumers, and regulators to consider intensified privacy protection. Further, the continuous availability of data in the metaverse after its intended use perpetuates the persistence of the heightened privacy risk (Buck & McDonnell, 2022).

Chan and Greenaway (2005) categorized information privacy research into three distinct tiers: personal, organizational, and sectoral, underscoring the deficiency of studies addressing the organizational level. This gap in organizational-level research is evident, as research predominantly examines the issue from a personal consumer perspective (Liyanaararchchi et al., 2021; Martin & Murphy, 2017). Gotsch and Schögel (2021) suggest that organizations can address the privacy paradox by altering their privacy strategy, structural framework, and human resource practices and introducing new services; the current study addresses the organizational literature gap by synthesizing all three levels—consumers,

organizations, and the sector—to create a comprehensive global ecosystem that mirrors the evolving metaverse.

2.2 Metaverse and virtual influencers

The word "metaverse" first appeared in the science fiction novel by Neal Stephenson named Snow Crash in 1992 (Mourtzis et al., 2022). Originally, the word is a crossword made up of the terms "*meta*" (i.e., beyond) and "*universum*" (i.e., all things, everybody, all people, the whole world), which was later assembled into "metaverse" (meta and universe). The metaverse is, therefore, a meta-universe, a universe that goes beyond the one we know. Journalists, practitioners, and academics now use this word to refer to any structured and open virtual world.

Even though the concept was coined three decades ago, the metaverse has recently gained worldwide attraction (Kim & Kim, 2021). It has been labeled as a new and disruptive paradigm that can potentially transform future business and social life (Barrera & Shah, 2023; Belk et al., 2022). The metaverse will revolutionize nearly every industry and "value functions" of companies in the future (Boyd & Koles, 2019; Hollensen et al., 2022). It could offer a unique opportunity for brands to strengthen their relationships with consumers by delivering new levels of customer interaction, engagement, and value cocreation (Barrera & Shah, 2023; Shen et al., 2021). Therefore, technology firms such as Facebook (now renamed Meta) or Microsoft are financing millions of dollars in building virtual worlds consistent with the notion of the metaverse (Kelly, 2021).

The metaverse represents a digital space of user-controlled avatars, virtual environments, and other computer-generated elements like virtual influencers. In this virtual world, humans (represented by avatars) can use their virtual identities to communicate and collaborate to generate value and co-create experiences (Gursoy et al., 2022). Further, as the

boundary between human and bot-like behavior becomes less separate (Robinson, 2020), a virtual influencer can have a considerable network of followers. It can be regarded as "a trusted taste-maker in one or several niches" (De Veirman et al., 2017, p. 798). Leveraging the immersive nature of this virtual realm, virtual influencers have the potential to establish more seamless connections with human participants. However, these interactions can result in heightened data collection and the potential for misuse. Due to unauthorized access, individuals' personal information becomes susceptible to manipulation, forgery, or misrepresentation. Furthermore, the invasion of followers' online profiles creates an unbalanced privacy risk, especially given that virtual influencers are non-human entities. Thus, the connection between virtual influencers and data privacy warrants a closer examination from both practical and academic perspectives.

Virtual influencers are computer-generated entities replicating human physical attributes, behaviors, and personalities (Park & Kim, 2022). These entities are generated through a fusion of 3D modeling and artificial intelligence (AI) to react to contextual situations and stimuli (Baudier et al., 2023). Employing virtual influencers allows brands the autonomy to hold their representatives in alignment with their creative concepts and represent a brand's values (Arsenyan & Mirowska, 2021; Djafarova & Rushworth, 2017), while human influencers aspire to garner recognition and cultivate cultural influence by sharing content on their social profiles (Audrezet et al., 2020). Moreover, virtual influencers offer cost benefits over time since traditional influencer marketing necessitates budget allocations and specific organizational endeavors (Tan & Liew, 2020; Arsenyan & Mirowska, 2021).

Only a limited number of studies have delved into the realm of virtual influencers, concentrating on understanding engagement motivations or disparities from real-world influencers (Arsenyan & Mirowska, 2021; Lou et al., 2022), investigating influencers' intersectionality (Miyake, 2023) as well as addressing specific ethical concerns (Robinson,

2020). Nonetheless, the potential privacy risks associated with virtual influencers and the metaverse have remained relatively unexplored, prompting calls for empirical investigations into this subject (Barrera & Shah, 2023; Dwivedi et al., 2022).

Data collection practices exhibit considerable diversity contingent upon the particular metaverse platform, service provider, and local regulations in the metaverse. For instance, users provide details such as usernames and e-mail addresses during the registration and account creation process. Additionally, behavioral and interaction data are accumulated when users engage with virtual influencers or avatars. Information about the user's device, location, virtual currency transactions, and social interactions (including messages, chats, and virtual engagements) also contribute to the potential data collection. In the metaverse, data is typically analyzed using a combination of predictive algorithms, real-time customer data analytics, and virtual navigation tools (Kliestik et al., 2022). These technologies allow for the processing and interpreting various types of data generated within the metaverse, enabling insights into user behaviors, preferences, interactions, and experiences.

Because of this extensive data collection, the metaverse denotes a significantly higher privacy risk. As a result, scholars have stressed the ethical implications of marketing within the metaverse, emphasizing the necessity for responsible and sustainable data collection and use (Dwivedi et al., 2022). The potential for unethical use of metaverse data is increasingly significant, with threats to consumer privacy arising from many forms, such as cybercrimes, identity theft, and blackmail (Hilken et al., 2022; Hollensen & Dwivedi, 2023; Rauschnabel et al., 2018). Understanding these challenges is thus crucial for firms and academics (Hollensen & Dwivedi, 2023).

3. Conceptual underpinnings

The research introduces a conceptual framework (see Figure 1) encompassing data vulnerability, cybercrime, and fake profiles as the antecedents for the emergence of unbalanced privacy. Aligned with this framework, we construct exploratory propositions to integrate the empirical results outlined in Viglia et al. (2023). The investigation posits that the cumulative impact of data vulnerability, cybercrime, and fake profiles culminates in an asymmetrical state of consumer privacy concerning virtual influencers.

3.1. Data Vulnerability

Virtual influencer marketing involves lifestyles and consumption trends to engage consumers and induce them to purchase sponsored products (Sands et al., 2022). Followers' personal information is available in the metaverse infinitely after an online engagement, leading to data vulnerability. Data vulnerability can be defined as the exploitation of personal information through unauthorized access, violating the original intention of data collection (Martin & Murphy, 2017). It represents an enormous threat to companies. For example, the hacking of the dating app 'Heyyo' exposed the personal details, images, location data, phone numbers, and dating preferences of nearly 72,000 users (Brown, 2020). Consumers are concerned about the risk of disclosure mainly due to losing control over data (Ameen et al., 2022; Audrezet et al., 2020).

Consumer data vulnerability arises due to the powerlessness that occurs from an unbalance in marketplace interactions where the consumer has no control or ownership over data (Echeverri & Salomonson, 2019; Wanjugu et al., 2022). Further, the dependency of virtual influencers on the metaverse for continuous correspondence with followers increases the risk of data vulnerability. Advanced advertising employing AI-driven manipulation techniques convinces consumers to embrace misleading perceptions, ultimately rendering them vulnerable to deceptive practices (Campbell et al., 2022). On the one hand, consumers

operate without a realistic idea of the gravity of unauthorized access and continue to share data, believing that the organizations can protect privacy (Nunan, 2021). On the other hand, they indirectly contribute to a data breach by ignoring self-regulatory privacy behavior, leading to data vulnerability (Martin & Murphy, 2017). Moreover, consumers experience a higher vulnerability due to the optimistic attitude toward information disclosure, expecting gratification, social status, and hedonic benefits (Brough & Martin, 2021; Langenderfer & Shimp, 2001).

