Privacy in hospitality: managing biometric and biographic data with immersive technology

Gajendra Liyanaarachchi, Giampaolo Viglia, Fidan Kurtaliqi

Privacy in hospitality: Managing biometric and biographic data with immersive technology

Gajendra Liyanaarachchi, Giampaolo Viglia, Fidan Kurtaliqi

Abstract

Purpose – This study investigates the implications, risks, and challenges of data privacy due to the use of immersive technology in the hospitality industry.

Design/methodology/approach – We adopt a mixed-method approach. Study 1 is a focus group. We then provide external and ecological validity with a field experiment conducted with 139 hotel clients at a three-star continental European hotel.

Findings – Collecting biometric data results in unbalanced privacy compared to biographic data, as it diminishes individuals' control over their data and grants organizations absolute power. This unbalanced privacy directly influences consumers' willingness to disclose information, affecting their choice of hotels and access to services.

Originality/value – This study introduces unbalanced privacy as a unique state due to sharing biometric data. We propose a novel doctrine, the uncontrollable privacy paradox, which is a shift from the privacy paradox. The uncontrollable privacy paradox addresses the unbalanced privacy envisaged through consumer powerlessness in data management. This research addresses the literature gap on the privacy paradox by offering a broader perspective, including business, industry, and mixed reality considerations.

Practical implications – Hotels should redesign their strategies to accommodate heightened privacy risks with biometric data. This can be obtained by introducing systems that foster customer confidence in data usage and facilitate customers' willingness to disclose biometrics through immersive technology or biographic data.

Keywords

Privacy paradox, unbalanced privacy, immersive technology, biometric data, hospitality, metaverse

1. Introduction

The service industry is at the forefront of using industry 4.0 technologies. Immersive technologies enable businesses and customers to co-create value throughout life (Flavián *et al.,* 2019). Service providers such as hotels, airlines, and travel agents can design a unique digital identity for each customer, providing a personalized experience. Delta Airlines has improved operational efficiency using biometric data by reducing boarding time with enhanced customer satisfaction (Chang, 2022). Using biometric data with immersive technology will be the future of the hospitality industry, as ninety percent of its retail executives foresee the dominance of immersive technology, bridging the digital and physical experience (Accenture, 2022).

Immersive technology-driven service experiences from hotels are about to connect 125 billion objects in 2030 (Kruyne, 2022). Hotels are already using immersive technology check-in systems. For example, Hoteza, an interactive guest-oriented platform, utilizes biometrics for mobile check-in with over 500 global hotels, including Hilton, Radisson, Wyndham, Kempinski, IHG, and Accor hotels (Amper, 2023). However, despite technological advancement and process improvement benefits, biometric data such as face recognition increases data privacy risk. The Information Commissioner's Office (ICO) in the U.K. fined US-based company Clearview A.I. for £7.5m for collecting images of people for commercial purposes without consent (Milmo, 2022). Further, Mary Kay and Ulta Beauty face legal action for collecting biometric data through face recognition apps violating privacy (Nash, 2021).

Companies that use biometric data lack clarity in protecting consumer privacy (Morosan, 2019). Hackers can manipulate immersive systems, penetrate the algorithm, and use customer biometrics, violating privacy (Tussyadiah, 2020). E.U. General Data Protection Regulation (GDPR) and local legislation such as the California Consumer Privacy Act (CCPA) require transparent policies for data collection and use (Tikkinen-Piri *et al.*, 2018). Biometric data differs from biographic data due to reliance on unique biological or behavioral traits specific to each individual, which are beyond the person's control after disclosure. In contrast, biographical data consists of factual information and details about an individual, constituting descriptive data disclosed and controlled by the individual.

Scholars agree that despite the growth in immersive technologies, there is a lacuna in research on privacy in the collection, sharing, and use of biometric information (Knani *et al.*, 2022; Lehto *et al.*, 2023). Biometric data is more sensitive than biographic data, as it is irrevocable and cannot be changed or overwritten. A user cannot control biometric information once disclosed to a system through immersive technology, as data is permanent. As such, there is a lack of investigation and evaluation of data protection approaches (Ioannou *et al*., 2020; Tussyadiah, 2020).

We argue that consumers experience unbalanced privacy due to the lack of flexibility in managing biometric data compared with biographic data. The existing privacy protection methods used in managing biographic data are inadequate to protect biometric data. Customers can change their biographic privacy preferences, a feature unavailable with immersive technology. This unbalanced power situation lingers in the hospitality industry, where cybercriminals can trace customers through biometric data. As a result, sharing biometrics leads to a privacy paradox. A privacy paradox originates from the contradiction between an individual's attitude and the behavior on disclosure of information.

Firms in the hospitality industry use rigid, immersive technology and pressure consumers to disclose sensitive data, regardless of the associated risks (Lehto *et al.,* 2023). Biometric data, such as fingerprints and facial recognition, are highly personal and unique identifiers. The collection of such data in hospitality raises concerns about the level of invasion of individuals' privacy (Cowan *et al.,* 2021). We portray that the privacy paradox will increase with a heightened awareness of privacy violations due to the irrevocable nature of biometric data compared with biographic data. For example, biometric data disclosure to visit Turkey may be obsolete if the consumer does not intend to revisit the same destination. However, the data will remain in the metaverse, creating continuous privacy risks irrespective of the use of further services.

Through a mixed-method study (refer to Figure 1), we introduce a novel doctrine, the "uncontrollable privacy paradox," highlighting the unbalanced privacy implications of disclosing biometric data. We provide a unique and significant addition to the literature on a distinct aspect: the elevated level of risk inherent in using biometric data with immersive technology, in contrast to biographic data. We summarize and systematically compare our findings with the core contributions of the literature in Table 1 to comprehend our distinctive contribution. Our findings contend that the conventional privacy paradox is inadequate in comprehending the impact of such disclosure, mainly due to individuals' limited autonomy in managing biometric data. This study provides practical recommendations for effectively managing biometric data and fostering consumer willingness to disclose personal information in the hospitality industry.

Authors	Context	Research design	Main findings
Morosan (2019)	Profile creation and biometric information disclosure via facial recognition systems in hotels with immersive technology.	A survey with 421 US consumers who stayed in hotels. The study employed confirmatory factor analysis using structural equation modeling.	The consumers consider a trade-off between the cost and benefit of biometric data disclosure.
Moon *et al*. (2022)	The perception of hotel guests on the effectiveness of privacy management to determine the disclosure decisions and hotel choice.	A survey with 492 South Korean consumers on their hotel experience. The study employed confirmatory factor analysis using structural equation modeling.	The privacy policy, privacy assurance, and employee information access controls are key factors shaping consumer trust building an effective privacy management system.
Lehto *et al*. (2023)	Compare the privacy attitude toward using biometrics data in hotels before and after receiving information about the risks and benefits of disclosure.	Split plot scenario-based experimental design with 579 US respondents containing multiple experiments. each with a unique subset of factors	Consumers are less willing to share biometric information through immersive technology once they have considerable knowledge of the privacy risks.
Femenia-Serra *et al.* (2022)	Privacy concerns in smart tourism and the influence of collecting biometric data to enhance the tourist experience	A mixed-methods approach with 34 semi-structured interviews and a survey of 1019 travelers from the UK and Spain.	Identifies key privacy concerns of biometric data as technology risks, past data misuse experiences, and unawareness of data management practices.
Flavián *et al.* (2019)	The integration of Virtual-Reality, Augmented-Reality, and Mixed-Reality technologies to identify a hybrid experience with physical and virtual world.	Conceptual paper	The "EPI Cube" taxonomy is proposed, combining embodiment, presence, and interactivity perspectives to classify technologies supporting customers in current and new experiences.

