



HAL
open science

When powerful artificial intelligence backfires

Saleh Shuqair, Diego Costa Pinto, Caroline Lancelot Miltgen, Giampaolo Viglia

► **To cite this version:**

Saleh Shuqair, Diego Costa Pinto, Caroline Lancelot Miltgen, Giampaolo Viglia. When powerful artificial intelligence backfires. *International Journal of Hospitality Management*, 2024, 120, pp.103778. 10.1016/j.ijhm.2024.103778 . hal-04576285

HAL Id: hal-04576285

<https://hal.science/hal-04576285>

Submitted on 15 May 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

When powerful artificial intelligence backfires

Authors

Saleh Shuqair

Diego Costa Pinto

Caroline Lancelot Miltgen

Giampaolo Viglia

**Manuscript published in the International Journal of Hospitality Management,
(ABS ***)**

Full Ref

Shuqair S., Pinto D., Lancelot Miltgen C. and Viglia G. (2024). When powerful AI backfires, International Journal of Hospitality Management, 120, 103778.

When powerful artificial intelligence backfires

ABSTRACT

Despite recent advancements in artificial intelligence (AI) in hospitality, little is known about its unintended consequences on consumers' privacy concerns. Through an empirical package combining qualitative and quantitative evidence, this research reveals that framing AI as "powerful" enhances privacy concerns (Studies 1–5) by reducing AI-control over data (Study 3). Notably, such effects are reduced in consumer-human agent interactions and increased in consumer-AI ones (Study 4). Finally, interventions providing privacy guarantees can reduce privacy concerns stemming from powerful artificial agents and enhance willingness to disclose data (Study 5). Our findings highlight the unique issues arising from human-AI interactions when using powerful AI and their influence on consumers' privacy concerns and provide practical implications for hospitality managers.

Keywords: Artificial intelligence, AI-control, human-AI interactions, power, privacy concerns, hospitality

1. Introduction

Artificial intelligence (AI) is revolutionizing and reshaping the hospitality landscape (Kim et al., 2021; Pentina et al., 2023). For instance, almost a third of U.S. travelers (32%) are likely to use ChatGPT to plan a trip (Forbes, 2023). Additionally, 70% of customers who receive personalized hotel booking recommendations express higher satisfaction and loyalty (DataArt, 2023). Indeed, the rise of AI technologies has massively reduced consumers' efforts and provided them with a wide range of choices, from travel-planning tools (Kaul, 2022) to personalized concierges (e.g., ConciergeBot) or AI recommendations, empowering consumers to make more informed decisions (Liu, Zhang, & Yao, 2021; Luo & Zhong, 2015).

While AI brings countless advantages to hospitality establishments (Zhang, Chen, & Li, 2019; Knani, Echchakoui, & Ladhari, 2022), such as using AI algorithms in automated concierges or chatbots (Kim, Erdem, & Kim, 2023; Liyanaarachchi, Viglia, & Kurtaliqi, 2023), modern AI systems can influence consumers in ways that may contradict their values or preferences (Bleier et al., 2020). Consequently, 70% of consumers have little to no trust in companies using AI. Additionally, nearly 80% foresee that using AI may make them less comfortable with sharing their personal information (Pew Research Center, 2023). Modern AI systems could thus make consumers feel manipulated or misled (Veale, 2023), and the possibility of data leaks or improper usage of consumers' data (Fast & Jago, 2020) could enhance their privacy concerns.

Throughout consumers' journeys, every interaction decision—such as searching for hotels or flights or making bookings—involves some form of AI assistance (Melzner, Bonezzi, & Meyvis, 2023). While the information they provide is valuable for companies (Puntoni et al., 2021) it also raises privacy concerns (e.g., Cai, Wang, &

Sun, 2024; Hu & Min, 2023). However, the factors influencing these privacy concerns towards AI remain unclear.

Given this complex context, our research provides a more nuanced understanding of the unintended consequences of AI adoption in the hospitality industry. Specifically, we examine individuals' risk perceptions of AI in terms of AI power: high (vs. limited). We suggest that empowering AI might harm consumers' privacy concerns by reducing their perceived sense of control over their data. We define "powerful AI" as a system characterized by complex algorithms and advanced problem-solving capabilities and handles tasks beyond human capacity, like personalized recommendations and facial recognition. In contrast, traditional (or limited) AI, with entry-level capabilities, focuses on less resource-intensive tasks such as smart lighting and staff management.

By doing so, this paper adds to recent studies on the unintended consequences of AI (Du & Xie, 2021). Despite growing studies on privacy concerns and AI (Cai et al., 2022), this literature has provided little evidence on AI-power. Furthermore, the literature provides mixed evidence on privacy concerns. While some studies suggest that privacy concerns are shaped by human-like characteristics (Hu & Min, 2023; Xie & Lei, 2022). Others suggest consumers are willing to disclose sensitive data with AI (vs. human) (Kim et al., 2021). We resolve mixed findings by demonstrating that privacy concerns are heightened when interacting with powerful AI compared to human counterparts. This study also highlights that the likelihood of information disclosure varies depending on who the consumers interact with, i.e., an AI agent compared to a human representative. Unlike previous findings (Kim et al., 2022), our research indicates that when consumers interact with powerful AI, their privacy concerns are

more pronounced than in human-to-human interactions, emphasizing the unique threat posed by power dynamics in human-AI interactions.

Privacy literature has highlighted the impact of privacy concerns on consumer behavior, including data disclosure (Miltgen, 2009). However, the privacy paradox paradigm makes unclear the relationship between privacy risks and subsequent data disclosure or behavioral intentions (Miltgen et al., 2016). To further explore the influence of AI characteristics and interactions on consumer behavior, we focus on privacy concerns as our primary dependent variable. Given its role as a driver of behavior and acknowledging its complex and sometimes indirect effects on consumer behavior, examining consumer perception at this exploratory stage better serves our immediate purpose. This research also contributes to the hospitality literature by examining the unique issues that arise from human-AI interactions and their potentially detrimental effects on consumers' privacy experiences in hospitality settings. This research thus contributes to a better understanding of AI for hospitality managers. In the hospitality context, addressing privacy concerns may indeed not only enhance trust among hotel guests (Moon et al., 2022) but also significantly boost positive word-of-mouth (WOM) and intentions to revisit (Wei et al., 2017).

2. Theoretical Framework and Hypotheses

2.1 Consumers and Artificial Intelligence in Hospitality

Artificial Intelligence (AI) refers to the capacity to combine perception, reasoning, learning, and actuation by an autonomous non-biological system replicating or exceeding human abilities (Belk, Belanche, & Flavián, 2023). Machines empower consumers by performing “intelligent” tasks, such as worldwide searches in milliseconds and sophisticated translation, thus offering highly customized services (Gratch & Fast, 2022).

In the hospitality context, AI facilitates a range of interactions, such as personalized assistance and recommendations (e.g., Yang, Zhang, & Feng, 2023; Hu, Lu, & Wang, 2022). Recent research on AI-human interaction (e.g., Pentina et al., 2023) has examined key areas, such as emotions (Pantano & Scarpi, 2022), attributions (Yalcin et al., 2022), and the effect of AI anthropomorphism (Belanche et al., 2021; Liu, Yi, & Wan, 2022). For example, Lin and Mattila (2021) indicated that socio-emotional and relational needs are critical factors driving robot acceptance and adoption. The anthropomorphism of robots also increases the acceptance of AI in hospitality (Pelau, Dabija, & Ene, 2021). Personalizing and naming robots may also contribute to a more favorable customer evaluation (Mariani & Borghi, 2021). Other research further explored how AI characteristics affect consumers' reactions (Belanche et al., 2021; Kull, Romero, & Monahan, 2021). For instance, in hotels, warm robots are favored in the hedonic-dominant service context, whereas competent robots are preferred in the utilitarian-dominant service context (Liu, Yi, & Wan, 2021). Hospitality research also explored the role of generative AI in hospitality and showed how creating personalized marketing content improves booking experiences (Dogru et al., 2023).