Consumers engaged with virtual influencers are a highly vulnerable segment to data breaches with the increased disclosure of personal information, IP addresses, and social media profiles. In the United States, 91 % of people accept online terms of service without reading them, leading to data vulnerability (Guynn, 2020). Hackers can manipulate the algorithm, inducing consumers to respond to false messages and obtain sensitive information, creating financial and psychological damage (Sands et al., 2022).

The celebrity status of virtual influencers overshadows the ability to determine the severity of privacy risk as followers perceive virtual avatars as being harmless compared with actual personalities (Appel et al., 2020). It is, therefore, essential to examine the coping mechanisms that consumers, organizations, and stakeholders can use to minimize data vulnerability (Liyanaarachchi 2021). Such research should elaborate on the differences in vulnerability between consumers and organizations (Hill & Sharma, 2020).

3.2 Cybercrime

Cybercrime is any illegal activity carried out in cyberspace through unauthorized access to data, violating privacy. Cybercrime is the greatest threat to businesses and individuals compared with other criminal activities in the metaverse (Ameen et al., 2021; Dehghanniri & Borrion, 2019). Statista estimates that the global cost of cybercrime will increase rapidly in

the next five years, rising from $8.44 trillion in 2022 to $23.84 trillion by 2027 (Fleck, 2022). However, most organizations still focus on improving online systems without developing a comprehensive privacy strategy. (Liyanaarachchi 2020; Martin et al., 2018).

Cybercriminals exploit consumer vulnerabilities through advanced online tracking systems. The celebrity status of virtual influencers depicts an unquestioned trust (Lou et al., 2022) that leads to accepting fake information, providing higher opportunities for cybercrime (Robinson, 2020). The desire to engage with a virtual influencer in the metaverse as a social need contributes to ignoring the cybercrime threat. Cybercriminals can forge the identity of a virtual influencer and obtain data from a follower through malware (Abroshan et al., 2021; Buck & McDonnell, 2022).

Managing consumer privacy and minimizing cybercrime in the metaverse is vital for the success of virtual influencers, creators/owners, and sponsors. Firms should improve surveillance of fake consumer profiles and track abnormal activity to prevent cybercrime (Bromium, 2019). For example, the data breach of the dating site 'Ashley Madison' led to resignations, divorces, and suicides, as the details of over 37 million members from over 40 countries (Lamont, 2016). Followers' vulnerability to cybercrime will directly damage the brand equity of sponsors of virtual influencers (Kim & Kim, 2021). One in five organizations is affected by malware distributed via social media (Bromium, 2019), and cybercriminals continue to exploit corporate secrets through industrial espionage (Basuchoudhary & Searle, 2019).

Educating consumers on the gravity of sharing information with virtual influencers is crucial for the industry to move forward with assurance. Existing research on privacy has addressed the impact of cybercrime purely on a symmetrical ideology depicting the effects on both parties (organization and consumer). However, we argue that this reciprocal impact is insufficient to determine the effect of privacy on the followers. The intended two-way

communication, which is the usual practice online, is one dimensional as the virtual influencer demonstrates limited privacy risk due to the artificial identity, resulting in an unbalanced impact on data privacy skewed towards the followers and consumers.

Despite the significance of cybercrime, there is limited research examining its impact on consumer vulnerability (De Kimpe et al., 2021). Recent studies elaborate that existing security controls and management policies cannot protect consumers of the metaverse from cybercrime and cyber-attacks (Dwivedi et al. et al., 2022). Thus, we argue that the negligence of followers toward their privacy due to the gratification of following an online avatar can result in victimization.

3.3 Fake profiles

As consumers can determine how they want to be seen or known, personal identity in a digital reality such as the metaverse can be illusionary or, at its extreme, completely fake (Mitrushchenkova, 2023). Consumers can provide fake data in their profiles or accounts or even create fake profiles. They thus can have multiple identities or accounts. While most users provide partially fake data in their user profiles to preserve anonymity and privacy or to provide online representations that are closer to their ideal selves (Belk, 2013), others create fake profiles impersonating fictitious or real persons to spread fake news or access a victim's financial or personal data (Smaili & de Rancourt-Raymond, 2022). Privacy invasions are among the most common and harmful cybercrimes (Ramalingam & Chinnaiah, 2018). For instance, in the second quarter of 2022, the social network platform Facebook had to remove 1.4 billion fake accounts to fight against potentially fraudulent activities (Statista, 2022).

Fake profiles damage user privacy and substantially impact the sustainability of the platform business model and companies that rely on the accuracy of the user data (Krombholz et al., 2012; Nunan & Di Domenico, 2016). These cybercrimes represent key

security and privacy concerns while moving to the metaverse (Di Pietro & Cresci, 2021). Like social media platforms, the metaverse enables trolling and bullying due to the anonymity of fictitious user identities, which conceals potential negative consequences. Consumers in the metaverse may interact with people represented by avatars without knowing if they are real or fake, so they may provide fake data or create fake profiles to rebalance their perceived privacy asymmetry while interacting with virtual influencers. In turn, creating wholly or partially fake identities may represent a critical threat to the metaverse business model as it leads to serious privacy concerns.

4. Empirical Study: Methodology

Given the dearth of studies on the interception between virtual influencers and data privacy, we conducted in-depth interviews with 28 followers of virtual influencers. This qualitative approach, based on the codification of participants' interviews (Gioia et al., 2013), enables the emergence of exploratory insights to assess "how" followers perceive the interaction with influencers and "what" their main concerns are in terms of privacy. We stopped at 28 participants because we reached code saturation.

4.1 Research approach and procedure

To exploit the exploratory power of the qualitative analysis, we selected purposive sampling, maximizing variation to capture solid patterns (Bell et al., 2022). We selected different participants in terms of backgrounds, educational levels, occupations, and ages. Compared to the average number of interviews which sits between 9 and 17 participants (see Hennink & Kaiser, 2022), this heterogeneous sample required a higher sample (28

participants), due to the need to reach code saturation. We interviewed participants from November 2022 to January 2023.

The key research questions were: i) what are your concerns about data privacy when dealing with virtual influencers? ii) how would you compare these concerns to the ones you would have interacting with human influencers? iii) who is responsible for the virtual influencers' behavior?" iv) do you regret sharing your information with virtual influencers in the metaverse v) what your concerns on cybercrime and fake profiles are? Data from the interviews were verified, compared, and triangulated (Yin, 2014).

4.2 Data analysis

Three coders manually validated the coding by measuring the level of agreement using a percentage agreement method. An intercoder agreement was carried out, and the percentage overlap between coders was 85% The three coders discussed the remaining 15% of data and reached an agreement.

We approached interview analysis and data interpretation through a general framework (Yin, 2014). First, we analyzed each interview singularly through a within-case approach (Charmaz, 2011). We analyzed emerging themes through a coding system of three stages (Gioia et al., 2013).