Cowan *et al.* (2021)	Examine the privacy concerns for sharing biometric facial data interacting with augmented reality face filter apps.	Study 1: Survey with 251 participants in the UK. Study 2: Experimental study of 165 Snapchat users in the UK.	Privacy concerns increase with the use of augmented reality face filter apps due to fear of manipulation of personal data.
Boo and Chua (2022)	Examine the attitude of hotel guests towards using facial recognition technology.	A survey with 371 hotel guests in Singapore using structural equation modeling	The hotel guests engaged in calculative cognitive processes, assessing the positives and negatives of a facial recognition check-in system,
This study	We examine the heightened privacy risk associated with utilizing biometric data vs. biographic data in hospitality.	A mixed-method approach with an exploratory focus group and a subsequent field experiment in a three-star continental European hotel with 139 clients.	We introduce the concept of unbalanced privacy, resulting in biometric data collection. We propose the uncontrollable privacy paradox as a novel doctrine, addressing consumer powerlessness in data management with immersive technology in hospitality.

Table 1. Key literature contributions. Source: Authors own creation.

2. Literature review

2.1 Privacy Paradox

The privacy paradox illustrates the dichotomy between attitude and behavior regarding disclosing personal information (Acquisti *et al.,* 2023; Barnes, 2006). Consumers continue to disclose data despite protecting their privacy, leading to inconsistent online behavior (Liyanaarachchi, 2021). This paradox exists due to the perceived trade-off between the expected benefits and the perceived risk of disclosure (Masur, 2023). In the context of the metaverse, where extensive consumer data collection occurs, the privacy paradox becomes more prevalent (Hilken *et al.,* 2022). As the value of consumer data increases over time, organizations and consumers must adapt their privacy behaviors to ensure data protection.

The privacy paradox persists because data remains online indefinitely, even after its initial use, creating a dilemma for consumers in assessing privacy risks. The privacy paradox, commonly examined within the consumer context, presents higher challenges for organizations with immersive technology in navigating privacy violations (Gotsch and Schögel, 2021). Moreover, the privacy paradox escalates as consumers have no ownership or the ability to control data after being collected through immersive technology within the metaverse. Despite extensive research on the privacy paradox, we need more consensus regarding its application and scope (Kokolakis, 2017; Masur, 2023).

Previous studies have primarily focused on the consumer-firm relationship, overlooking broader conditions such as the advancement of technology (2021Cowan et al., 2021; Zhang *et al*., 2023). Scholars have tried to establish a universally applicable definition of privacy using various theories (Acquisti *et al.,* 2023; Masur, 2023), but with limited success. Research is needed to explore the privacy paradox in various settings involving socio-technical systems, aiming to comprehensively capture this phenomenon's full scope and implications

(Dienlin *et al*., 2023 ; Kokolakis, 2017). The privacy paradox remains an unresolved issue despite significant research. To bridge the research gap and comprehensively explore the impact of the privacy paradox, we conducted a mixed-method approach encompassing various platforms, technologies, organizational settings, and industry contexts.

2.2 Metaverse and immersive technology

Metaverse became popular after Facebook changed its name to Meta in 2021, altered the logo, rebranded, and repositioned its business. Meta is investing $10 billion with similar investments from Google, Microsoft, Nvidia, and Qualcomm (Tucci, 2023). The Metaverse economy could reach $5 trillion by 2030, transforming business and social life and creating a new world order (McKinsey and Company, 2022). Metaverse denotes a significant impact on hospitality as consumers can link past, present, and future experiences with immersive technology. Moreover, the experiences can be permanently stored, reused, or sold, providing more significant benefits than a physical experience (Dwivedi *et al*., 2023). The transition between the virtual and physical world enables consumers to consider a hybrid mode as a new experience and a benchmark for the industry.

The consumers can achieve their aspirations, such as enjoying luxuries beyond their financial capacity. For example, enjoy experiences such as staying in a super luxury resort, visiting the Gobi Desert, or challenging adventures such as climbing the Himalayas. With a National Geographic V.R. subscription, a consumer can use a V.R. headset or Google Cardboard on a smartphone and kayak through icebergs in Antarctica (Barrell, 2021). The hospitality industry is at the forefront of collecting vast amounts of biometric data that require stringent data security measures (Knani *et al*., 2022). Therefore, organizations must introduce radical processes and reengineer the systems to accommodate disruptions and transformation

(Buhalis *et al*., 2023). Consumers must disclose biometric data to access services, where data is stored permanently with immersive technology (Cowan *et al.,* 2021).

Furthermore, using facial recognition for customer identification before arriving at a hotel amplifies the risk of privacy violations, as it allows hackers to monitor customer intentions, locations, and service usage, thereby enabling fraudulent activities and identity theft. Organizations can design privacy strategies to protect biometric data from affecting consumer well-being, which is pivotal for industry growth. However, despite the hospitality industry's size and significance, there needs to be more research on managing the risk of biometric data (De Keyser *et al.,* 2021). Firms should prioritize consumer privacy over the commercial interest of using biometrics-based service decisions and denounce decisions purely on efficiency improvements (Lehto *et al.,* 2023).

3. Method

This study employs a mixed-method approach, integrating qualitative and quantitative investigations to enhance the overall quality and robustness of the study (Creswell and Clark, 2017). Combining qualitative and quantitative methods in information technology-driven research offers notable benefits, facilitating a comprehensive and in-depth understanding of the phenomenon under investigation (Venkatesh *et al*., 2013). To achieve this objective, an exploratory sequential design mixed-methods approach is adopted, wherein qualitative findings from a focus group in Study 1 reinforce a subsequent quantitative investigation in Study 2 (Teddlie and Tashakkori, 2011). Study 1, consisting of a focus group, examines the impact of privacy by comparing biometric and biographic data. The subsequent experimental Study 2 validates the findings and further strengthens the privacy paradox's proposed theoretical extension (see Figure 1).