2.2 Artificial Intelligence and privacy concerns in Hospitality

Advancements in information technologies have increased concerns about individuals' privacy (Liyanaarachchi et al., 2023). The term "*privacy concerns*" refers to perceptions of potential negative consequences associated with personal information (Baruh, Secinti, & Cemalcilar, 2017) and to individuals' beliefs about the risks and potential negative consequences associated with sharing personal information (Cho, Lee, & Chung, 2010). It also refers to individuals subjectively perceiving privacy situations in various contexts, such as the illegal collection, monitoring, acquisition, transmission, and storage of private information (Martin et al., 2017). These consumers'

concerns influence their reactions, including trusting beliefs and intentions to disclose information (Bansal, Zahedi, & Gefen, 2016).

Recent research suggests that privacy concerns towards AI have mainly focused on factors such as service robots (Song et al., 2023) or AI characteristics, such as anthropomorphism (Cai et al., 2022; Hu & Min, 2023). In this paper, instead of examining factors beyond those associated with AI features, such as human-like characteristics, we shift our focus to how AI power shapes privacy concerns.

2.3 Artificial Intelligence and Power

We refer to powerful AI as systems that are often characterized by higher levels of complexity and sophistication in terms of algorithms, models, and problem-solving capabilities, enabling them to handle complex tasks and provide sophisticated analyses (Davenport, 2018) that humans are unable to handle (Belk et al., 2023). Examples of powerful AI systems include personalized recommendation systems, voice-activated room controls, facial recognition for check-in, and robotic services (Boo & Chua, 2022). Conversely, limited AI refers to systems with entry-level or limited capabilities, characterized by limited computational resources, and designed for basic or less resource-intensive tasks, such as smart lighting solutions, efficient staff management, and automated check-in and check-out.

In the age of AI, consumer data has become highly valuable (e.g., Lee & Cranage, 2011), particularly in the hospitality context (Song et al., 2023). Hence, we suggest that power AI comes to light through the loss of control from consumers over their data, making them feel disempowered (Campbell & Miller 2011; Cooper & Maxwell 1995) or vulnerable (e.g., Morgan, Schuler, & Stoltman, 1995).

The extant literature on the psychology of power (e.g., Labrecque et al., 2013) refers to power as a social construct that emerges from asymmetric control over valued resources in relations and typically involves a comparison or interaction between two or more parties (Lammers, Stoker, & Stapel, 2009). Power shapes consumer behavior and activities in various ways. Particularly, in the digital world, consumers have the power to manage and control their online identities by adjusting their privacy preferences and controlling what type of information they are willing to share with firms (Tucker, 2014). While the impact of power on consumer behavior is well-documented (Fiske, 2010; Lammers et al., 2009), we still do not clearly understand how AI power characteristics could affect consumers' privacy concerns, especially in the hospitality sector. We suggest that powerful AI could lead consumers to anticipate possible personal data misuse. Consequently, when interacting with powerful AI, such as facial recognition systems, we anticipate heightened privacy concerns compared to limited AI systems.

H1. Powerful (vs. limited) AI systems trigger higher (lower) privacy concerns.

2.4 Power and AI-Control in Human-AI Interactions

Control is a psychological concept that captures individuals' belief in control over events or environments (Cloarec, 2022; Rotter, 1966). We define AI-control as individuals' perceptions that AI-systems creates a sense of control on their personal information, which is similar to the sense of control that which an individual feels when a system allows them to control the use of their personal information through privacy settings (e.g., Hajli & Lin, 2016).

Individuals are likely to have lower privacy concerns when they have some control over their data (Sheehan & Hoy, 2000). This effect is obvious in social network

sites which reduce people's control over their personal information, which often raises their privacy concerns (Hajli & Lin, 2016; Tucker, 2014); however, this effect is lessened when users are offered more control over their personal information through enhanced regulation (Tucker, 2014) or more protective privacy settings (Baruh et al., 2017).

Extending prior research, we anticipate that highly powered AI will cause consumers to face a lack of control over their data (e.g., Fast & Schroeder, 2020). Since AI often relies on large datasets to make predictions (Mariani et al., 2022), the use of personal data by those AI systems might raise the feeling that information is being used in ways consumers cannot control or fully understand, leading to a sense of diminished control over their data. Prior research on technology autonomy and power suggests that when websites or mobile apps make decisions on behalf of users, it potentially reduces their autonomy and freedom of choice (Hu & Wise, 2021). Such perceptions are typically reduced when users have control over their personal information (e.g., Martin et al., 2017; Tucker, 2014)

As AI uses consumer data and data is a resource that matters to consumers, powerful AI may increase consumers' privacy concerns (Kopalle et al., 2021) and their fear when interacting with such AI systems. Prior hospitality and marketing research has mainly focused on the trade-offs between disclosing data (Kim et al., 2019; Tussyadiah, 2020; Zhou, Lu, & Ding, 2020) and consumers' desire to protect their privacy (Acquisti, Taylor, & Wagman, 2016), disregarding how AI power can affect consumers' privacy concerns. If, for example, a hotel was utilizing AI algorithms to analyze guest preferences and behavior and recommend personalized room amenities, such as room temperature, lighting, and entertainment options, we predict such AI systems could make some consumers uncomfortable because such use of their

preferences without their explicit consent could be experienced as a loss of control over their data which could then raise their privacy concerns. With AI collecting and analyzing extensive data, consumers may feel they are losing control over their data, which is associated with a risk that their data is over-used or even misused by algorithms, consequently raising privacy issues. For instance, highly personalized ads may lead consumers to believe AI enhances hospitality companies' control over their data, fostering concerns about extensive tracking of their preferences and behavior without explicit consent. As a consequence,

H2. AI-control mediates the relationship between power AI systems and privacy concerns.

Overview of Studies

We test the unintended consequences of powerful (vs. limited) AI on consumers' privacy concerns through the mediating effect of AI-control over their personal information. We expect that in AI-human interaction in hospitality, privacy concerns are salient because AI relies on large amounts of data to make predictions or decisions about the tourists (Longoni et al., 2019), and this could be associated with unethical issues such as unauthorized access, misuse of data, or data breaches (Knani et al., 2022). We rely on a set of studies to test our predictions, using different manipulations and samples to increase the robustness of our results (Francis, 2012).

Study 1 provides initial evidence of how human-AI interactions enhance consumers' privacy concerns over the use of their data. Studies 2 and 3 provide further evidence by testing the main effect of powerful (vs. limited) AI on privacy concerns and the underlying mediating effect of AI-control. Importantly, Study 4 provides an important boundary condition for the AI power effects to hold: privacy concerns are

high when powerful (vs. limited) AI performs data collection tasks but are mitigated when human agents process the data instead. Finally, Study 5 shows that highly powerful AI is less of a liability when AI tools are explicitly portrayed as giving high data control, compared to when no such control is described.

Study 1: Focus group on hotel guests' perception of AI.

Fourteen hotel guests discussed their AI concerns during a focus group conducted in Louisiana, United States. Referrals were used to enlist pertinent participants (i.e., hotel guests who have visited at least one hotel in the previous year) (Aiello et al., 2020). We employed a stratified sampling technique, targeting individuals who had visited at least one hotel in the calendar year. Our participant selection guidelines aimed to encompass adults of diverse ages, educational backgrounds, occupations, and life experiences. Moreover, participants were required to possess familiarity with AI and prior interactions with AI within the hospitality context. The initials of participants are provided at the end of each quote.

The session was converted into a word processing program to enable NVivo content analysis (Bazeley & Jackson, 2013). Interrater reliability was achieved through the independent reading, analysis, and comparison of the transcripts. The transcripts were independently read, analyzed, and compared, leading to interrater reliability measured with Cohen's kappa coefficient (0.81). Using a categorizing method proposed by Brocato, Voorhees, and Baker (2012), items that showed comparable qualities were listed to identify reoccurring themes in the data.