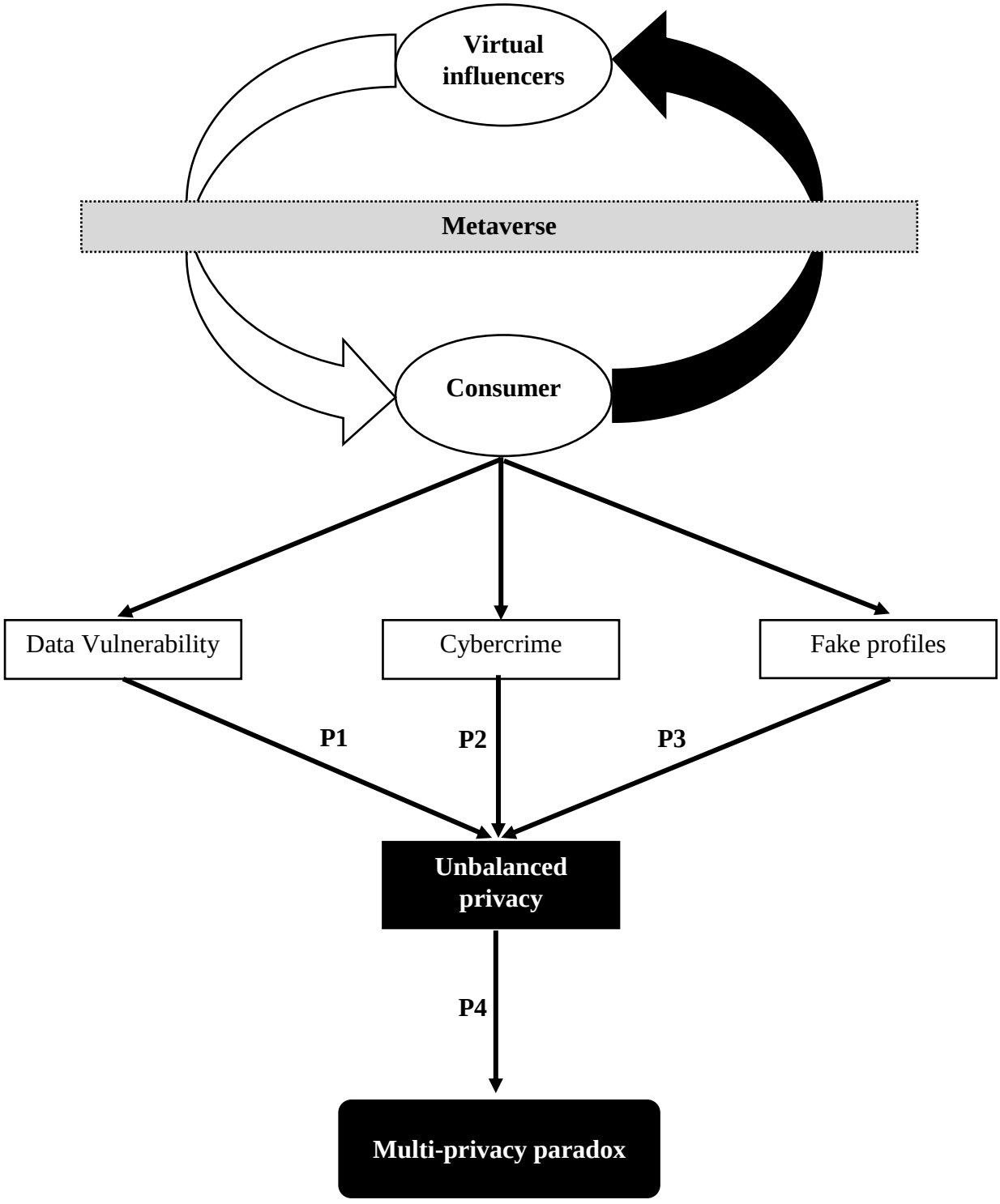
In the first stage, we coded interviews and organized them into a set of 1st-order concepts: *Perceptions toward data privacy when dealing with influencers; Difference between virtual and human influencers in terms of privacy and data vulnerability; Cybercrime issues; Fake identity; Specific responsibilities for influencers' behavior*. In the second stage, we developed a 2nd-order analysis to establish links between data and develop

new concepts: *Data vulnerability, cybercrime, and fake profiles.* In the third stage, we aggregated key themes into newly developed dimensions: *Unbalanced privacy and the extended privacy paradox.* We explored participants' experiences and businesses by considering research questions as lenses through the coding system.

4.2 ***Discussion of findings***

Based on the findings in Figure 1, we develop a conceptual framework and a set of exploratory propositions that identify three sources of consumers unbalanced privacy risks when interacting with virtual influencers (i.e., data vulnerability, cybercrime, fake profiles). Our results also suggest that this unbalanced privacy leads to a multi-privacy paradox, a broader psychological dilemma than the existing one.

Figure 1. Multi-privacy paradox



4.3.1 Data vulnerability

The findings highlight that followers discern a pronounced sense of data vulnerability due to their interactions with virtual influencers. The participants believe their data can be manipulated and used for malicious purposes. Data vulnerability can influence the psychological wellbeing of consumers, and a fear of engaging with online entities due to data misuse (Martin & Murphy, 2017). Also, followers are concerned about the risk of disclosing their personal information mainly due to losing control over data (Ameen et al., 2022; Audrezet et al., 2020). *"Compared to human-to-human interactions, I fear that my dialogues can be misused as no one is responsible. I can't do anything about it and feel I have no protection as it is a one-sided risk" [GP]*. This perceived data vulnerability arises due to the powerlessness that occurs from an unbalance with data privacy where the followers have no control or ownership over data (Echeverri & Salomonson, 2019; Wanjugu et al., 2022). Thinking at their experiences, they are particularly concerned about screenshots: "I feel that they store all my information and take screenshots. *"I am worried that these may be used against me by someone online" [MD]*. Accordingly, they do not feel free to share information as they worry about retaliation. *"Sometimes virtual influencers look very artificial, and I would like to offer critiques to improve them. But I am scared to do so, as anyone can use my data and retaliate with a personal attack" [GC]*. The data concern extends beyond the company behind the virtual influencer, also involving third parties. "There is a lot of curiosity about virtual influencers. This attracts the attention of third parties who might hold that information against me. *I feel vulnerable as they don't have a risk as I do with data" [MP]*. This vulnerability significantly impacts the broader adversaries on consumers' social employment or business relationships (Liyanaarachchi, 2020). This leads to our first proposition:

P1: ***Follower data vulnerability is more pronounced with virtual influencers than with human influencers, leading to unbalanced privacy.***

4.3.2 Cybercrime

The findings show that followers are concerned about being exposed one-dimensionally to cyber criminals due to communicating with an artificial avatar. Engagement with virtual influencers requires sharing information in the metaverse, thus exposing followers to cybercrime risks. Cybercrime is any illegal activity carried out in cyberspace through unauthorized access to data, violating privacy. It is the greatest threat to businesses and individuals compared with other criminal activities in the metaverse (Ameen et al., 2021; Dehghanniri & Borrion, 2019). Cybercriminals can forge the identity of a virtual influencer and obtain data from a follower through malware (Abroshan et al., 2021; Buck & McDonnell, 2022). In such a context, followers tend to feel that cybercrimes could occur while interacting with virtual influencers. Cybercriminals target actual people rather than virtual avatars, forming an unbalanced privacy risk: *"I am worried about my data as they remain in the metaverse. Hackers will target humans as virtual influencers are not real"* [SL]. *"I almost got trapped clicking a web link that tried to access my bank accounts. I don't know how I connected, but I am sure it was through a conversation with a virtual character"* [NW]. *"I feel hackers track my online experience. I am exposed 100% as Miquela types have no risk of cybercrime as they don't exist in real life"*. [GP].

In summary, the interviewees are concerned about the one-sided risk with cybercriminals while dealing with virtual characters. They are worried about the lack of assurance of their data and privacy. They believe cybercriminals target them due to financial resources and possession of wealth being real people compared with virtual characters. Building on the preceding discussion, the second proposition is that:

P2: ***Cybercriminals specifically target followers of virtual influencers on their powerlessness in data sharing, contributing to an unbalanced privacy situation.***

4.3.3 Fake profiles

Virtual influencers are often ideal models, almost heroes. Therefore, consumers might want to create a perfect (i.e., fake) *persona* to minimize the risk of exposure to privacy due to unbalanced risk. Further, followers can be reluctant to expose their true identity and to be part of any fake news. In 2019, Lil Miquela, a CGI influencer, publicized fake information about experiencing a sexual assault during a ride share in Los Angeles. This dissemination prompted concerns of potential harm and distress among her followers (Block & Lovegrove, 2021). Therefore, stringent legislative measures are necessary to regulate fake profiles and communications by virtual influencers to mitigate deceptive practices in the context of sponsored products and the promotion of fictitious experiences (Lou et al., 2022). Artificial intelligence systems can interchange the faces or voices of any individual, including celebrities, and create fake communications using virtual influencers (Campbell et al., 2022).