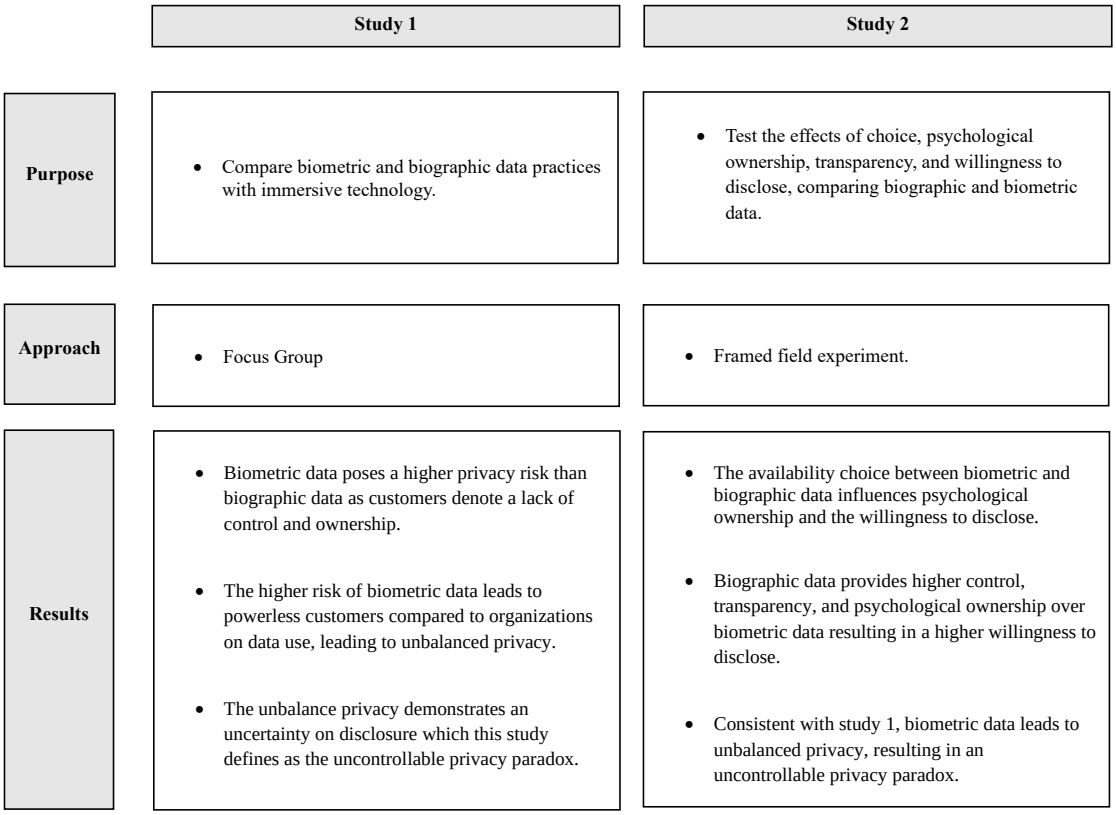

Figure 1. Purpose, approach, and results of Studies 1 and 2. Source: Authors own creation.

3.1. Study 1: Qualitative research on customer perception of biographic vs. biometric data collection

Qualitative research aids in investigating emergent phenomena by integrating theory and reality and yielding compelling insights (Bouncken *et al.*, 2021). Consistent with the literature review, the goal of Study 1 is to investigate how hotel consumers perceive these two data-gathering methods (biographic and biometric) and their privacy concerns. We take a qualitative approach, relying on the focus group method (Fern, 2001) to obtain exploratory data. The focus-group technique is a qualitative strategy that focuses on small, non-probability samples with a range of age, gender, education, socioeconomic status, and other relevant variables (Ritchie *et al.*, 2013). The focus group provided us with the opportunity to examine group interaction.

3.1.1 Data collection, study design, and procedure

Online focus groups with a shared discussion format developed by the research team are a validated research protocol (Cyr, 2019). The research team developed a coherent protocol after developing generic research questions based on the objectives. In particular, the moderator must adhere to a topic guide to stimulate a conversation. In this case, the goal was to understand how we can manage our private data when interacting with hotels and what are the subjective views of biometric vs. biographic data.

Twelve relevant subjects (i.e., hotel customers) were found through referrals (Aiello *et al.*, 2020). Recruiters were given stringent referral parameters to guarantee a broad set of participants. The heterogeneous participants include people of various origins, educational levels, occupations, and ages. We used a stratified sampling technique with people familiar with hotel bookings (i.e., have already booked a room and stayed in a hotel at least two times). The participants' initials are specified at the end of each quote below.

Before the focus group began, the moderator explained the procedure and the purpose of the session. The focus group lasted 2 hours, starting with exploring the main factors around data privacy in the hotel context and the perception of customers' control of such data depending on the used technology (biometric vs. biographic data collection). The session was transcribed into a word processing package to allow NVivo content analysis (Bazeley and Jackson, 2013). The transcripts were independently read, analyzed, and compared, leading to interrater reliability measured with Cohen's kappa coefficient (0.83). Using a categorization process suggested by Brocato *et al.* (2012), recurring themes in the data were identified by listing items that reflected similar characteristics. We first open-coded all the data, which provided the basis for developing the coding framework. As we progressed through the data analysis, our codes became more specific.

3.1.2 Results

Overall, the qualitative findings reveal that consumers consider biometric data collection a riskier privacy threat than biographic information.

Hotel consumers are concerned about what data will be stored and for how long: “I find it very intrusive when at the check-in they encourage me to leave my fingerprint or facial image to access their services more easily. My data will be stored by them forever” (M.N.). Similarly, the participants are worried about losing control over the data they are giving away. Indeed, as one participant reported, “Despite I do not want to give away my data, I often do it because it is practical to access hotel services more easily. However, I regret it ex-post because, in several data breaches, the customer has no control”(L.C.).

On the contrary, the findings show that hotel customers are less concerned with biographic data. “I am in better control with biographic data. I can log in to my account and amend or remove my private information. Even if I don't do it, that possibility gives me peace of mind” (K.G.); “Compared to biometric data, I prefer biographic data as I have a better control of what is going on” (M.H.). Moreover, hotel customers realize that immersive technologies increase their tendency to give away sensitive data they would not normally share: “With immersive technologies, I feel I am living a dream. Sharing sensitive data does not seem to be a big issue. However, when I realize they now have a digital copy of every inch of my face, I find it scary” (T.T.).

Importantly, participants discuss the behavioral action they take from interacting with such technologies: “I get frustrated when I cannot delete my data. They make it harder to do it. Therefore, unless extremely necessary, like at the airport security borders, I tend to avoid services that are uniquely based on biometric information” (V.V.); similarly, “Hotel stays should remain private unless we want to share what we are doing. Giving away my biometric

data would mean having that data stored forever on a server somewhere. I would rather switch hotel" (L.T.); additionally, "If they offer me the option to either go with biometric or biographic data, I am fine. It is my choice and my risk" (F.P.). Thus, consumers are aware of the unbalanced privacy risk with biometric data; however, they are occasionally ready to take that risk provided they are offered a choice.

3.1.3 Discussion

The exploratory approach offers new insights that can enrich our theoretical understanding. A conceptual framework (see Figure 2) and two propositions highlight the main evidence visually. Participants are concerned that disclosing biometric data leads to vulnerability and powerlessness due to a lack of choice in managing their data. Specifically, they feel subordinated compared to the companies that collect data. This indicates a lack of confidence, credibility, and fear of sharing information due to privacy violations. Further, they are concerned about the lack of choice in determining the disclosure level due to collecting biometric data. As data collection through immersive technology happens in real-time, there is no time to think or provide a counterargument on privacy as they are compelled to experience the services.