Results

The emerging themes of the interviews were (i) powerful algorithms, (ii) AI-privacy concerns, (iii) AI-control, and (iv) sensitive information. Although hotel guests

have mixed feelings regarding AI algorithms: for instance, one participant indicated that *“I find AI algorithms useful, but the idea that they know everything about me makes me feel vulnerable”* (RB). Interestingly, the participants are at ease with giving up some sensitive information, but only up to a point. Indeed, as one participant reported, *“I find it creepy when algorithms are particularly powerful as I worry they will control our lives soon”* (LC).

In some situations, consumers feel giving up their data to AI systems to improve their travel experiences could be useful. *“When I land after a long flight, I am glad to see AI support me in speeding up the security controls and passport clearance”* (LT). However, they particularly worry about advanced biometric approaches: *“When I realize hotels and airports now have a digital copy of every inch of my face, I find it invasive and scary”* (SU).

Importantly, participants discuss the consequences of interacting with AI agents: *“What is frustrating is that I lose control of my data. This is concerning when traveling, as I do not even know the rules and regulations of a particular country in terms of data custody”* (SB); similarly, *“I feel my privacy is at stake here, and it looks like I have no control”* (MS). Consumers seem to be more worried when they interact with a robot because they feel the relationship is unbalanced in such a case: *“When the agent is human, we are on the same page, and I feel I have more control. When the agent is a robot, there is a clear unbalance here, and I feel even more vulnerable.”* (AM).

Discussion

The exploratory qualitative approach enhances our understanding of the phenomenon. While finding AI useful, hospitality consumers also experience a sense of loss of control and vulnerability, indicating potential negative consequences for the

preservation of their privacy. Study 1 highlights that concerns are particularly associated with powerful AI tools, perceived as more threatening to their personal information. Study 1 has a notable limitation: addressing specific questions necessitates expertise in “algorithms” since AI algorithms often lack transparency, even in the AI systems themselves (Loi, Ferrario, & Viganò, 2021).

Study 2. Powerful AI and privacy concerns

Study 2 investigates whether powerful AI, compared to limited AI, influences consumers' perceptions of privacy risks. Participants were informed that the study aimed to assess their perceptions of booking websites. Specifically, they were asked to imagine planning a trip to London and seeking travel advice (flights and hotels) online. Participants were then introduced to the FindHotels app. They were randomly assigned to one of two conditions: high AI power versus limited AI power (see Appendix B for details).

Participants and procedure

One hundred US consumers participated in this single factor between-subjects experiment. Participants were recruited from Amazon Mechanical Turk (Mturk) (34% Women, $M_{\text{age}} = 33.44$, $SD = 8.66$) in exchange for a nominal payment. Eight participants were dropped from the analysis for failing attention checks, leaving a final sample size of 92. Participants were randomly assigned to a scenario involving high-power ($N=49$) versus limited-power AI ($N=43$).

We used a procedure adapted from Gilad et al. (2021) to manipulate powerful (vs. limited) AI and modified it to fit our context, using a description of a fictitious booking website (www.find-hotels.com). Since power is a crucial variable involved in AI's ability to use consumers' data, we manipulated powerful AI by describing AI's

performance to predict future consumer behavior as 90% (high power) vs. 10% (low power) (See Appendix B).

Measures and Manipulation checks

After reading the scenario, participants responded to our privacy concerns measures adapted from Mwesiumo et al. (2021) (see Appendix A). In particular, we focused on their concerns regarding how AI uses and captures their data, on a scale ranging from 1 (strongly disagree) to 9 (strongly agree¹).

As a manipulation check, participants reported to what extent they thought 1/ the company could predict their travel behavior ($M_{\text{high}} = 7.67$ $SD = 1.14$, $M_{\text{limited}} = 6.00$, $SD = 2.16$; ($F(1,91) = 16.55$, $p < .0.01$), and 2/ whether the scenario was about high vs low-performance AI ($M_{\text{high}} = 7.43$ vs. $M_{\text{limited}} = 6.05$; ($F(1,91) = 15.75$, $p < .001$).

Main effect

The results of an Univariate Analysis of Variance (ANOVA) showed that the participants reported higher levels of privacy concerns towards powerful AI ($M = 7.29$, $SD = 1.31$) as opposed to the limited AI condition ($M = 6.65$, $SD = 1.68$; ($F(1, 91) = 4.163$, $p = .05$).

Discussion

Study 2 provided initial evidence of the validation of H1, i.e., a signal about the effect of powerful (vs. limited) AI on consumer privacy concerns. The results indicate that powerful AI used by travel websites introduces unique privacy concerns.

Study 3 The Mediation of AI Control

¹ All scales used in our studies range from (1) “strongly disagree” to (9) “strongly agree.”

Study 3 aims to expand our understanding of AI power by testing whether powerful AI introduces threats that impact consumers' control perceptions, heightening privacy concerns.

Procedure and Sample

One hundred and forty US participants from Prolific participated in the study in exchange for a nominal payment. Six participants failed attention checks. Our final sample comprised 134 participants (38.8 % Women, $M_{\text{age}} = 37.62$, $SD = 10.57$). Participants read the same scenario as in Study 2, then responded to our key measures, privacy concerns ($\alpha = .71$), and three items for AI-control (see Appendix A).

Manipulation checks

We confirmed participants in the limited AI condition perceived the website as low in power ($M_{\text{limited}} = 7.01$; $SD = 1.40$) as compared to the participants in the high power condition ($M_{\text{high}} = 7.44$; $SD = 1.14$, $F(1,132) = 3.789$; $p < .05$).

Main Effects

An ANOVA with AI power (high vs. limited) as the independent variable and privacy concerns as the dependent variable revealed a significant main effect. In particular, participants reported significantly higher privacy concerns towards high AI power ($M = 7.27$, $SD = 1.24$) than their counterparts in the limited-power AI condition ($M = 6.90$, $SD = 1.29$, $F(1,131) = 2.822$, $p < .05$).

An ANOVA with AI power (high vs. low) predicting participants' AI-control confirmed that, as expected, participants in the high AI power condition reported higher beliefs that AI controls their data ($M = 7.18$, $SD = 1.20$) as compared to participants in the limited AI condition ($M = 6.68$, $SD = 1.44$, $F(1, 132) = 4.81$, $p = .05$).

Mediation Analysis of AI-Control

A bootstrapping analysis (PROCESS, model 4; Hayes, 2017) with 10,000 samples tested whether AI-control indeed mediated the effect of AI power (high vs. limited) on privacy concerns. Findings suggest AI power (0 = limited; 1 = high) increased AI-control ($b = 0.50, SE = 0.22, t(131) = 2.19, p = .005$), and AI-control significantly predicted privacy concerns ($b = 0.42, SE = 0.07, t(131) = 5.70, p < .001$). The direct effect was not significant ($b = 0.15, SE = 0.20, 95\% CI = [-0.24, .54]$). The total effect ($b = 0.36, SE = 0.21, 95\% CI = [-0.06, .80]$) and the indirect effect of AI power on consumers' privacy concerns via AI-control were significant ($b = 0.31, SE = 0.11, 95\% CI = [0.01, .48]$). This suggests that the relationship between AI power and privacy concerns is mediated by AI-control.

Discussion

Study 3 shows that AI power creates a sense of control, making consumers more concerned about their data being captured by high (vs. limited) power AI. Although AI is intended to empower consumers, helping them to achieve tasks or improve their online experience (e.g., Hu et al., 2023), our findings suggest that powerful AI tools might, on the contrary, reduce consumers' sense of control in support of H2.

Study 4. Boundary Condition of Agent Type

Study 4 tests a potential boundary condition to AI power effects. Although recent research shows that consumers have lower privacy concerns towards AI (vs. human agents) (Kim et al., 2019), we expect that high (vs. limited) AI power is likely to have a reversed effect. We expect the AI power effects on privacy concerns to only hold for artificial agents, not for human agents. Powerful AI, such as service robots, may be perceived as more invasive than humans when dealing with people's data. This study

compares consumer privacy concerns regarding AI (vs. human agents) to test such an effect (Kim et al., 2019).