Consequently, substantial user-generated content exhibits conspicuous fabrication: "Virtual influencers operate in an artificial realm. I would not share my true persona, and I am sure other followers would behave like me" [NT]. *"I was interacting with a follower of a virtual influencer. However, I realized it was a fake profile"* [SS].

To summarize, while interviewees enjoy watching the content produced by virtual influencers, they are concerned about having meaningful touchpoints during the live stream. They are worried about fake profiles influencing their privacy due to the unbalanced risk. Moreover, participants create fake profiles to protect their identity: *"I enjoy watching virtual influencers, but I do not interact with them with my real profile due to the risk of identity theft*

and fraud" [DF]. This is evident as exposing their genuine identity online renders consumers susceptible to personal hazards such as blackmail, identity theft, and harassment, prompting them to conceal their true identity (Mustak et al., 2023).

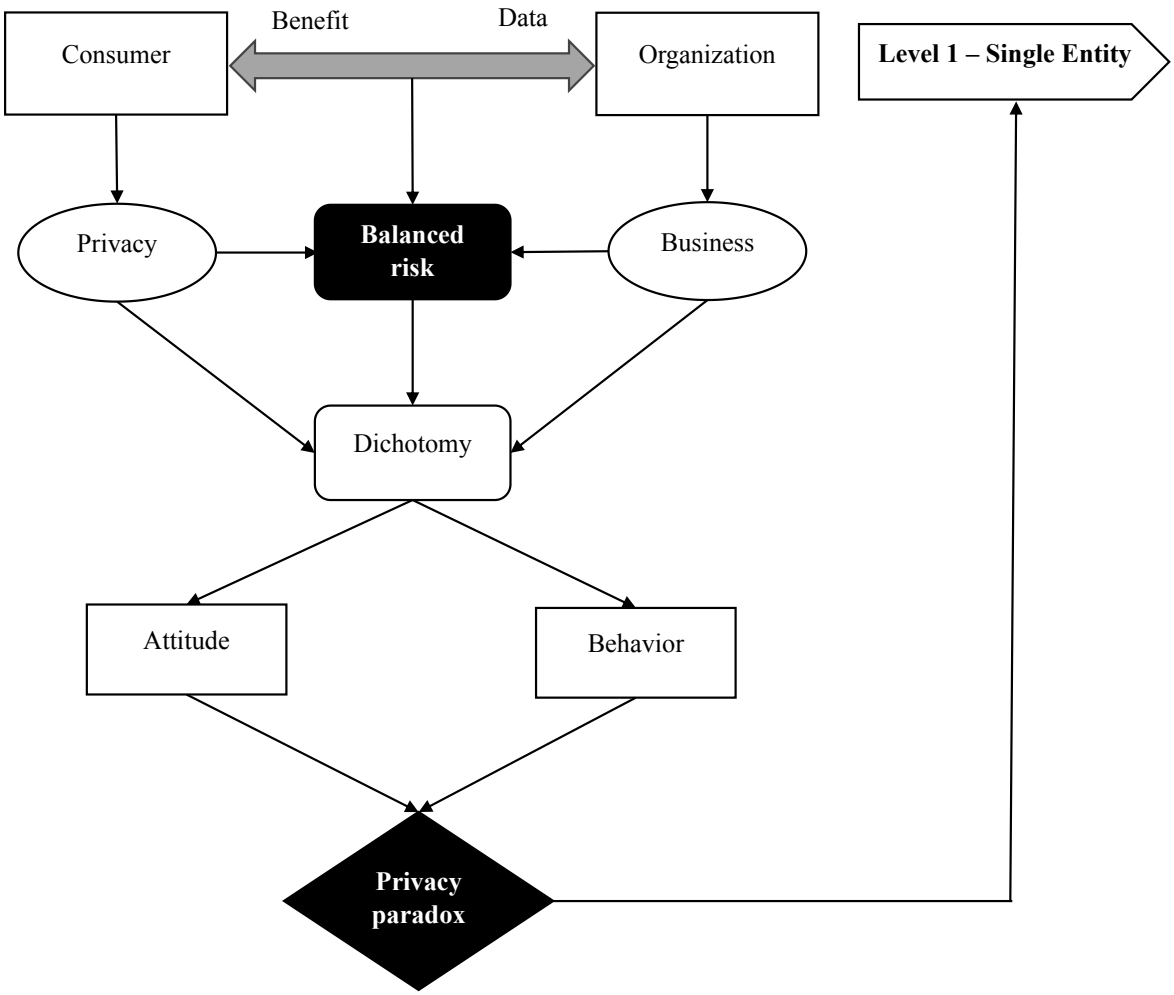
This leads to our third proposition:

P3: ***The followers create fake profiles to protect their identity due to the unbalanced privacy risk associated with virtual influencers,***

4.3.4 Unbalanced privacy

Sharing customer data with external entities can enhance service quality and business returns. However, inter-organizational data sharing poses challenges despite potential advantages, exposing companies to uncontrollable privacy risks (Upadhyay, 2020). This can lead to unbalanced privacy, where data is used beyond its original purpose, increasing risks beyond customer awareness (Schneider et al., 2017). Customers prefer balanced privacy with transparency and control, rather than companies having sole authority over data use (Dwivedi et al., 2023). Consumers are reluctant to share data with dominant, manipulative companies, underscoring the importance of equal privacy risk (Ameen et al., 2022). The lack of flexibility in managing sophisticated systems like biometrics also causes unbalanced privacy risks for consumers (Liyanaarachchi et al., 2023). Organizations' complete data control renders consumers vulnerable to an unbalanced exchange, potentially causing privacy violations (Tan & Saraniemi, 2023). A similar vulnerability arises with virtual influencers. Consumers face greater privacy risks than virtual influencers, influenced by a one-sided risk perspective. This unbalance leads to negative perceptions and reduced willingness to share data.

Figure 2. Privacy paradox



The privacy paradox stems from the reciprocal relationship between consumers and firms involving mutual benefits. Consumers share data to gain benefits while taking on privacy risks. This direct exchange, the first level in Figure 2, underlies the paradox. The current privacy paradox occurs at level 1, where a consumer's privacy risk ties directly to a single entity. The consumer and entity have a reciprocal risk-reward relationship. The consumer gets a benefit for providing data, while the firm sees a business return based on the risk level. However, virtual influencers lack real entity status, removing reciprocity. This leaves consumers with an unbalanced privacy risk.

Interviewees are concerned that their relationship with virtual influencers is uneven in terms of privacy. Specifically, they feel weaker compared to their counterpart. This negative feeling decreases the trustworthiness of the interactions and the fear of privacy violation. The interviews suggest that data vulnerability experienced due to being the human element in the relationship leads to unbalanced privacy.

Cybercriminals target followers due to this singular exposure as followers share sensitive personal information compared to virtual characters with no data. Moreover, fake profiles that depict virtual influencers can obtain access to personal data and devices, prompting followers to create an ideal self or forge their true identity, resulting in unbalanced privacy. The current study proposes three primary sources of data vulnerability, cybercrime, and fake profiles leading to unbalanced privacy.