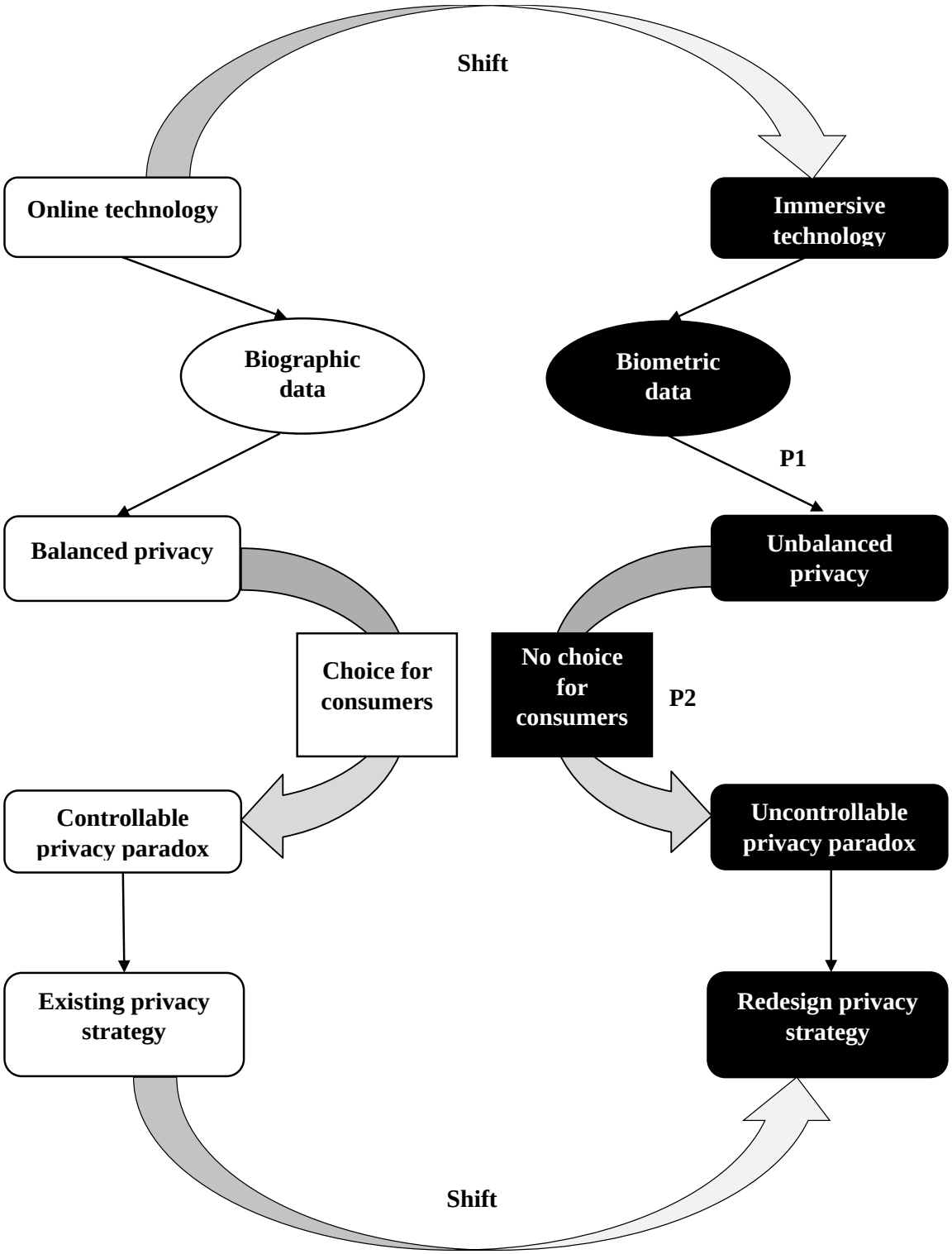

Figure 2. Redesigning privacy strategies transitioning from biographic to biometric data management. Source: Authors own creation.

The findings suggest that consumers experience unbalanced privacy due to the lack of flexibility in managing biometric data compared with biographic data. The existing privacy protection methods used in managing biographic data are inadequate to protect biometric data. We identify this powerlessness as "unbalanced privacy," where one party (the company that collects data) has the absolute power to decide on the use of data over the original owner (consumer) who discloses the data. This unbalanced power situation lingers in the hospitality industry, where cybercriminals can trace customers through biometric data. This leads to our first proposition:

P1: Consumers experience unbalanced privacy due to organizations obtaining biometric data compared with biographic data.

Participants denote a higher regret after disclosing biometric data, including fingerprints and facial images, which are highly sensitive and unique. Also, there is a change of attitude between the time of disclosure and after the experience. The findings suggest that the gratification of obtaining a novel experience undermines privacy risk, leading to later remorse for such disclosure, depicting a privacy paradox. We argue that the lack of autonomy to manage biometric data disclosure results in a more significant privacy paradox than the biographic data situation. We propose that the privacy paradox will increase due to the irrevocable nature of biometric data driven by unbalanced privacy compared with biographic data.

Further, with biographic data, a consumer can change the disclosure preference and control the privacy paradox. We argue that the privacy paradox shifts beyond the personal control state to an uncontrollable level with biometric data. Thus, building on this premise, we propose a novel concept, the "uncontrollable privacy paradox," adding a new theoretical

paradigm. With unbalanced privacy risk due to biometric data, consumers experience a higher privacy paradox that we identify as uncontrollable. This leads to our second proposition:

P2: The lack of choice to manage biometric data due to unbalanced privacy leads to an uncontrollable privacy paradox.

3.2 Study 2

In line with Study 1 and the proposed Figure 2, Study 2 aims to focus on the impact of biometric data privacy and test the effects of choice, psychological ownership, transparency, and willingness to disclose in a framed field experiment. The difference between a framed field experiment and a natural field experiment is that in framed field experiments, participants are aware of being the subjects of an experimental study (Viglia *et al*., 2021).

3.2.1 Choice, psychological ownership, and transparency

Consumer choice directly influences the privacy paradox (Acquisti *et al.,* 2023). The privacy choice depends on the relative risk and benefit of disclosure. Within the hotel industry, data privacy and information disclosure on digital platforms significantly impact consumer choice (D'Acunto *et al*., 2021). Biographic data makes the choice more specific due to the control associated with and after disclosure. Hence, the privacy paradox is controllable as a consumer has autonomy on the level of disclosure. We identify this state as the balanced privacy paradox. In contrast, with biometric data, the consumers have no choice on the level of disclosure. Thus, the company that collects biometric data will possess absolute authority, undermining the

existing basis of the privacy paradox. Consumers experience an unbalanced privacy paradox due to a lack of disclosure choices.

We focus on testing the impact of the choice between biographic and biometric data.

Thus, we hypothesize that:

H1. *The availability of the choice to use biographic or biometric data to access hotel services positively influences the willingness to disclose.*

Psychological ownership is a “state in which individuals feel as though the target of ownership (material or immaterial in nature) or a piece of it is 'theirs” (i.e., It is MINE!)" (Pierce *et al.*, 2001, p. 299). For example, Yao *et al*. (2023) showed that tourism engagement predicts psychological ownership, influencing citizen behavior. Indeed, controlling own data facilitates a sense of psychological ownership (Morewedge *et al.*, 2021). Psychological ownership refers to individuals' sense of control, responsibility, and attachment to personal data in data privacy.