Participants and Procedure

Two hundred US travelers were carefully selected from MTurk, using specific screening criteria based on travel behavior (34.5% Women, $M_{age} = 38.72$, $SD = 9.99$). We used a scenario-based experiment to measure privacy concerns. Participants were randomly assigned to 2 (Agent type: AI-chatbots vs. human agent) x 2 AI power (high vs. limited) between-subjects factorial design using a travel-related scenario.

To measure privacy concerns, they were asked to imagine: “*You are planning to visit London, and you are looking for travel advice (flights and hotels).*” They were then assigned to one of the four conditions. We used the manipulation proposed by Wien and Peluso (2021) to manipulate agent type: “*During your search, you come across an online travel agency that provides travel recommendations by chatbots [travel consultant]. We used the same manipulation as the one applied in previous studies regarding AI power.*” Participants then responded to our key measures.

Manipulation checks

AI-condition participants indicated that the service was made by chatbots ($M = 7.40$, $SD = 1.44$), different from human agent-condition participants ($M = 6.89$, $SD = 1.78$, $F(1, 93) = 15.73$, $p < .001$), confirming the success of the manipulation.

Results

We conducted a 2x2 ANOVA to investigate the joint impact of agent type (chatbot vs. human) and power (high vs. limited). First, we found a non-significant

effect of agent type on privacy concerns ($F_{(2, 196)} = .313, p = .577, \eta^2 = .002$ $M_{AI} = 7.44, SD = 1.19$ vs. $M_{human} = 7.36, SD = 1.00$), and a non-significant effect of power on privacy concerns ($F_{(2, 196)} = .337, p = .562, \eta^2 = .002; M_{limited} = 7.35, SD = 1.10$ vs. $M_{high} = 7.45, SD = 1.10$). More importantly, there was a significant two-way interaction between agent type (human vs. AI) and power (powerful vs. limited) on privacy concerns ($F_{(2, 196)} = 4.071; p < .045, \eta^2 = .020$).

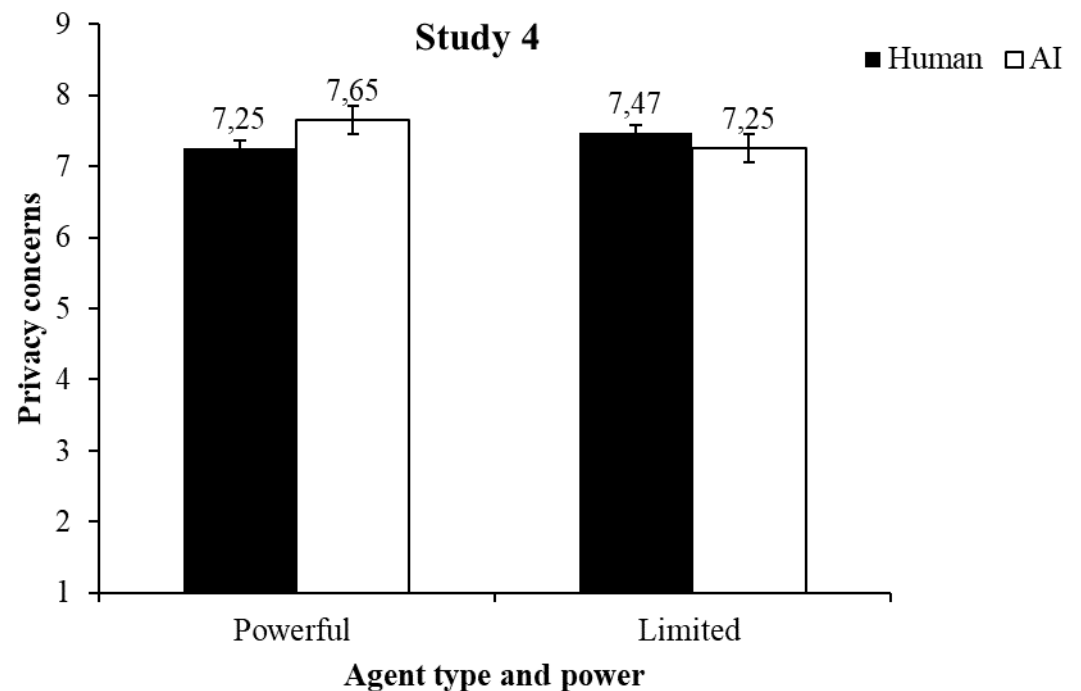


Figure 1. Agent type and power

Discussion

Study 4 provides insights into the impact of AI power on privacy concerns in human-AI interactions in tourism. Our findings suggest that interactions between tourists and powerful AI may heighten privacy concerns compared to interactions solely involving humans. Specifically, participants exhibited increased privacy concerns when interacting with powerful AI agents compared to interactions exclusively involving human agents. These results underscore the nuanced relationship between AI-power and

privacy concerns in the context of human-AI interactions in tourism. Our findings extend existing research on human-AI interactions (e.g., Kim et al., 2019) by highlighting the role of power dynamics in exacerbating privacy concerns.

Study 5. Overcoming AI Power Effects with Privacy Guarantees

Studies 2–4 mainly focused on privacy concerns. Study 5 tests another critical outcome variable in the privacy realm (i.e., willingness to disclose data) and examines whether providing consumers with a privacy guarantee would enhance data disclosure willingness. Prior research suggests that having control over data might affect consumers' willingness to disclose data (e.g., Xu et al., 2012). Managers may overcome AI liability by providing explicit guarantees about data control, mitigating consumers' reliance on a default inference about a negative relationship between powerful AI and data disclosure willingness. We predict that AI power is less of a liability when AI tools are explicitly portrayed as providing privacy guarantees than when no such information is provided.

Participants and procedure

Two hundred and twenty US participants were recruited from Prolific (42.7% women, $M_{\text{age}} = 38.61$, $SD = 11.38$) in exchange for compensation. After initial checks, seven participants were removed from the analysis for failing attention checks, leading to a final sample size of ($N=213$). This study employs 2 levels of AI power (high vs. limited) x 2 levels of privacy guarantee (high guarantee vs. no guarantee) between-subject design. Participants were randomly assigned to one of the four conditions.

In order to manipulate AI power, participants were asked to read the scenarios of Study 2, then were assigned to one of the two conditions of privacy guarantee adapted

from Martin et al. (2017) and modified to fit our context; they then responded to the measures.

Manipulation checks

The manipulation had the intended effect: participants in the high (vs. limited) AI power condition reported that the website predicts more of their travel preferences ($M_{\text{powerful}} = 7.25$, $SD = 1.82$ vs. $M_{\text{limited}} = 6.34$, $SD = 2.24$; $F(1, 211) = 11.79$, $p < .001$). Furthermore, participants in the guaranteed (vs. no-guarantee) condition reported that the website gave more guarantee over the use of their data ($M_{\text{high}} = 7.08$, $SD = 1.78$ vs. $M_{\text{limited}} = 6.50$, $SD = 2.29$; $F(1, 211) = 4.36$, $p < .001$).

AI Power Effects on Willingness to Disclose Data

We conducted a 2x2 ANOVA to investigate the joint impact of AI power and privacy guarantee on willingness to disclose data. First, we found a significant main effect of AI power on willingness to disclose data ($F(2, 209) = 4.387$, $p < .037$, $\eta^2 = .021$; $M_{\text{high}} = 5.52$, $SD = .88$ vs. $M_{\text{limited}} = 5.76$, $SD = .76$), and a non-significant effect of privacy guarantee (guarantee vs. no-guarantee) on willingness to disclose data ($F(2, 209) = .000$, $p = 1.000$, $\eta^2 = .000$ $M_{\text{guarantee}} = 5.65$, $SD = .78$ vs. $M_{\text{no-guarantee}} = 5.63$, $SD = .88$). More importantly, there was a significant two-way interaction between AI power and privacy guarantee on willingness to disclose data ($F(2, 209) = 9.87$, $p < .001$, $\eta^2 = .045$).