We define unbalanced privacy as:

"The privacy risk originates from engaging with a virtual influencer resulting in one-dimensional exposure due to an uneven power relationship."

Also, the interviews suggest that the followers experience a privacy paradox when dealing with virtual influencers due to unbalanced privacy. Thus, while they welcome this new technology, they prefer human influencers because they worry about unbalanced privacy. Third parties' utilization and sharing of data obtained through virtual influencers as intermediaries constitute an unmanageable threat for followers, as privacy breaches remain concealed and beyond control.

"*When interacting with virtual influencers, I feel I am alone with unknown forces in the metaverse. Sometimes, I regret posting certain ideas, and I know companies are keen to know consumer preferences just for advertising purposes*" [BY]. "*There is a huge unbalance here. I offer my data, and I get pre-coded information from a robot in exchange which has no risk*

[FK]. The consumers acknowledge the hedonic benefits of sharing information but are simultaneously worried about the privacy risk. *It is fun dealing with a virtual influencer, but I fear later about the whole thing as everyone sees my data. Who knows whether a hacker has already targeted me"* [GP]. *"I enjoy following Miquela as I believe in equal rights but do not trust them. I don't know who controls them. I always doubt sharing information, as I don't want to be a victim of a data breach*" [SA].

The consumers indicate a dilemma on the credibility of virtual influencers primarily due to the hidden agendas of business and commercial interest in using personal information: *"I welcome this technological advancement, but I am skeptical here. I know they promote companies as I get a lot of personal ads through social media"* [KP]. *"How do they use my data, and who are these people? It is better to know who is responsible for my privacy"* [SD].

The evidence suggests that the followers experience a deeper level of privacy paradox due to the anonymity of the sources that control the virtual influencers. This is outside the existing privacy paradox doctrine, which denotes the discrepancy in attitude and behavior of sharing information with a single party, such as a retailer, bank, etc. We argue that the privacy paradox shifts beyond this reciprocal relationship toward a multi-stakeholder level with the additional privacy threat beyond a single organization. The data brokering industry, estimated to generate US$ 200 billion annually in revenue, significantly influences consumer privacy (Duxfield & Mitchell, 2019). Data brokering is a substantial threat to consumer privacy as the impact of a privacy violation is not immediately identifiable by a consumer. In 2018, hackers collected over 244,000 credit card details from a major airline carrier and sold the data on the Dark Web, earning an estimated US$12.2 million (KPMG, 2019). Moreover, the Dark Web, functioning as a black market for data, is estimated to contribute to over US$ 1.5 trillion annually (Wilson, 2019). Transactions on the Dark Web occur inconspicuously, without direct evidence of the exchanges.

From the interviews' evidence, the study proposes that:

P4: ***Due to the unbalanced privacy perceptions, consumers experience a multi-privacy paradox with the anonymity of information users.***

5. Implications, limitations, and further research agenda

5.1. Theoretical implications

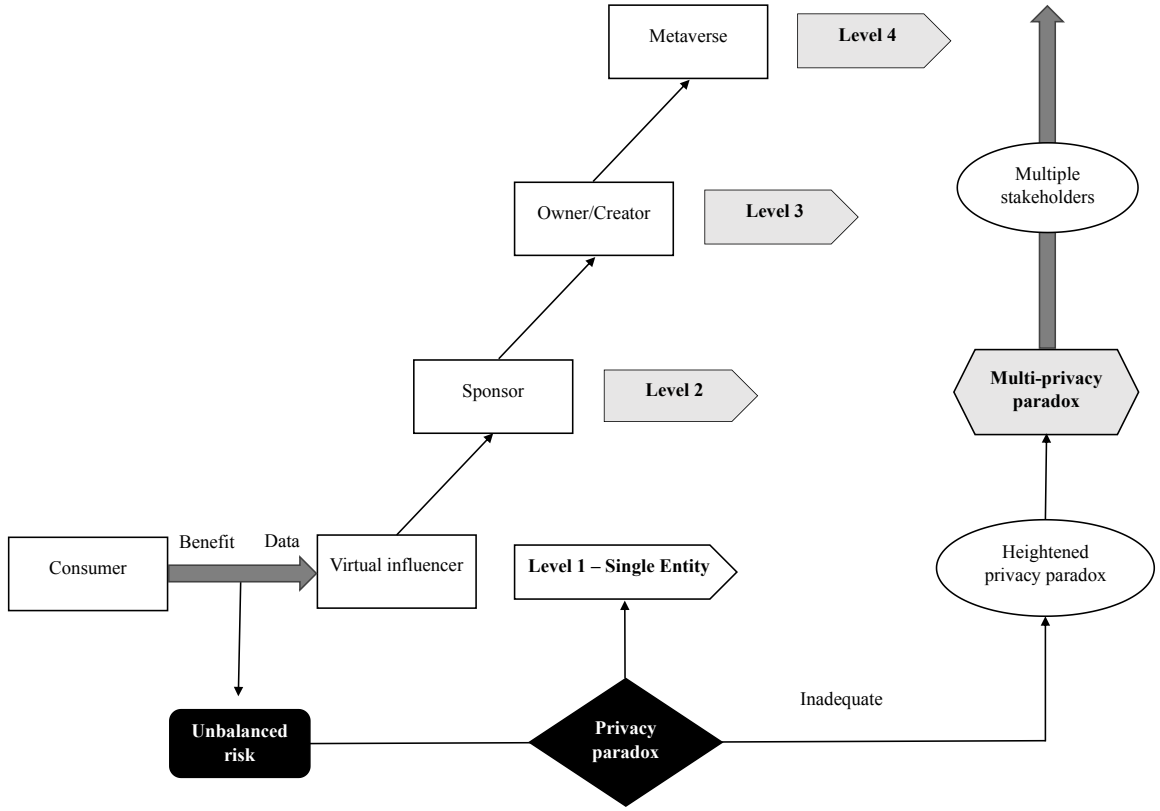
This study offers two distinct theoretical contributions. Firstly, we introduce the concept of "unbalanced privacy risk," which presents a unique privacy scenario for consumers engaging with virtual influencers. This novel concept emerges at the intersection of data vulnerability, cybercrime, and fake profiles. The prominence of virtual influencers has recently garnered significant attention, particularly in connection with the metaverse (Hollensen & Dwivedi, 2023). The concept of unbalanced privacy responds to scholars' calls to investigate potential privacy risks associated with virtual influencers and the metaverse, a topic that has remained relatively unexplored, prompting appeals for empirical research in this domain (Appel et al., 2020; Barrera & Shah, 2023; Dwivedi et al., 2022).

Unbalanced privacy contributes to the literature as a distinctive privacy challenge faced by followers of virtual influencers arising from privacy risks inherent in interactions involving artificial personas. Further, unbalanced privacy illuminates how consumers experience a sense of powerlessness in controlling their data within systems driven by non-human characters empowered by artificial intelligence.

Second, this study contributes significantly to the existing literature by introducing a multi-privacy paradox, elucidated through the lens of unbalanced privacy risk. Our principal theoretical advancement, the multi-privacy paradox, holds wide-ranging relevance to the privacy literature. In contrast, the unbalanced privacy risk represents a distinct phenomenon faced by followers of virtual influencers, which extends to their interactions with any non-

human system or platform characterized by asymmetric disclosure risk. The multi-privacy paradox is a pioneering extension that addresses scholarly calls (Barth & De Jong, 2017; Colnago et al., 2023; Dienlin et al., 2023; Gerber et al., 2018; Gotsch & Schögel, 2021; Kokolakis, 2017; Liyanaarachchi, 2021; Martin & Murphy, 2017) on the literature gap of privacy paradox by synthesizing consumers, organizations and sectors to create a comprehensive global ecosystem.