The availability of data choice will facilitate a sense of control in decision-making, thus increasing the feeling of psychological ownership. Eighty-one percent of customers consider passwords for online payments due to greater security and control than biometric alternatives (Paysafe, 2019). Psychological ownership is prominent concerning biographic data owing to personal control, a factor absent in the case of biometric data. The significance of control is evident with the following quote from study 1: “If they offer me the option to either go with biometric or biographic data, I am fine. It is my choice and my risk” (F.P.). With biographic data, consumers can change the scope of information revealed, during and after the process, depicting psychological ownership.

We hypothesize that:

H2. *Control available with biographic data over biometric data positively influences psychological ownership.*

Martin and Murphy (2017) emphasize that consumers have a positive tendency to share data with service providers supporting data ownership. Psychological ownership reflects how consumers value their data, resulting in a positive attitude toward disclosure (Barth *et al.,* 2022). The ability to manage own data and determine the level of disclosure facilitates favorable opinions about the organization. Research by Kokolakis (2017) demonstrates that customers who exert greater control over their shared data have higher confidence in service providers. Therefore, psychological ownership significantly influences individuals' willingness to disclose data.

We hypothesize that:

H3. *Psychological ownership positively influences willingness to disclose.*

Transparency in data use by allowing customers to amend data will enhance the willingness to disclose information in hospitality (Lei *et al.,* 2022). The inability to delete or modify biometric data is a critical factor that can significantly impact willingness to disclose compared to biographic data. With biographic data, consumer willingness is high due to the transparency associated with data usage. Transparency in data management is critical to induce customers to disclose information (Barth *et al.,* 2022). Lack of transparency leads to an unbalance in

privacy, as sharing biometric data with third parties occurs without obtaining the customer's explicit consent. The inability to change own data after disclosure can negatively influence psychological ownership (Morewedge *et al.*, 2021). Thus, a lack of transparency in data usage will have a negative effect.

Therefore, we predict:

H4. *The level of transparency moderates the impact of offering a choice on psychological ownership.*

Figure 3 presents the overall model to be tested in the field experiment.

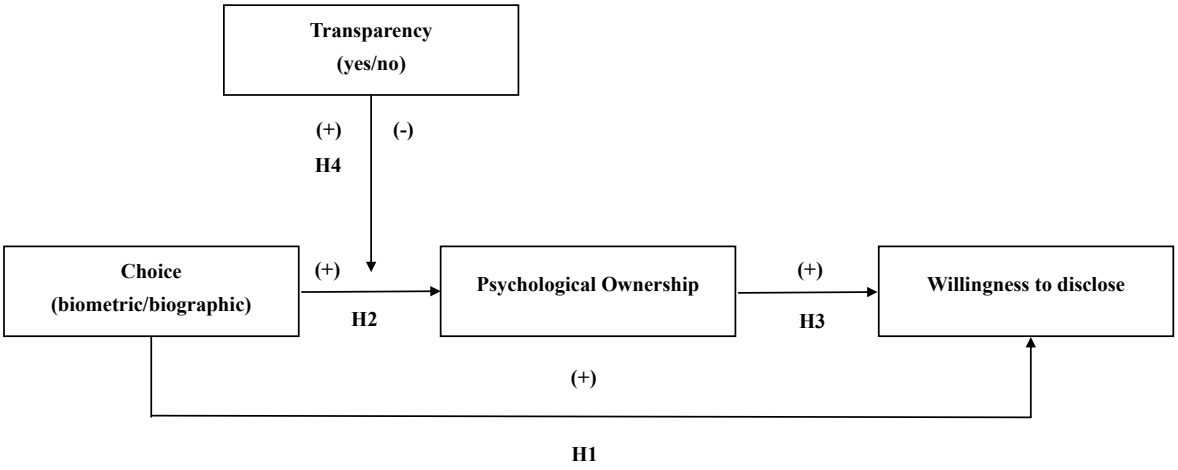

Figure 3. Model of Study 2. Source: Authors own creation.

3.2.2 Data collection, study design, and procedure

The field experiment examines the combined impact of choosing between biometric and biographic data on willingness to disclose. Building on qualitative evidence, this study explores the significance of the hotel's data usage transparency and the role of psychological ownership

that explains the connection between offering data choice and willingness to disclose. We conducted the field study at a three-star family business hotel in continental Europe in April 2023 with real hotel clients under higher involvement than a lab study (Viglia and Dolnicar, 2020). One hundred thirty-nine random clients participated in the field study.

The guests were randomly allocated across four conditions (i.e., choice: we give a choice to customers to use biometric data to access services to the hotel or use biographic; no choice: we inform customers that hotel services are available after giving biometric data; transparency: we inform customers that they can no longer modify or delete their biometric data; no transparency: we do not inform customers that they can no longer change or delete their biometric data). The four conditions are synthetized in Figure 4. The average age of the clients was 36, and 43% of customers were women. Our dependent variable was consumer willingness to disclose, measured through 7 levels (1 strongly disagree; 7 strongly agree).

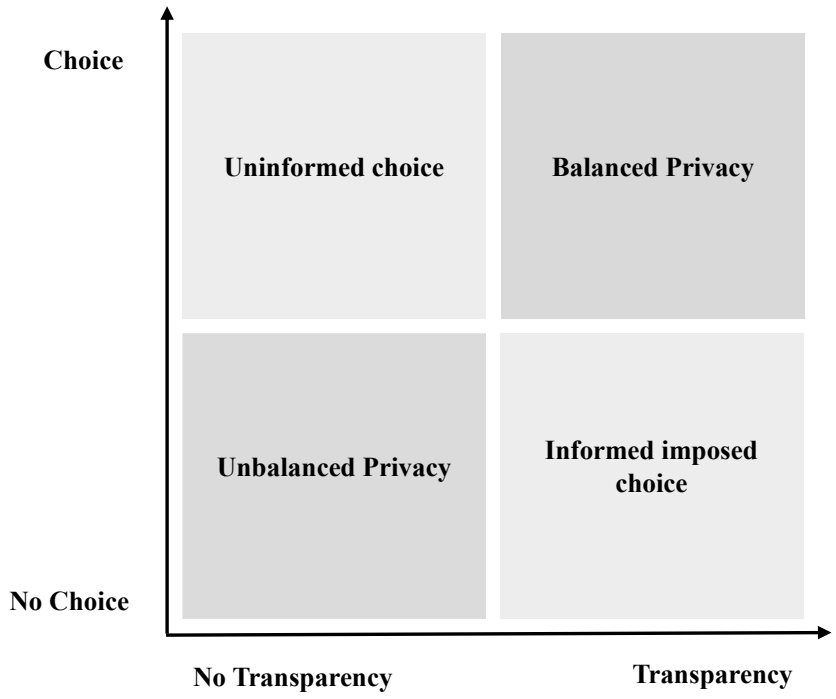

Figure 4. Conditions of the field experiment. Source: Authors own creation

3.2.3 Results

Study 2 tested a moderated mediation model using the PROCESS macro (Model 7) by Hayes (2022), with biometric/biographic as the independent variable, the level of transparency as the moderator of choice on willingness to disclose, and psychological ownership as the mediator. As established in prior experimental research, we used a dummy variable coding approach to include experimental treatments as the independent variables in the model (Bagozzi, 1977). We coded one dummy variable for message framing (0 no choice vs. 1 choice for biographic or biometric) and another for transparency level (0 no vs. 1 yes).