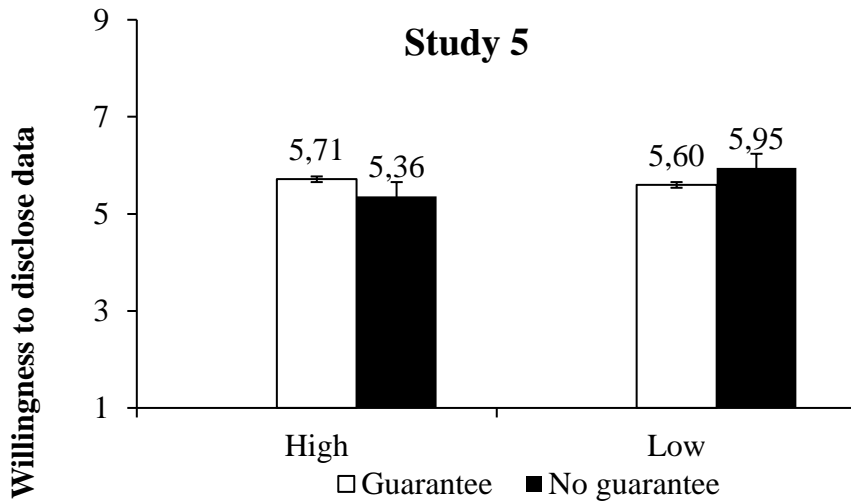


Figure 2. Levels of control

Moderated mediation of AI- control.

We examined whether the effects of privacy guarantee and AI power on data disclosure is mediated by AI-control using PROCESS (Model 8 in Hayes, 2017). First, we found a significant indirect effect of AI power (high= 2; limited = 1) and privacy guarantee (guarantee = 1; no-guarantee = 2) on disclosure willingness ($b = -.75$, $SE = .36$, 95% CI = [0.04; 1.46]). More importantly, the conditional direct effects were significant in the no-guarantee condition ($b = -.51$, $SE = .14$, 95% CI = [-.80, -.22]) but not in the privacy guarantee condition ($b = .00$; $SE = .14$; 95% CI = [-.28, .29]). Finally, as predicted, the moderated mediation index was significant ($b = -.17$, $SE = .08$; 95% CI = [0.01, 0.03]), further supporting our moderated mediation prediction.

Discussion

Study 5 reveals that giving consumers a guarantee over the use of their data when interacting with powerful AI tools can lessen AI power's detrimental effects on data disclosure. Notably, our findings show that providing consumers with a guarantee over the use of their data is helping them to manage the adverse effects of AI power bias.

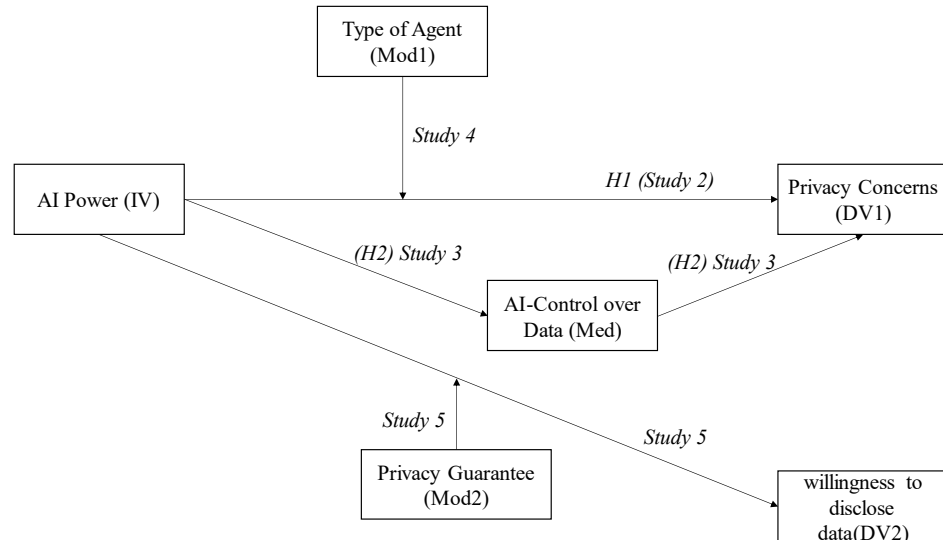


Figure 3. Summary of model results

Discussion and Theoretical Implications

The findings of this research contribute to the literature related to consumer reactions toward AI (Arici, Saydam, & Koseoglu, 2023), consumer power (Kim & McGill, 2011), and privacy concerns (Ioannou et al., 2021) in the context of hospitality.

Prior research suggests that consumers tend to exhibit higher privacy concerns towards AI (e.g., Hu & Min, 2023). However, limited attention was given to AI-power, and the factors that underline this effect. Prior research also suggests that while individuals often express privacy concerns, they tend to share their personal information (Lee & Cranage, 2011). Prior work further suggests that perceived contextual personalization (Aguirre et al., 2015; Zhang, Pan, & Lu, 2023) or guarantee policies (Martin et al., 2017) affect privacy concerns and disclosure. Despite this emerging literature on human-technology interaction (Gelbrich et al., 2021; Pantano & Scarpi, 2022), the fact that consumers may feel powerless while interacting with AI has been largely overlooked in the current literature, especially in hospitality settings.

This work extends prior literature by demonstrating that consumer privacy risk perception is influenced by AI-power. We further show that AI power restricts consumers' control over their data, which in turn triggers privacy concerns (Kopalle et al., 2021), showing AI-control as the mediating process through which AI power influences those privacy perceptions. Furthermore, we contribute to recent studies on consumer journeys with AI (e.g., Dhiman, Jamwal, & Kumar, 2023; He & Zhang, 2023) by showing that the use of AI-empowered tools can facilitate or, on the contrary, complexify consumer journeys (Saadi, Touhami, & Yagoub, 2020) through its effect on consumer privacy concerns.

Our findings further advance previous research on consumer-AI interaction by indicating that engaging with modern AI is associated with consumers feeling a sense of power towards AI systems. This suggests that the perception of power is not solely confined to social interactions (Fiske, 2010) but also manifests during human-AI interactions. This observation implies that interacting with potent AI could impact consumers' perceptions and subsequent behavioral intentions.

In addition, our research contributes to studies that compare consumer reactions to AI versus human-related decision-making (Kim et al., 2022). Previous research has produced mixed findings, with some studies indicating a higher willingness to share information with a human (Kang & Gratch, 2010; Pickard, Roster, & Chen, 2016), while other studies suggest that consumers tend to favor disclosing information with AI to avoid negative social judgment (Kim et al., 2023). Our findings indicate that when consumers interact with powerful AI, their privacy concerns are heightened compared to human interactions. This facet suggests that the effects of power, which threaten privacy concerns, are specific to interactions between humans and AI rather than within human-to-human interactions.

Finally, we further broaden the scope of studies on empowering customers with privacy guarantees to reduce negative reactions to AI. We found that providing consumers with more guarantees increases their intentions to disclose personal information, even when interacting with powerful AI. Such findings extend prior research on the consequences of powerful AI and give solutions to mitigate the negative side effects of AI power.

Practical Implications

Our findings guide hospitality providers when designing and implementing AI technologies. The hospitality industry is witnessing a growing adoption of AI-powered technologies, such as facial recognition and data analytics tools (Forbes, 2023; Gonçalves et al., 2024). However, without careful governance, these technologies may pose a risk of privacy breaches or increase consumers' privacy concerns. Consequently, hospitality businesses must establish robust data protection policies and safeguards against potential breaches to enhance customer trust.

Several recent examples illustrate how customers fear AI, with 71% of consumers being concerned about their privacy when interacting with AI (Pew Research Center, 2022). Although policymakers view AI as a trade-off between regulation and innovation, how to regulate AI remains unclear.

One way to guide policymakers is to force companies to develop or use AI that provides consumers with enhanced control over their data to lessen their fears associated with powerful AI. Hospitality providers would also need to carefully balance the power dynamic between consumers and AI systems and design AI interactions that empower users without compromising their privacy. This action could be done, for example, by providing hotel guests with the option to customize the level of interaction

with the AI system. Guests could also choose whether the virtual assistant can access certain personal preferences or limit the data collected during their stay.