Figure 3. Application of multi-privacy paradox



This paper argues that the current privacy paradox, focused on a single entity, cannot explain unbalanced risk. The actual consumer privacy situation expands to other entities at further levels. With Lil Miquela, sponsors like Prada, Samsung, and Calvin Klein pay for services at certain times. Therefore, risk spreads to another level involving stakeholders like the owner or original creator for legal and regulatory purposes. In 2021, Dapper Labs

acquired Brud, Lil Miquela's owner (Keely, 2001). Trevor McFedries and Sara Decou founded Brud, a tech company that creates virtual avatars (Lawn, 2018).

The involvement of various stakeholders at different risk levels heightens the privacy paradox. Consumers cannot determine the full privacy risk as it goes beyond one entity. To address this complexity, we introduce the multi-privacy paradox in Figure 3. While applied here specifically, the multi-privacy paradox can be used for any unbalanced, multi-entity privacy situation across industries, sectors, or ecosystems.

The multi-privacy paradox will provide the foundation for future studies, providing a solution for the normative and behavioral ideologies debate. More specifically, it strengthens the behavior-dominant understanding of the paradox. Also, the paper provides a universally applicable definition of the paradox, manifesting a broader appeal to manage privacy with assurance and consistent strategy. The multi-privacy paradox will provide a new dimension to managing future challenges of the paradox, especially with the metaverse and immersive technology.

We define the multi-privacy paradox as:

*"**A state that arises through unbalanced privacy where consumers experience a more profound mismatch between privacy concerns and self-disclosure due to the anonymity of the users of information."***

5.2. Managerial implications

This paper provides three actionable implications for practice. First, organizations should understand the broader application of the multi-privacy paradox on stakeholders and consider it a core element in designing the digital strategy. This will enable organizations to build a privacy-conscious culture and a decision-making process adhering to a privacy protection

strategy. This strategic stance aligns with Gotsch & Schögel's (2021) recommendation for an organizational-level approach to address the privacy paradox. Drawing from Liyanaarachchi (2020), organizations can proactively detect and address privacy breaches in real-time. For instance, in identity theft cases, the interconnected stakeholder network can rapidly trace the origin of the data breach, including unauthorized access or hacker involvement. Employing traceability mechanisms with a designated path and data violation trail ensures swift and accurate breach detection. This transparency aligns seamlessly with the dynamics of the privacy paradox, reassuring customers of the organization's capability to rectify privacy violations. Consequently, this minimizes the disparity between the privacy paradox context and customer perceptions, strengthening their faith in the organization's adeptness in safeguarding privacy.

Second, by introducing a proactive strategy for managers to identify and address the stakeholder privacy depicted through virtual influencers, our framework enables a manager to understand the role of each stakeholder in safeguarding consumer data. For example, a sponsor will determine the nature and level of information that should be collected from consumers, ensuring better privacy control. Cybercriminals can generate fake information that can have a detrimental impact on the image of brands and organizations. Further, deep fake-based deceptions result in a loss of brand equity, stakeholder credibility, and negative financial implications (Mustak et al., 2023). It is paramount to address the responsibility of virtual influencers demarcating the boundary between the owners/creators and sponsors. Many countries, including the United States and India, have already regulated this practice to include stringent disclosure requirements on the legal responsibility of avatars (Franke et al., 2022).

Third, the paper recommends the development of a matrix structure integrating sponsors and owners/creators of virtual influencers. The proposed structure will provide a

cohesive platform to integrate the digital and marketing teams into a single unit to manage privacy. The specialized unit should design proactive measures, big data, digital security, and tracking systems to recognize and block cybercriminals and fake profiles. Creators have used Lil Miquela to raise awareness for various causes that can be controversial due to radical political, social, and sexual considerations (Arsenyan & Mirowska, 2021). For instance, Calvin Klein issued an apology following accusations that their campaign featuring model Bella Hadid and virtual influencer Lil Miquela was employing provocative sexual appeals (Jarvis, 2019).

5.3. Limitations and future research agenda

This article provides a framework with a rich research agenda (see Table 1).

Table 1. Multi-privacy paradox: An agenda for future research

Focal research area	Research questions
Consumer attitude and behavior	• How do data vulnerability, cybercrimes, and the creation of fake profiles differently impact consumers' unbalanced privacy perceptions? • What are the psychological mechanisms leading to unbalanced privacy? • How do consumer characteristics (e.g., consumer experience of the metaverse, technology anxiety) act as boundary conditions that reduce or favor the perception of privacy risks?
Consumers cultural differences	• Can culture shape the multi-privacy paradox? • What is the influence of data privacy regulation in the multi-privacy paradox?

Virtual influencers characteristics	• How can virtual influencers from different sectors and industries enhance or reduce the multi-privacy paradox? • How do virtual influencers' appearance and anthropomorphic traits influence the multi-privacy paradox?

First, building on existing literature with an exploratory qualitative design, this paper proposes four initial conceptual propositions subject to refinement and empirical testing. Our framework identifies data vulnerability, cybercrime, and fake profiles as key sources of consumers' unbalanced privacy perceptions. Future studies could experimentally assess these factors' impact and how they may affect privacy perceptions. Testing boundary conditions like consumer characteristics (e.g. metaverse experience, tech anxiety) could enrich the framework. As this research is conceptual and exploratory, findings have limited generalizability. Examining unbalanced privacy across customer segments could enable tailored privacy strategies.

Second, different cultures, values, and regulations lead to varied privacy attitudes across countries (Oghaz et al., 2020). We encourage examining our propositions and the multi-privacy paradox impact in diverse country settings. Despite regulations like GDPR, CCPA, and APP, businesses often need more data protection. Enforcing these regulations remains rare owing to limited consumer data ownership awareness, underscoring the need for reform. Our framework addresses data management power unbalances as a foundation for improving policies and corporate accountability, ultimately restoring consumer data rights.

Third, virtual influencers are used across sectors (Barrera & Shah, 2023). We invite scholars to explore our framework's impacts across fashion, entertainment, etc. Influencers' features (human vs. robot, gender, emotions) should also be investigated further as marketing research stresses understanding anthropomorphic characteristics digitally (Blut et al., 2021).

6. Conclusion

Amid the rise of virtual influencers within the metaverse, our research highlights the significant potential for engagement and entertainment while accentuating the pressing data privacy concerns that arise. Our study presents a comprehensive conceptual framework that illuminates the multifaceted privacy risks inherent in this evolving landscape. By shedding light on the intricate privacy panorama encompassing virtual influencers, we provide practical insights valuable to organizations and stakeholders. Our study offers a timely and relevant contribution to the dynamic realm of the metaverse, where virtual influencers assume a growing role. By comprehensively exploring the multi-privacy paradox, we aim to stimulate further research and discussions regarding the ethical ramifications of interactions with virtual influencers. As technology continues shaping our digital interactions, protecting collective privacy remains crucial, empowering individuals to engage securely with virtual influencers.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, *9*, 44928-44949.

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

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2018). Privacy and Human Behavior in the Information Age. *The Cambridge Handbook of Consumer Privacy*, 184.

Acquisti, A., Adjerid, I., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., ... & Wilson, S. (2023). Nudges (and Deceptive Patterns) for Privacy: Six Years Later. In *The Routledge Handbook of Privacy and Social Media* (pp. 257-269). Routledge.

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.

Adorjan, M., & Ricciardelli, R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. *Canadian Review of Sociology/Revue canadienne de sociologie*, *56*(1), 8-29. https://onlinelibrary.wiley.com/doi/pdf/10.1111/cars.12227

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Ahn, R. J., Cho, S. Y., & Sunny Tsai, W. (2022). Demystifying Computer-Generated Imagery (CGI) Influencers: The Effect of Perceived Anthropomorphism and Social Presence on Brand Outcomes. *Journal of interactive advertising*, 1-9.