Regarding H1, we predicted that choosing biographic or biometrics to access hotel services would positively influence the customer's willingness to disclose information. Results show that this direct effect is significant (β=0.812, SE=0.227, t = 3.56, p=0.005), validating H1. Psychological ownership also positively affects the willingness to disclose (β=0.297, SE=0.075, t = 3.95, p=0.001), in support of H3. Taking the outcome variable psychological ownership (mediator), the interaction between choice and transparency on psychological ownership shows a significant positive effect (β=1.88, SE=0.498, t = 3.77, p=0.002). Only age was positively substantial among the control variables, with older guests feeling higher psychological ownership when offered a choice (p = 0.0255).

3.2.4 Discussion

Study 2 investigates the impact of choice and transparency on customers' willingness to disclose information and psychological ownership. Both choice and psychological ownership

significantly affect customers' willingness to disclose, supporting H1 and H3, respectively. The finding that giving customers the choice of using biographic or biometrics to access hotel services positively influences their willingness to disclose is consistent with previous research on the value of giving customers control over their information (Dienlin *et al.,* 2023 ; Lei *et al., 2022)*. This result implies that customers demonstrate a higher willingness to disclose information when they have the power to decide on managing data.

Consistent with previous research, psychological ownership significantly affects the willingness to disclose (Morewedge *et al.,* 2021). Further, the finding highlights the importance of cultivating a sense of psychological ownership in customers by giving them control over their data. The study also investigated the impact of transparency on psychological ownership, and the results show that transparency significantly affects psychological ownership, supporting H4. This finding is consistent with prior research that indicates transparency is perceived as a favorable characteristic, fostering a greater inclination to disclose information (Lei *et al.,* 2022). Lack of transparency can reduce or eliminate a sense of psychological ownership. Although the interaction between choice and transparency was significant, we did not find support for the H2 effect of choice on psychological ownership. This finding is inconsistent with previous research that suggests greater choice leads to higher psychological ownership (Morewedge *et al.,* 2021).

Consistent with Study 1, customers understand the difference in privacy risk between biographic and biometric data. Customers prefer balanced privacy to unbalanced privacy, which provides better choice, transparency, and psychological ownership. It is evident from the findings of both studies that biometric data denote a higher risk due to unbalanced privacy beyond the traditional privacy paradox situation.

4. Conclusions, implications, limitations, and future research

4.1 Conclusions

This paper highlights the significant privacy concerns with collecting biometric data compared with biographic data in the hospitality industry. We introduce the "uncontrollable privacy paradox" as a novel concept, highlighting the unique privacy challenges with immersive technology. The study provides practical recommendations for efficiently managing biometric data collection in hospitality to ensure consumer willingness to disclose information. The conceptual framework introduced in this paper extends its applicability to industries beyond hospitality, such as banking, advertising, and entertainment, all of which rely significantly on immersive technology.

4.2. Theoretical implications

We offer two clear theoretical contributions. First, we present unbalanced privacy risk as a unique privacy situation for consumers due to the disclosure of biometric data. The use of immersive technology in the metaverse and its impact on data privacy is at the forefront of current research (Dwivedi *et al.*, 2021; Femenia-Serra *et al.*, 2022; Koohang *et al.*, 2023). Scholars have emphasized the need to introduce comprehensive strategies to manage data privacy and protect consumer interest (Barrera and Shah, 2023; Dwivedi *et al.*, 2023; Tussyadiah, 2020). Addressing the concern of scholars, we identified a unique privacy condition depicting an unbalanced privacy risk on the powerless of consumers in sharing biometric data. Hence, identifying the inequality of the bargaining power of consumers, we introduce a unique dimension to privacy literature.

Second, this study contributes to the existing literature by defining the privacy paradox through the lens of unbalanced privacy, shedding light on the challenges of using immersive technology in the metaverse. This study offers a novel doctrine, the uncontrollable privacy

paradox (see Figure 2), acknowledging the unbalanced privacy of consumers in sharing biometric data in the metaverse. In doing so, we address the call of scholars (Barth *et al.,* 2022; Gotsch and Schögel, 2021; Kokolakis, 2017; Masur, 2023), offering a holistic understanding of the privacy paradox. The demarcation of privacy paradox from biographic to biometric data strengthens the privacy paradox literature and its position in the dynamic metaverse environment. Unbalanced privacy and the uncontrollable privacy paradox will provide a new theoretical lens to understand consumer vulnerability and the resulting impact on decision-making. Further, the proposed definition that addresses the future data privacy issues of using immersive technology in the metaverse provides a new direction for future research.

We define the uncontrollable privacy paradox as follows:

"The uncontrollable privacy paradox emerges due to unbalanced privacy, which confers unfair advantages to firms with absolute power to manage customer data".

4.3. Managerial implications

This paper also provides three actionable implications for practice. Firstly, organizations should redesign the privacy strategy by adhering to the relevant national and international legislature, such as GDPR and CCPA, regarding the use of biometric data. The city of Portland, Oregon, US, introduced legislation prohibiting public-facing businesses like stores, restaurants, and hotels from using facial recognition technology (Metz, 2020). Consumers remain unaware of the risks associated with disclosing biometric data. For instance, in the UK, a survey found that 60% of people were unaware that their biometric data can be shared with other companies (Garcia, 2022). Article 9 of GDPR recognizes biometric data as a particular category necessitating businesses to enforce stringent privacy measures, including impact assessment of

customers (Kindt, 2018). Our framework enables a manager to understand the higher challenges of biometric data and the impact on consumer willingness to obtain future services.

Secondly, we recommend that systems be designed with automatic verification mechanisms to prevent unauthorized data transfer without obtaining the necessary consent. Biometric data collection provides a significant business value in hospitality with the ability to build intelligence to derive a competitive advantage (Tussyadiah, 2020). However, to disclose data confidently, consumers should be aware of the transparency of data use. Therefore, companies should redesign strategies to encourage consumers to share biometric data by providing higher transparency, indicating an audit trail allowing the consumer to trace the data management process. Therefore, one possible approach is to implement a system, such as a loyalty card with points based on usage, to notify and inform consumers about using their biometric data. This can be in the form of an SMS or by updating a consumer profile that is visible to the consumer, like having an online bank account.

Third, managers should consider unbalanced privacy a core element in redesigning a privacy strategy. Companies should create consumer risk profiles by classifying data on controllable and uncontrollable privacy to differentiate biometric from biographic data. Firms can rank consumers based on the impact of unbalanced privacy. This ranking will enable managers to detect vulnerable consumers based on the effect of uncontrollable privacy paradox in advance. Profiling consumers based on privacy risk will provide a unique platform to manage the privacy paradox (Ioannou *et al.,* 2020; Liyanaarachchi, 2020). Management of uncontrollable privacy paradox will enable an organization to build customer loyalty on privacy protection and create a competitive advantage through immersive technology.