Instead of automating data collection, hospitality organizations are encouraged to adopt an opt-in-based consent approach. For example, guests could enable (or not) biometric recognition for room access and decide the extent to which they want to authorize the use of AI systems to interact with the firm.

4.3. Limitations and Future Research

In this work, we mainly focused on customer perceptions of power in AI (high vs. limited power), neglecting other key features in AI, such as anthropomorphism. Recent research suggests that humanizing AI might reduce customers' privacy concerns (Liu & Tao, 2022). Thus, future research could explore how interacting with anthropomorphized AI could affect customer concerns.

High-power AI can be utilized to track individuals' data across multiple devices. Customers may not realize it, but without consent, many images' users post online can be harvested and used to train facial recognition systems. Additionally, AI can perform designated tasks without supervision, which in turn can affect privacy in different ways (Leong, 2019). Future research could thus explore whether AI power effects are salient when the use of AI is unnoticed or subtle.

In our studies, we mainly focused on privacy concerns, neglecting other important outcomes such as consumers' attitudes or intentions to use the apps/website in the future. Future studies could examine the link between AI-power and attitude toward the AI system.

As our studies mainly focused on online hospitality platforms, future research would benefit from exploring face-to-face hospitality service encounters (e.g., check-

in). Furthermore, we did not directly inquire about participants' overall views of AI power, limiting our ability to fully understand the broader context of influence. Future research may consider exploring participants' overall impressions to provide a more comprehensive perspective.

Furthermore, while our studies addressed specific aspects of privacy concerns related to AI, they may not have fully captured broader privacy concerns that individuals may have across different contexts. Additionally, this research also did not examine the effect of the type of data collected and/or used by AI (e.g., sensitive information) (Mothersbaugh et al., 2012). In such cases, the risks associated with the misuse of such sensitive information might also shape how consumers feel toward AI. Thus, future research would benefit from exploring this area further.

In Study 4, it's noteworthy that the main effect of AI power was not significant. However, the interaction effect was, indicating a cross-over interaction dependent on the type of agent. This finding underscores the importance of contextual factors in interpretation (Umesh et al., 1996), emphasizing the need for nuanced analysis in understanding the impact of AI power.

Finally, while in many instances, consumers interact with technology without knowing that AI makes recommendations or personalized ads, this research focused on customers' perceptions and reactions without explicitly examining their awareness levels of AI power.

References

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–92.

- Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49.
- Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, *96*(4), 490–506.
- Arici, H. E., Saydam, M. B., & Koseoglu, M. A. (2023). How Do Customers React to Technology in the Hospitality and Hospitality Industry? *Journal of Hospitality & Hospitality Research*, 10963480231168609.
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy risks perceptions in disclosing private information online. *Information & Management*, *53*(1), 1–21.
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy risks perceptions and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.
- Bazeley, P., & Jackson, K. (2013). Perspectives: qualitative computing and NVivo. *Qualitative data analysis with NVivo*, 1–46.
- Belk, R. W., Belanche, D., & Flavián, C. (2023). Key concepts in artificial intelligence and technologies 4.0 in services. *Service Business*, *17*(1), 1–9.
- Belanche, D., Casaló, L. V., Schepers, J., & Flavián, C. (2021). Examining the effects of robots' physical appearance, warmth, and competence in frontline services: The Humanness-Value-Loyalty model. *Psychology & Marketing*, *38*(12), 2357–2376.

- Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480.
- Boo, H. C., & 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*, 34(11), 4052–4079.
- Brocato, E. D., Voorhees, C. M., & Baker, J. (2012). Understanding the influence of cues from other customers in the service experience: A scale development and validation. *Journal of Retailing*, 88(3), 384–398.
- Cai, R., Cain, L. N., & Jeon, H. (2022). Customers' perceptions of hotel AI-enabled voice assistants: does brand matter? *International Journal of Contemporary Hospitality Management*, 34(8), 2807–2831.
- Campbell, W. K., & Miller, J. D. (2011). *The handbook of narcissism and narcissistic personality disorder*. Hoboken, NJ: John Wiley & Sons.
- Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987–995.
- Cooper, J., & Maxwell, N. (Eds.). (1995). *Narcissistic wounds: Clinical perspectives*. Whurr Publishers.
- Cloarec, J. (2022). Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. *Journal of Business Research*, 152, 144–153.

- DataArt (2023). AI in hospitality: more than a passing trend. Available from <https://www.dataart.com/blog/ai-in-hospitality-more-than-a-passing-trend> accessed on 14-12-2023
- Davenport, T. H. (2018). From analytics to artificial intelligence. *Journal of Business Analytics, 1*(2), 73–80.
- Dhiman, N., Jamwal, M., & Kumar, A. (2023). Enhancing value in customer journey by considering the (ad) option of artificial intelligence tools. *Journal of Business Research, 167*, 114142.
- Dogru, T., Line, N., Mody, M., Hanks, L., Abbott, J. A., Acikgoz, F., & Zhang, T. (2023). Generative artificial intelligence in the hospitality and tourism industry: Developing a framework for future research. *Journal of Hospitality & Tourism Research, 10963480231188663*.
- Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. *Journal of Business Research, 129*, 961–974.
- Fast, N. J., & Jago, A. S. (2020). Privacy matters... or does it? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology, 31*, 44–48.
- Fast, N. J., & Schroeder, J. (2020). Power and decision making: new directions for research in the age of artificial intelligence. *Current opinion in psychology, 33*, 172-176.
- Fiske, S. T. (2010). Interpersonal stratification: Status, power, and subordination. In S. T. Fiske, D. T. Gilbert, & G. Lindzey (Eds.), *Handbook of social psychology* (pp. 941–982). John Wiley & Sons, <https://doi.org/10.1002/9780470561119.socpsy002026>
- Francis, G. (2012). The psychology of replication and replication in psychology. *Perspectives on Psychological Science, 7*(6), 585–594.

Forbes (2023). A third of travelers are likely to use ChatGPT to plan a trip, says survey.

Available from

<https://www.forbes.com/sites/suzannerowankelleher/2023/05/10/chatgpt-to-plan-a-trip/?sh=7b56c6de17ac> accessed on 05/12/2023

Gelbrich, K., Hagel, J., & Orsingher, C. (2021). Emotional support from a digital assistant in technology-mediated services: Effects on customer satisfaction and behavioral persistence. *International Journal of Research in Marketing*, 38(1), 176–193.

Gilad, Z., Amir, O., & Levontin, L. (2021, May). The effects of warmth and competence perceptions on users' choice of an AI system. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–13).

Gonçalves, A. R., Costa Pinto, D., Shuqair, S., Mattila, A., & Imanbay, A. (2024). The paradox of immersive artificial intelligence (AI) in luxury hospitality: how immersive AI shapes consumer differentiation and luxury value. *International Journal of Contemporary Hospitality Management*.

Gratch, J., & Fast, N. J. (2022). The power to harm: AI assistants pave the way to unethical behavior. *Current Opinion in Psychology*, 101382.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, 133, 111–123.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford publications.

He, A. Z., & Zhang, Y. (2023). AI-powered touch points in the customer journey: a systematic literature review and research agenda. *Journal of Research in Interactive Marketing*, 17(4), 620–639.