Alashoor, T., Keil, M., Smith, H. J., & McConnell, A. R. (2022). Too Tired and in Too Good of a Mood to Worry About Privacy: Explaining the Privacy Paradox Through the Lens of Effort Level in Information Processing. *Information Systems Research*, Forthcoming.

Ameen, N., Hosany, S., & Paul, J. (2022). The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty. *Computers in Human Behavior*, *126*, 106976.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure : A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531.

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, *48*(1), 79-95.

Arsenyan, J., & Mirowska, A. (2021). Almost human? A comparative case study on the social media presence of virtual influencers. *International Journal of Human-Computer Studies*, *155*, 102694.

Audrezet, A., de Kerviler, G., & Moulard, J. G. (2020). Authenticity under threat: When social media influencers need to go beyond self-presentation. Journal of Business Research, *117*, 557-569.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28.

Bandara, R., Fernando, M., & Akter, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. *Procedia Computer Science*, *121*, 562-567. https://doi.org/10.1016/j.procs.2017.11.074

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*, 101947.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).

Barrera, K. G., & Shah, D. (2023). Marketing in the Metaverse: Conceptual understanding, framework, and research agenda. *Journal of Business Research*, *155*, 113420.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, *41*, 55-69.

Basuchoudhary, A., & Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security*, *87*, 101591.

Belk, R. W. (2013). Extended self in a digital world. *Journal of consumer research*, *40*(3), 477-500.Belk, R., Humayun, M., & Brouard, M. (2022). Money, possessions, and

ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *Journal of Business Research, 153*, 198-205.
Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods*. Oxford University Press.
Block, E., & Lovegrove, R. (2021). Discordant storytelling, 'honest fakery,' identity peddling: How uncanny CGI characters are jamming public relations and influencer practices. *Public Relations Inquiry*, *10*(3), 265–293.
Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, *49*, 632-658.
Bromium. (2019). *Cybercriminals earning over $3B annually exploiting social platforms*. Retrieved 16.01.2023 from https://www.globenewswire.com/en/news-release/2019/02/26/1742251/0/en/Cybercriminals-earning-over-3B-annually-exploiting-social-platforms.html
Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108-110.
Brown, D. (2020). Retrieved 11.01.2023 from https://eu.usatoday.com/story/tech/2020/01/21/grindr-tinder-privacy-how-keep-dating-apps-selling-your-data/4479534002/
Boyd, D. E., & Koles, B. (2019). Virtual reality and its impact on B2B marketing: A value-in-use perspective. *Journal of Business Research, 100*, 590-598.
Buck, L., & McDonnell, R. (2022). Security and Privacy in the Metaverse: The Threat of the Digital Human. Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality, April 29 - May 5, 2022, New Orleans, LA, US.
Campbell, C., Plangger, K., Sands, S., & Kietzmann, J. (2022). Preparing for an era of deepfakes and AI-generated ads: A framework for understanding responses to manipulated advertising. *Journal of Advertising, 51*(1), 22-38.
Charmaz, K. (2011). Grounded theory methods in social justice research. *Strategies of qualitative inquiry*, *4*, 291-336.
Chan, Y. E., & Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. Journal of the Association for Information Systems, *6*(6), 7.
Cheng, X., Zhang, S., Fu, S., Liu, W., Guan, C., Mou, J., . . . Huang, C. (2022). Exploring the metaverse in the digital economy: an overview and research framework. *Journal of Electronic Business & Digital Economics*(ahead-of-print).
Cloarec, J., Meyer- Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, *39*(3), 647-661.
Colnago, J., Cranor, L. F., & Acquisti, A. (2023). Is there a reverse privacy paradox? an exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies*, *1*, 455-476.
De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, 1-13.
De Veirman, M., Cauberghe, V., & Hudders, L. (2017). Marketing through Instagram influencers: the impact of number of followers and product divergence on brand attitude. *International journal of advertising*, *36*(5), 798-828.
Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*. https://doi.org/10.1177/1477370819850943

Duxfield, F. & Mitchell, S. (2019). *Personal data of thousands of Australians sold for just $US60*, Retrieved 20.08.2023 from https://www.abc.net.au/news/2019-05-31/online-privacy-personal-data-purchased-for-$us60-warning-experts/11157092

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

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in- depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), 285-297.

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, *25*(5), 1043-1064.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., . . . Cheung, C. M. (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.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., . . . Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994.

Dwivedi, Y. K., Hughes, L., Wang, Y., Alalwan, A. A., Ahn, S. J. G., Balakrishnan, J., . . . Dutot, V. (2022). Metaverse marketing: How the metaverse will shape the future of consumer research and practice. *Psychology & Marketing*, *40*(4), 750-776.

Dwivedi, Y. K., Balakrishnan, J., Das, R., & Dutot, V. (2023). Resistance to innovation: A dynamic apability model based enquiry into retailers' resistance to blockchain adaptation. Journal of Business Research, 157, 113632.

Echeverri, P., & Salomonson, N. (2019). Consumer vulnerability during mobility service interactions: causes, forms and coping. *Journal of Marketing Management*, *35*(3-4), 364-389.

Feliciano-Cestero, M. M., Ameen, N., Kotabe, M., Paul, J., & Signoret, M. (2023). Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization. *Journal of Business Research*, *157*, 113546.

Fleck, A. (2022). *Cybercrime Expected To Skyrocket in Coming Years*. Retrieved 08.01.2023 from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: the privacy paradox revisited. *In Quantum Interaction*: 6th International Symposium, QI 2012, Paris, France, June 27-29, 2012, Revised Selected Papers 6 (pp. 148-159). Springer Berlin Heidelberg.

Franke, C., Groeppel-Klein, A., & Müller, K. (2022). Consumers' Responses to Virtual Influencers as Advertising Endorsers: Novel and Effective or Uncanny and Deceiving? *Journal of Advertising*, 1-17.

Gartner. (2022). *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the metaverse by 2026.* Retrieved 05.01.2023 from https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.

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.
Gotsch, M. L., & Schögel, M. (2021). Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly*, 1-34.
Gursoy, D., Malodia, S., & Dhir, A. (2022). The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions. *Journal of Hospitality Marketing & Management*, 1-8.
Guynn, J. (2020). *What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy*. Retrieved 15.01.2023 from https://eu.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/
Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*, *292*, 114523.
Hilken, T., Keeling, D. I., Chylinski, M., de Ruyter, K., Golf Papez, M., Heller, J., . . . Alimamy, S. (2022). Disrupting marketing realities: A research agenda for investigating the psychological mechanisms of next- generation experiences with reality- enhancing technologies. *Psychology & Marketing*, *39*(8), 1660-1671.
Hill, R. P., & Sharma, E. (2020). Consumer vulnerability. *Journal of Consumer Psychology*, *30*(3), 551-570.
Hollensen, S., & Dwivedi, Y. K. (2023). Metaverse marketing: How the metaverse will shape the future of consumer research and practice. *Psychology & Marketing*, *40*(4), 750-776.
Hollensen, S., Kotler, P., & Opresnik, M. O. (2022). Metaverse–the new marketing universe. *Journal of Business Strategy* (ahead-of-print).
Keely, A (2021). Dapper Labs acquires Lil Miquela creator Brud to build a unit focused on DAOs, Retrieved 10.01.2024 from https://www.theblock.co/linked/119431/dapper-labs-acquires-lil-miquela-creator-brud-to-build-a-unit-focused-on-daos
Jarvis, J. (2019). *Calvin Klein apologises for 'queerbaiting' advert showing kiss between Bella Hadid and fictional woman Lil Miquela*. Retrieved 12.01.2023 from https://www.standard.co.uk/news/world/calvin-klein-apologises-for-queerbaiting-advert-showing-kiss-between-bella-hadid-and-fictional-woman-lil-miquela-kiss-a4145461.html
Jorstad, E. (2000). The privacy paradox. William Mitchell Law Rev., 27 (3), 1503
Jung, B. R., Choi, K.-S., & Lee, C. S. (2022). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(2), 4-24.
Kelly, S. M. (2021). Facebook Changes Its Company Name to Meta. *CNN Business. Retrieved 12.01.2023 from www. cnn. com/2021/10/28/tech/facebook-mark-zuckerberg-keynote-announcements/index. Html*
Kim, D. Y., & Kim, H.-Y. (2021). Trust me, trust me not: A nuanced view of influencer marketing on social media. *Journal of Business Research*, *134*, 223-232.
Kliestik, T., Novak, A., & Lăzăroiu, G. (2022). Live shopping in the metaverse: Visual and spatial analytics, cognitive artificial intelligence techniques and algorithms, and immersive digital simulations. *Linguistic and Philosophical Investigations*, *21*, 187-202.
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