4.4. Limitations and future research

First, building on the existing literature while adopting a mixed-method study, this paper proposes a unique direction to research biometric data in immersive technology use. Scholars can test the propositions across various contexts to achieve a broader perspective in future studies across different contexts. Additionally, the conceptual model will be helpful for application in industries such as banking, advertising, and entertainment, which extensively utilize immersive technology.

Secondly, testing key boundary conditions, such as consumer characteristics, readiness to utilize immersive technology, understanding the metaverse, and acceptance of privacy imbalances, can further enhance our framework. This also applies to the American population, in that recent research found that Americans particularly care about their privacy in hospitality (D'Acunto *et al.*, 2021, Hwang *et al.*, 2012). The strategy redesign based on the study's conceptual framework will ensure ethical conduct and adherence to the national and international protocols in data protection.

Third, future research could examine the impact of the uncontrollable privacy paradox on selecting service providers in hospitality. More specifically, the degree of competitive advantage a firm can achieve by designing a proactive privacy strategy in managing biometric data. Also, it is essential to test the conceptual model with consumers from different countries and cultures to examine different degrees of privacy (Liyanaarachchi *et al*., 2021). We thus encourage future research to investigate the impact of the uncontrollable privacy paradox in different country settings, international contexts, and continents.

Fourth, we invite scholars to explore the differential impacts of the proposed framework across consumers with different age levels (baby boomers to Gen Z) and identify the effect of unbalanced privacy on disclosure decisions.

References

Accenture. (2022), "Consumer Interest in "Virtual Living" Intensifies, Accenture Survey Finds", available at: https://newsroom.accenture.com/news/consumer-interest-in-virtual-living-intensifies-accenture-survey-finds.htm (accessed 10 August 2023).

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

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V. and Viglia, G. (2020), "Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth," *Journal of Retailing*, Vol. 96 No. 4, pp. 490-506.

Amper, R. (2023), "How Biometrics Helps Modernize the Hotel Guest Experience", available at: https://hoteltechnologynews.com/2023/02/how-biometrics-helps-modernize-the-hotel-guest-experience/ (accessed 10 August 2023).

Barnes, S. B. (2006), "A privacy paradox: Social networking in the United States", *First Monday*, Vol 11 No 9.

Bagozzi, R.P. (1977), "Structural Equation Models in Experimental Research", *Journal of Marketing Research*, Vol. 14 No. 2, pp. 209–226.

Barrell, S. (2021), "Virtual reality travel: is it more than just a gimmick?" available at: https://www.nationalgeographic.co.uk/travel/2021/05/virtual-reality-travel-is-it-more-than-just-a-gimmick (accessed 26 April 2023).

Barrera, K. G., and Shah, D. (2023), "Marketing in the Metaverse: Conceptual understanding, framework, and research agenda," *Journal of Business Research*, Vol.155 No. 113420.

Barth, S., de Jong, M.D. and Junger, M. (2022), "Lost in privacy? Online privacy from a cybersecurity expert perspective", *Telematics and informatics*, Vol. 68 No. 101782.

Bazeley, P., and Jackson, K. (2013), "Perspectives: qualitative computing and NVivo. Qualitative data analysis with *NVivo"*, pp.1-46.

Boo, H.C. and Chua, B.L. (2022), "An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore", *International Journal of Contemporary Hospitality Management*, Vol. 34 No.11, pp.4052-4079.

Bouncken, R. B., Qiu, Y., and García, F. J. S. (2021), "Flexible pattern matching approach: Suggestions for augmenting theory evolvement," *Technological Forecasting and Social Change*, Vol. 167 No. 120685.

Brocato, E. D., Voorhees, C. M., and Baker, J. (2012), "Understanding the influence of cues from other customers in the service experience: A scale development and validation," *Journal of Retailing*, Vol. 88 No. 3, pp. 384-398.

Buhalis, D., O'Connor, P. and Leung, R. (2023), "Smart hospitality: from smart cities and smart tourism towards agile business ecosystems in networked destinations," *International Journal of Contemporary Hospitality Management*, Vol. 35 No. 1, pp.369-393.

Chang, N. L. (2022), "New Delta airport screen shows personalised flight info to dozens of travellers at once using A.I", available at: https://www.euronews.com/next/2022/07/07/new-delta-airport-screen-ai-shows-personalised-flight-info-to-dozens-of-travellers-at-once (accessed 24 February 2023).

Cowan, K., Javornik, A., and Jiang, P. (2021), "Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs", *Psychology & Marketing*, Vol. 38 No. 10, pp. 1799-1813.

Creswell, J.W. and Clark, V.L.P. (2017), *Designing and conducting mixed methods research*, (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Cyr, J. (2019), *Focus groups for the social science researcher*, Cambridge University Press.

D'Acunto, D., Volo, S. and Filieri, R. (2021), "Most Americans like their privacy :Exploring privacy concerns through U.S. guests' reviews," *International Journal of Contemporary Hospitality Management*, Vol. 33 No. 8, pp. 2773-2798.

De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G. and Kannan, P. K. (2021), "Opportunities and challenges of using biometrics for business: Developing a research agenda," *Journal of Business Research*, Vol. 136, pp. 52-62.

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

Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A. and Galanos, V., (2021), "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy", *International Journal of Information Management*, Vol. 57 No. 101994.

Dwivedi, Y.K., Hughes, L., Wang, Y., Alalwan, A.A., Ahn, S.J., Balakrishnan, J., Barta, S., Belk, R., Buhalis, D., Dutot, V. and Felix, R., (2023), *Psychology & Marketing*, Vol. 40 No. 4, pp. 750-776.

Femenia-Serra, F., Ioannou, A., and Tussyadiah, I. P. (2022), "Is smart scary? A mixed-methods study on privacy in smart tourism", *Current Issues in Tourism*, Vol. 25 No. 14, pp. 2212-2238.

Fern, E. F. (2001), *Advanced focus group research*, Thousand Oaks, CA: Sage.

Flavián, C., Ibáñez-Sánchez, S., and Orús, C. (2019), "The impact of virtual, augmented and mixed reality technologies on the customer experience," *Journal of Business Research*, Vol. 100, pp. 547-560.

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

Garcia, E. (2022), "Has COVID-19 monitoring changed how UK consumers feel about sharing biometric data?", available at: https://www.capterra.co.uk/blog/2715/covid-monitoring-and-biometric-data-uk-consumers (accessed 9 August 2023).

Gotsch, M.L. and Schögel, M. (2021), "Addressing the privacy paradox on the organizational level: review and future directions," *Management Review Quarterly*, Vol. 73 No. 1, pp 263–296.

Hayes, A.F. (2022), *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, Third edition., The Guilford Press, New York London.

Hilken, T., Keeling, D. I., Chylinski, M., de Ruyter, K., Golf Papez, M., Heller, J., Mahr, D. and Alimamy, S. (2022), "Disrupting marketing realities: A research agenda for investigating the psychological mechanisms of next-generation experiences with reality-enhancing technologies," *Psychology & Marketing*, Vol. 39 No. 8, pp.1660-1671.