- Hu, X., & Wise, K. (2021). How playable ads influence consumer attitude: exploring the mediation effects of perceived control and freedom threat. *Journal of Research in Interactive Marketing*, 15(2), 295–315.
- Hu, P., Gong, Y., Lu, Y., & Ding, A. W. (2023). Speaking vs. listening? Balance conversation attributes of voice assistants for better voice marketing. *International Journal of Research in Marketing*, 40(1), 109–127.
- Hu, Y., & Min, H. K. (2023). The dark side of artificial intelligence in service: The “watching-eye” effect and privacy risks perceptions. *International Journal of Hospitality Management*, 110, 103437.
- Hu, P., Lu, Y., & Wang, B. (2022). Experiencing power over AI: The fit effect of perceived power and desire for power on consumers’ choice for voice shopping. *Computers in Human Behavior*, 128, 107091.
- Kaul (2022). What is the role of AI-based personalization in the fast-evolving travel industry? <https://hospitality.economictimes.indiatimes.com/-news/speaking-heads/what-is-the-role-of-ai-based-personalization-in-the-fast-evolving-travel-industry/91599570?redirect=1>
- Kang, S. H., & Gratch, J. (2010). Virtual humans elicit socially anxious interactants’ verbal self-disclosure. *Computer Animation and Virtual Worlds*, 21(3-4), 473–482.
- Knani, M., Echchakoui, S., & Ladhari, R. (2022). Artificial intelligence in tourism and hospitality: Bibliometric analysis and research agenda. *International Journal of Hospitality Management*, 107, 103317.
- Kim, J., Erdem, M., & Kim, B. (2023). Hi Alexa, do hotel guests have privacy risks perceptions with you? A cross-cultural study. *Journal of Hospitality Marketing & Management*, 1–24.

- Kim, T. W., Jiang, L., Duhachek, A., Lee, H., & Garvey, A. (2022). Do you mind if I ask you a personal question? How AI service agents alter consumer self-disclosure. *Journal of Service Research*, 25(4), 649-666.
- Kim, S. S., Kim, J., Badu-Baiden, F., Giroux, M., & Choi, Y. (2021). Preference for robot service or human service in hotels? Impacts of the COVID-19 pandemic. *International Journal of Hospitality Management*, 93, 102795.
- Kim, T., Jiang, L., Lee, H., & Duhachek, A. (2019). Telling Your Secrets to an Ai: Consumers Prefer Disclosing Private Personal Information to an Ai (Vs. a Human). *ACR North American Advances*.
- Kim, S., & McGill, A. L. (2011). Gaming with Mr. Slot or Gaming the Slot Machine? Power, Anthropomorphism, and Risk Perception. *Journal of Consumer Research*, 38(1), 94–107
- Kopalle, P. K., Gangwar, M., Kaplan, A., Ramachandran, D., Reinartz, W., & Rindfleisch, A. (2022). Examining artificial intelligence (AI) technologies in marketing via a global lens: Current trends and future research opportunities. *International Journal of Research in Marketing*, 39(2), 522–540.
- Kull, A. J., Romero, M., & Monahan, L. (2021). How may I help you? Driving brand engagement through the warmth of an initial chatbot message. *Journal of Business Research*, 135, 840–850.
- Labrecque, L. I., Vor Dem Esche, J., Mathwick, C., Novak, T. P., & Hofacker, C. F. (2013). Consumer power: Evolution in the digital age. *Journal of Interactive Marketing*, 27(4), 257–269.
- Lammers, J., Stoker, J. I., & Stapel, D. A. (2009). Differentiating social and personal power: Opposite effects on stereotyping, but parallel effects on behavioral approach tendencies. *Psychological Science*, 20(12), 1543–1548.

- Lee, C. H., & Cranage, D. A. (2011). Personalization–privacy paradox: The effects of personalization and privacy assurance on customer responses to travel Web sites. *Tourism Management*, 32(5), 987–994.
- Leong, B. (2019). Facial recognition and the future of privacy: I always feel like... somebody's watching me. *Bulletin of the Atomic Scientists*, 75(3), 109–115.
- Lin, I. Y., & Mattila, A. S. (2021). The value of service robots from the hotel guest's perspective: A mixed-method approach. *International Journal of Hospitality Management*, 94, 102876.
- Liyanaarachchi, G., Viglia, G., & Kurtaliqui, F. (2023, forthcoming). Privacy in hospitality: managing biometric and biographic data with immersive technology. *International Journal of Contemporary Hospitality Management*.
<https://doi.org/10.1108/IJCHM-06-2023-0861>
- Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, 127, 107026.
- Liu, X. S., Yi, X. S., & Wan, L. C. (2022). Friendly or competent? The effects of perception of robot appearance and service context on usage intention. *Annals of Tourism Research*, 92, 103324.
- Liu, Y., Zhang, R., & Yao, Y. (2021). How tourist power in social media affects hospitality market regulation after unethical incidents: Evidence from China. *Annals of Hospitality Research*, 91, 103296.
- Loi, M., Ferrario, A., & Viganò, E. (2021). Transparency as design publicity: explaining and justifying inscrutable algorithms. *Ethics and Information Technology*, 23(3), 253–263.

- Longoni, C., Bonezzi, A., & Morewedge, C. K. (2019). Resistance to medical artificial intelligence. *Journal of Consumer Research*, 46(4), 629–650.
- Luo, Q., & Zhong, D. (2015). Using social network analysis to explain communication characteristics of travel-related electronic word-of-mouth on social networking sites. *Tourism Management*, 46, 274–282.
- Mariani, M., & Borghi, M. (2021). Customers' evaluation of mechanical artificial intelligence in hospitality services: a study using online reviews analytics. *International Journal of Contemporary Hospitality Management*, 33(11), 3956–3976.
- Mariani, M. M., Perez-Vega, R., & Wirtz, J. (2022). AI in marketing, consumer research and psychology: A systematic literature review and research agenda. *Psychology & Marketing*, 39(4), 755–776.
- Melzner, J., Bonezzi, A., & Meyvis, T. (2023). Information disclosure in the era of voice technology. *Journal of Marketing*, 87(4), 491–509.
- Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organizations*, 6(6), 574-603.
- Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*, 69(10), 4659-4666.
- Moon, H., Yu, J., Chua, B. L., & Han, H. (2022). Hotel privacy management and guest trust building: A relational signaling perspective. *International Journal of Hospitality Management*, 102, 103171.

- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76–98.
- Morgan, F. W., Schuler, D. K., & Stoltman, J. J. (1995). A framework for examining the legal status of vulnerable consumers. *Journal of Public Policy & Marketing, 14*(2), 267–277.
- Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., & Bråthen, S. (2021). An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. *Journal of Business Research, 136*, 63–75.
- Pantano, E., & Scarpi, D. (2022). I, robot, you, consumer: Measuring artificial intelligence types and their effect on consumers emotions in service. *Journal of Service Research, 25*(4), 583–600.
- Pentina, I., Xie, T., Hancock, T., & Bailey, A. (2023). Consumer–machine relationships in the age of artificial intelligence: Systematic literature review and research directions. *Psychology & Marketing, 40*(8), 1593–1614.
- Pelau, C., Dabija, D. C., & Ene, I. (2021). What makes an AI device human-like? The role of interaction quality, empathy and perceived psychological anthropomorphic characteristics in the acceptance of artificial intelligence in the service industry. *Computers in Human Behavior, 122*, 106855.
- Pickard, M. D., Roster, C. A., & Chen, Y. (2016). Revealing sensitive information in personal interviews: Is self-disclosure easier with humans or avatars and under what conditions? *Computers in Human Behavior, 65*, 23–30.
- Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing, 85*(1), 131–151.

- Pew Research Center (2022). Understanding algorithmic bias and how to build trust in AI. Available from <https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html>, accessed on 12/07/2022
- Pew Research Center (2023). Growing public concern about the role of artificial intelligence in daily life. Available from <https://www.pewresearch.org/short-reads/2023/08/28/growing-public-concern-about-the-role-of-artificial-intelligence-in-daily-life/> accessed on 15/11/2023
- Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, 80(1), 1–28
- Saadi, H., Touhami, R., & Yagoub, M. C. (2020). Revolution of artificial intelligence and the internet of objects in the customer journey and the air sector. *Journal of Information Technology Management*, 12(2), 59–69.
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62–73.
- Song, B., Xu, H., Hu, W., Li, Y., & Guo, Y. (2023). How to calculate privacy: privacy concerns and service robots' use intention in hospitality. *Current Issues in Tourism*, 1-17.
- Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546–562.
- Tussyadiah, I. (2020). A review of research into automation in hospitality: Launching the Annals of Hospitality Research Curated Collection on Artificial Intelligence and Robotics in Hospitality. *Annals of Hospitality Research*, 81, 102883.
- Umesh, U. N., Peterson, R. A., McCann-Nelson, M., & Vaidyanathan, R. (1996). Type IV error in marketing research: The investigation of ANOVA interactions. *Journal of the Academy of Marketing Science*, 24, 17–26.