KPMG (2019), *Global Banking Fraud Survey*, Retrieved 12.08.2023 from https://kpmg.com/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html

Krombholz, K., Merkl, D., & Weippl, E. (2012). Fake identities in social media: A case study on the sustainability of the Facebook business model. *Journal of Service Science Research*, *4*(2), 175-212.

Lamont, T. (2016). *Life after the Ashley Madison affair*. Retrieved 07.01.2023 from https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763-783.

Lawn, W (2021). The Making of a Virtual Influencer, Retrieved 10.01.2024 from https://containermagazine.co.uk/the-making-of-a-virtual-influencer/

Leung, F. F., Gu, F. F., & Palmatier, R. W. (2022). Online influencer marketing. *Journal of the Academy of Marketing Science*, *50*(2), 226-251.

Liyanaarachchi, G. (2020). Online privacy as an integral component of strategy: allaying customer fears and building loyalty. *Journal of Business Strategy*, *41*(5), 47-56.

Liyanaarachchi, G. (2021). Managing privacy paradox through national culture: Reshaping online retailing strategy, *Journal of Retailing and Consumer Services*, *60*, 102500.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Online banking and privacy: redesigning sales strategy through social exchange. *The International Journal of Bank Marketing*, *39*(6), 955-983.

Liyanaarachchi, G., Viglia, G., & Kurtaliqi, F. (2023). Privacy in hospitality: managing biometric and biographic data with immersive technology. International Journal of Contemporary Hospitality Management. Ahead-of-print, https://doi.org/10.1108/IJCHM-06-2023-0861

Lou, C., Kiew, S. T. J., Chen, T., Lee, T. Y. M., Ong, J. E. C., & Phua, Z. (2022). Authentically Fake? How Consumers Respond to the Influence of Virtual Influencers. *Journal of Advertising*, 1-18.

Martin, K. D., Borah, A., & Palmatier, R. W. (2018). *Research: A Strong Privacy Policy Can Save Your Company Millions*. Retrieved 10.07.2020 from https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155.

Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e- commerce: A multilevel meta- analysis. *Psychology & Marketing*, *38*(10), 1779-1798.

McKenna, B., & Chughtai, H. (2020). Resistance and sexuality in virtual worlds: An LGBT perspective. *Computers in Human Behavior*, *105*, 106199.

Miao, F., Kozlenkova, I. V., Wang, H., Xie, T., & Palmatier, R. W. (2022). An emerging theory of avatar marketing. *Journal of Marketing*, *86*(1), 67-90.

Mitrushchenkova, A. N. (2023). Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Review*, *9*(4), 793-817.

Miyake, E. (2023). I am a virtual girl from Tokyo: Virtual influencers, digital-orientalism and the (Im) materiality of race and gender, *Journal of Consumer Culture*, *23*(1), 209-228.

Mourtzis, D., Panopoulos, N., Angelopoulos, J., Wang, B., & Wang, L. (2022). Human centric platforms for personalized value creation in metaverse. *Journal of Manufacturing Systems*, *65*, 653-659.
Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, *154*, 113368.
Nunan, D. (2021). Collection: Privacy and research ethics. *International Journal of Market Research*, *63*(3), 271-274.
Nunan, D., & Di Domenico, M. (2016). Exploring reidentification risk: Is anonymisation a promise we can keep*?*. *International Journal of Market Research*, *58*(1), 19-34.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.
Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N. P., & Rad, F. F. (2020). User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts. *Journal of Business Research*, *112*, 531-540
Park, S.-M., & Kim, Y.-G. (2022). A Metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, *10*, 4209-4251.
Rajaobelina, L., Prom Tep, S., Arcand, M., & Ricard, L. (2021). Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychology & Marketing*, *38*(12), 2339-2356.
Ramalingam, D., & Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165-177.
Rauschnabel, P. A., He, J., & Ro, Y. K. (2018). Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research*, *92*, 374-384.
Robinson, B. (2020). Towards an ontology and ethics of virtual influencers. *Australasian Journal of Information Systems*, *24*, 1-8.
Sands, S., Ferraro, C., Demsar, V., & Chandler, G. (2022). False idols: Unpacking the opportunities and challenges of falsity in the context of virtual influencers. *Business Horizons*, *65* (6), 777-788.
Shen, B., Tan, W., Guo, J., Zhao, L., & Qin, P. (2021). How to promote user purchase in metaverse? A systematic literature review on consumer behavior research and virtual commerce application design. *Applied Sciences*, *11*(23), 11087.
Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, 34(3), 593-603.
Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. *Journal of Financial Crime* (ahead-of-print).
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review, *MIS Quarterly*, 989-1015.
Solove, D. (2021), The Myth of the Privacy Paradox. George *Washington Law Review*, *89*, 1.
Statista. (2022). Global number of fake accounts taken action on by Facebook from 4th quarter 2017 to 2nd quarter 2022. Retrieved 06.01.2023 from https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/
Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. *Journal of the Academy of Marketing Science*, *51*(4), 914-939.

Thomas, V. L., & Fowler, K. (2021). Close encounters of the AI kind: Use of AI influencers as Brand endorsers. *Journal of Advertising*, *50*(1), 11-25.

Time. (2018). *The 25 Most Influential People on the Internet*. https://time.com/5324130/most-influential-internet/

Tussyadiah, I., Li, S., & Miller, G. (2019). Privacy protection in tourism: Where we are and where we should be heading for. In *Information and Communication Technologies in Tourism 2019* (pp. 278-290). Springer.

Ulaga, W., Kleinaltenkamp, M., Kashyap, V., & Eggert, A. (2021). Advancing marketing theory and practice: Guidelines for crafting research propositions. *AMS Review*, 1-12.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, pplications, and opportunities. *International Journal of Information Management*, *54*, 102120.

Viglia, G., Pera, R., Dyussembayeva, S., Mifsud, M., & Hollebeek, L. D. (2023). Engagement and value cocreation within a multi-stakeholder service ecosystem. *Journal of Business Research*, *157*, 113584.

Wanjugu, S., Moulard, J. G., & Sinha, M. (2022). The paradoxical role of relationship quality on consumer privacy: Its effects on relinquishing and safeguarding information. *Journal of Consumer Behaviour*, *21*(5), 1203-1218.

Wilson, E. (2019). Disrupting dark web supply chains to protect precious data. *Computer Fraud & Security*, *2019* (4), 6-9.

Yin, R. K. (2014). *Case study research : Design and methods* (5 edition. ed.). SAGE.

Zhang, F., Pan, Z., & Lu, Y. (2023). AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management*, *60*(2), 103736.