Hwang, J., Yoon, S. J. and Bendle, L. J. (2012), "Desired privacy and the impact of crowding on customer emotions and approach-avoidance responses: waiting in a virtual reality restaurant." *International Journal of Contemporary Hospitality Management,* Vol. 24 No. 2, pp. 224-250.

Ioannou, A., Tussyadiah, I. and Lu, Y. (2020), "Privacy concerns and disclosure of biometric and behavioral data for travel," *International Journal of Information Management,* Vol. 54, p. 102122.

Kruyne. T. (2022), "How Hotels Can Leverage New Technologies and Emerging Trends to Deliver Better Guest Experiences", available at: https://hoteltechnologynews.com/2022/07/how-hotels-can-leverage-new-technologies-and-emerging-trends-to-deliver-better-guest-experiences/ (accessed 8 August 2023).

Kindt, E.J. (2018) "Having yes, using no? About the new legal regime for biometric data", *Computer law & security review*, Vol. 34 No .3, pp. 523-538.

Knani, M., Echchakoui, S., & Ladhari, R. (2022), "Artificial intelligence in tourism and hospitality: Bibliometric analysis and research agenda," *International Journal of Hospitality Management*, Vol. 107 No. 103317.

Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, Vol. 64, pp. 122-134.

Koohang, A., Nord, J.H., Ooi, K.B., Tan, G.W.H., Al-Emran, M., Aw, E.C.X., Baabdullah, A.M., Buhalis, D., Cham, T.H., Dennis, C. and Dutot, V. (2023), "Shaping the metaverse into reality: a holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation," *Journal of Computer Information Systems*, Vol. 63 No. 3, pp.735-765.

Lehto, X. Y., Park, S., Mohamed, M. E., and Lehto, M. R. (2023), "Traveler attitudes toward biometric data-enabled hotel services: Can risk education play a role?", *Cornell Hospitality Quarterly*, Vol. 64 No. 1, pp. 74-94.

Lei, S.S.I., Chan, I.C.C., Tang, J. and Ye, S. (2022), "Will tourists take mobile travel advice? Examining the personalization-privacy paradox", *Journal of Hospitality and Tourism Management*, Vol. 50, pp. 288-297.

Liyanaarachchi, G. (2020), "Online privacy as an integral component of strategy: allaying customer fears and building loyalty", *Journal of Business Strategy*, Vol. 41No. 5, pp.47-56.

Liyanaarachchi, G. (2021), "Managing privacy paradox through national culture: Reshaping online retailing strategy," *Journal of Retailing and Consumer Services*, Vol. 60 No. 102500.

Liyanaarachchi, G., Deshpande, S. and Weaven, S. (2021), "Market-oriented corporate digital responsibility to manage data vulnerability in online banking," *International Journal of Bank Marketing*, Vol. 39 No. 4, pp.571-591.

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

Masur, P.K., (2023), "Understanding the effects of conceptual and analytical choices on 'finding'the privacy paradox: A specification curve analysis of large-scale survey data", *Information, Communication & Society*, Vol.26 No.3, pp.584-602.

McKinsey and Company. (2022), "Value creation in the metaverse," available at: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse (accessed 20 March 2023).

Metz, R. (2020), "Portland passes broadest facial recognition ban in the US", available at: https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html (accessed 09 August 2023).

Milmo, D. (2022). "UK Watchdog fines facial recognition firm £7.5m over image collection", available at: https://www.theguardian.com/technology/2022/may/23/uk-data-watchdog-fines-facial-recognition-firm-clearview-ai-image-collection (accessed 03 April 2023).

Moon, H., Yu, J., Chua, B.L. and Han, H. (2022), "*Hotel privacy management and guest trust building: A relational signaling perspective", International Journal of Hospitality Management*, Vol. 102, p.103171.

Morosan, C. (2019), "Disclosing facial images to create a consumer's profile: A privacy calculus perspective of hotel facial recognition systems," *International Journal of Contemporary Hospitality Management*, Vol. 31 No. 8, pp.3149-3172.

Morewedge, C.K., Monga, A., Palmatier, R.W., Shu, S.B. and Small, D.A. (2021), "Evolution of Consumption: A Psychological Ownership Framework," *Journal of Marketing*, Vol. 85 No. 1, pp.196-218.

Nash, J. (2021), "Try-on facial recognition apps land cosmetics firms in court," available at: https://www.biometricupdate.com/202107/try-on-facial-recognition-apps-land-cosmetics-firms-in-court (accessed 22 March 2023).

Pierce, J.L., Kostova, T. and Dirks, K.T. (2001), "Toward a Theory of Psychological Ownership in Organizations," *The Academy of Management Review, Academy of Management*, Vol. 26 No. 2, pp. 298–310.

Paysafe, (2019), "Consumers reluctant to swap passwords for biometrics for fear of identity fraud", available at: https://www.paysafe.com/en/paysafegroup/news/consumers-

reluctant-to-swap-passwords-for-biometrics-for-fear-of-identity-fraud/ (accessed 25 March 2023).

Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R. (2013), *Qualitative research practice: A guide for social science students and researchers*. Thousand Oaks, CA: Sage.

Teddlie, C. and Tashakkori, A. (2011), "Mixed methods research*", The Sage handbook of qualitative research*, pp.285-300.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018), "E.U. General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law & Security Review*, Vol. 34 No. 1, pp. 134-153.

Tucci, L. (2023), "What is the metaverse? An explanation and in-depth guide", available at: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know (accessed 15 March 2023).

Tussyadiah, I. (2020), "A review of research into automation in tourism: Launching the Annals of Tourism Research Curated Collection on Artificial Intelligence and Robotics in Tourism," *Annals of Tourism Research*, Vol. 81 No.102883.

Venkatesh, V., Brown, S.A. and Bala, H. (2013), "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," *MIS Quarterly*, Vol. 37 No. 1, pp.21-54.

Viglia, G., and Dolnicar, S. (2020), "A review of experiments in tourism and hospitality," *Annals of Tourism Research*, Vol. 80 No. 102858.

Viglia, G., Zaefarian, G., and Ulqinaku, A. (2021), "How to design good experiments in marketing: Types, examples, and methods," *Industrial marketing management*, Vol. 98, pp. 193-206.

Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., Thomas, S. and Phalp, K. (2022), "Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications", *Computers in Human Behavior*, p.107545.

Yallop, A.C., Gică, O.A., Moisescu, O.I., Coroș, M.M. and Séraphin, H. (2023), "The digital traveller: implications for data ethics and data governance in tourism and hospitality", *Journal of Consumer Marketing*, Vol. 40 No. 2, pp.155-170.

Yao, Y., Wang, G., Ren, L. and Qiu, H. (2023), "Exploring tourist citizenship behavior in wellness tourism destinations: The role of recovery perception and psychological ownership," *Journal of Hospitality and Tourism Management*, Vol. 55, pp.209-219.

Zhang, F., Pan, Z., and Lu, Y. (2023), "AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home," *Information & Management*, Vol. 60 No. 2, p103736.