- Veale, K., (2023). Does ChatGPT Have Privacy Issues? Available from <https://www.makeuseof.com/chatgpt-privacy-issues/> accessed on 12-06-2023
- Wei, W., Hua, N., Fu, X. and Guchait, P. (2017). The impacts of hotels' error management culture on customer engagement behaviors (CEBs). *International Journal of Contemporary Hospitality Management*, 29(12), 3119–3137.
- Wien, A. H., & Peluso, A. M. (2021). Influence of human versus AI recommenders: The roles of product type and cognitive processes. *Journal of Business Research*, 137, 13–27.
- Xie, L., & Lei, S. (2022). The nonlinear effect of service robot anthropomorphism on customers' usage intention: A privacy calculus perspective. *International Journal of Hospitality Management*, 107, 103312.
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 23(4), 1342–1363.
- Yang, X., Zhang, L., & Feng, Z. (2023). Personalized tourism recommendations and the E-tourism user experience. *Journal of Travel Research*, 00472875231187332.
- Yalcin, G., Themeli, E., Stamhuis, E., Philipsen, S., & Puntoni, S. (2022). Perceptions of justice by algorithms. *Artificial Intelligence and Law*, 1–24.
- Zhang, K., Chen, Y., & Li, C. (2019). Discovering the tourists' behaviors and perceptions in a tourism destination by analyzing photos' visual content with a computer deep learning model: The case of Beijing. *Tourism Management*, 75, 595–608.

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.

Zhou, Y., Lu, S., & Ding, M. (2020). Contour-as-face framework: A method to preserve privacy and perception. *Journal of Marketing Research*, 57(4), 617–639.

Appendix A. Measurements and Items

Study	Concept	Items	Cronbach's Alpha	Source
Study 2, 3, and 4	Privacy concerns	<p>In such a context</p> <p>It would bother me when I am asked for personal data.</p> <p>I would think carefully before providing personal data.</p> <p>I am concerned that too much personal data is collected</p>	<p>Study 2 $\alpha = .84$</p> <p>Study 3 $\alpha = .71$</p> <p>Study 4 $\alpha = .74$</p> <p>Study 5 $\alpha = .82$</p>	Mwesiumo et al. (2021)
Studies 3 and 5	AI-control	<p>I believe that AI has control over what happens to my personal information.</p> <p>It is up to me how much these apps use my information.</p> <p>I have a say in whether my personal information is shared with others</p>	<p>Study 3 $\alpha = .70$</p> <p>Study 5 $\alpha = .81$</p>	Mothersbaugh et al. (2012)
Study 5	Willingness to disclose data	<p>I am willing to reveal my data with Skyapp</p> <p>I will probably reveal my personal information with this app.</p> <p>I will reveal my personal information with Skyapp</p>	Study 5 $\alpha = .90$	Zhang et al. (2018)

Appendix B. Experimental scenarios

** Notes: Scenarios adapted from Gilad et al. (2021), Roy & Naidoo (2021) and Wien and Peluso (2021) and modified to fit our context.*

Studies 2 and 3

Powerful AI	FindHotel is a new mobile app for travel (hotels). It uses high-performance machine learning. It is highly competent as it analyzes large datasets. FindHotel is highly trained algorithms that can predict up to 90% of travel behavior (e.g., your travel preferences)
Limited AI	Find-hotels is a new mobile app for travel (hotels). It uses a low-performance machine learning. It has low competence as it analyzes small datasets. FindHotel uses basic algorithms, which are only trained to predict only 10% of travel behavior (e.g., your travel preferences).

Study 4: AI vs. Human “Power”

Low power AI	Imagine you are planning to visit London and you are looking for travel advice (Flights and hotels). To make the best possible decision, you search the Internet for information regarding your holiday. During your search, you come across an online travel agency that provides travel recommendations by using chatbots with artificial intelligence. To get travel advice, you start interacting with a chatbot that provides with you online recommendations. The Chatbot was developed to help people in their search and to be satisfied with their travel goals. The chatbot task to suggest several travel options and seemed extremely happy to give you information.
Low power - Human	Imagine you are planning to visit London and you are looking for travel advice (Flights and hotels). To make the best possible decision, you search the Internet for information regarding your holiday. During your search, you come across an online travel agency that provides travel recommendations by using travel agents (travel consultant). To get travel advice, you start interacting online with a service employee travel consultant, which provides with you online recommendations. The employee was trained to help people in their search and to be satisfied with their travel goals. The employee task to suggest several travel options and seemed extremely happy to give you information.
High PowerAI	Imagine you are planning to visit London and you are looking for travel advice (Flights and hotels). To make the best possible decision, you search the Internet for information regarding your holiday. During your search, you come across an online travel agency that provides travel recommendations by using chatbots with artificial intelligence. To get travel advice, you start interacting with a chatbot that provides with you online recommendations. The chatbot was very competent at serving customers because it uses a state-of-the-artificial neural network algorithm that was trained on data from over millions of requests. The chatbot was able to suggest a great deal that was customized for you.

High Power - human	<p>Imagine you are planning to visit London and you are looking for travel advice (Flights and hotels). To make the best possible decision, you search the Internet for information regarding your holiday.</p> <p>During your search, you come across an online travel agency that provides travel recommendations by using travel agents (travel consultant). To get travel advice, you start interacting online with a service employee travel consultant which provides with you online recommendations.</p> <p>The employee was very competent at helping customers. He is trained in dealing with many requests. The agent was able to suggest a great deal that was customized for you.</p>
---------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Study 5: Powerful AI and Privacy Guarantees

Powerful AI + guarantee	<p>Skyapp is a new mobile app for travel (Flights and hotels). It uses a high-performance machine learning. It is highly competent as it analyzes large datasets. Skyapp is highly trained algorithms that can predict up to 90% of travel behavior (e.g., your travel preferences) Skyapp gives you great control in how they manage your personal information using data protection guidelines (GDPR). For example, you may change at any time your personal settings that dictate how your information is used</p>
Powerful AI + no guarantee	<p>Skyapp is a new mobile app for travel (Flights and hotels). It uses a high-performance machine learning. It is highly competent as it analyzes large datasets. Skyapp is highly trained algorithms that can predict up to 90% of travel behavior (e.g., your travel preferences). Skyapp does not give you any control in how they manage your personal information. For example, you do not have the ability to choose the ways in which your personal information is used.</p>
Limited AI + guarantee	<p>Skyapp is a new mobile app for travel (Flights and hotels). It uses a low-performance machine learning. It has low competence as it analyzes small datasets. Skyapp uses basic algorithms, which are only trained to predict only 10% of travel behavior (e.g., your travel preferences). Skyapp gives you great control in how they manage your personal information using data protection guidelines (GDPR). For example, you may change at any time your personal settings that dictate how your information is used.</p>
Limited AI + no guarantee	<p>Skyapp is a new mobile app for travel (Flights and hotels). It uses a low-performance machine learning. It has low competence as it analyzes small datasets. Skyapp uses basic algorithms, which are only trained to predict only 10% of travel behavior (e.g., your travel preferences). Skyapp gives you great control in how they manage your personal information using data protection guidelines (GDPR). For example, you may change at any time your personal settings that dictate how your information is used.</p>

Appendix C. Summary of the results

Study	Key findings
Study 1 Qualitative data (focus group)	Powerful AI systems and technologies empower tourists; however, it engenders a sense of loss of control.
Study 2 Main effect	High power AI increases privacy concerns compared to traditional AI.
Study 3 Mediation analysis	Replicates the findings of Study 2 and shows that this effect is driven via our key mechanism, perceived control
Study 4. Boundary condition agent type	Study 4 demonstrates that the impact of power on privacy concerns is distinct in human-AI interactions. The results indicate that when tourists interact with powerful AI systems, their privacy concerns are heightened compared to human interactions.
Study 5. Data control	This study shows that when consumers are given control over their data, they are better equipped to manage the negative consequences of powerful AI.