The following publication Han H, Fakfare P, Manosuthi N, Lee J, Kim JJ (2025), "Optimum combination impact of data privacy on customer trust and willingness to accept personal information collection in the lodging sector". Journal of Hospitality and Tourism Technology, Vol. 16 No. 5 pp. 1103–1123 is published by Emerald and is available at https://doi.org/10.1108/JHTT-06-2024-0377.

Optimum combination impact of data privacy on customer trust and willingness to accept personal information collection in the lodging sector

Abstract

Purpose – This study aims to develop a comprehensive model, which elucidated the data privacy, cognitive and affective trust, and the customers' willingness to accept personal information collection in the lodging industry.

Design/methodology/approach – This study employed the tenets of the privacy-trust-intention framework, and used multi-procedures via rigorous methodologies, such as the generalized structured component analysis with measurement errors incorporated ($GSCA_M$), sufficient condition analysis (SCA), necessary condition analysis (NCA), and fuzzy-set qualitative comparative analysis (fsQCA).

Findings - The findings show that certain data privacy factors, such as ethical and lawful data usage are important for either the increment or the manifestation of willingness to accept personal information collection.

Originality/value - The application of the fsQCA provides novel insights by demonstrating that optimal results for data privacy and trust factors, which can be individually applied or in combination, can instill confidence in customers in regards to sharing personal data.

Keywords Ethical data usage, general data usage, secure data usage, lawful data usage, customer trust, willingness to accept personal information collection, the lodging industry

1. Introduction

The significance of safeguarding personal information has become increasingly apparent in this digital era, which is where over 5.3 billion individuals worldwide are actively engaged

online (Petrosyan, 2023). The heightened risk of unauthorized access by third parties poses a serious threat, because the potential leakage of personal information can result in significant harm to service providers as well as consumers (Moon *et al.*, 2022). The hotel industry is particularly vulnerable to this threat, and it is not exempt from the challenges that are associated with securing sensitive information. The commitment to delivering exceptional customer experiences is at the core of the lodging industry, which necessitates the collection and analysis of sensitive customer data as a fundamental strategy for modern businesses. However, the nature of collecting, processing, and storing substantial amounts of customer data makes the lodging sector an attractive target for cybercriminals (Morosan and DeFranco, 2015).

Governments and regulatory bodies have responded by implementing stringent data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, which impose strict data protection obligations on businesses while granting consumers greater control over their personal information (European Commission, 2024). These regulations have significant implications for hotel operations, requiring rigorous adherence to privacy standards. However, many hotels continue to struggle with implementing effective privacy management practices, creating a gap between regulatory requirements and actual practices. This gap not only exposes hotels to potential legal penalties and financial risks but also undermines customer trust—a crucial factor for business sustainability (Balsalobre-Lorente et al., 2024a).

The policy-level problem lies in this disconnect between data privacy regulations and hotel industry practices. While regulatory frameworks are designed to protect consumer rights and establish data security standards (European Commission, 2024), their implementation at the operational level is often inadequate, leading to vulnerabilities and

breaches. Moreover, the erosion of customer trust due to perceived privacy risks can negatively impact willingness to share information, undermining customer relationships and affecting long-term business viability (Esmaeili et al., 2023; Rafei et al., 2022). Addressing this policy gap requires a deeper understanding of how privacy management practices affect both cognitive trust (based on rational assessments) and affective trust (based on emotional connections).

Despite the importance of data privacy, particularly in the lodging industry, research remains limited in exploring how privacy management practices directly influence trust-building and customer behavior. While some studies have used the Privacy-Trust-Intention (PTI) mechanism to examine related constructs (e.g., Choi et al., 2023; Jaspers & Pearson, 2022), empirical work specifically examining how data privacy influences the formation of multi-dimensional trust in hotels is scarce (Moon et al., 2022). Furthermore, the predominant focus on trust as a singular construct overlooks how privacy management may differentially impact cognitive and affective trust (Johnson & Grayson, 2005).

Additionally, most quantitative research has relied on sufficiency logic to explore variable relationships (Richter et al., 2020), which limits the identification of critical factors necessary for desired outcomes. Conventional causal analyses, such as structural models and regression, face limitations in addressing complex and asymmetric relationships within data (Woodside, 2014; Wattanacharoensil et al., 2023). This calls for more holistic approaches to understanding the intricate interactions between privacy practices, trust dimensions, and customer willingness to share personal data.

To address these gaps and align with policy-level requirements, this study extends the PTI model by explicitly incorporating cognitive and affective trust as separate constructs and examining how specific privacy management practices influence these dimensions within

the hotel industry. By moving beyond traditional models that treat trust as a single entity, the study aims to offer a detailed understanding of how privacy practices contribute to the development of both cognitive and affective trust and, subsequently, customer willingness to share information. We employ advanced analytical methods, including generalized structured component analysis ($GSCA_M$), Necessary Condition Analysis (NCA), and fuzzy-set qualitative comparative analysis (fsQCA), to explore the complex interactions between privacy management practices, trust dimensions, and customer willingness to share personal data. $GSCA_M$ assesses the relationships among variables based on sufficiency logic, while NCA identifies critical factors necessary for desired outcomes using necessity logic (Richter et al., 2020). fsQCA allows us to identify specific combinations of privacy management practices that lead to higher levels of trust and greater customer willingness to share personal data (Woodside, 2014).

The study utilizes advanced analytical methods—generalized structured component analysis ($GSCA_M$), Necessary Condition Analysis (NCA), and fuzzy-set qualitative comparative analysis (fsQCA)—to explore complex interactions between privacy management practices, trust dimensions, and customer behavior. $GSCA_M$ assesses the relationships among variables within the model based on sufficiency logic, providing insights into the direct effects of privacy management practices on trust dimensions (Richter et al., 2020). NCA complements this by identifying critical factors that are necessary for achieving desired outcomes, such as customer willingness to share personal data (Richter et al., 2020). Finally, fsQCA identifies optimal combinations of privacy practices that result in higher levels of trust and greater willingness to share personal data (Woodside, 2014).

The specific privacy management attributes analyzed include ethical, lawful, and secure data usage, which are derived from the literature (e.g., Mohd et al., 2019; Yu et al.,

2022). This approach ensures a comprehensive understanding of both direct relationships and critical conditions driving customer behavior within the context of privacy management in the lodging industry. Furthermore, by examining the gap between regulatory frameworks and operational practices (Balsalobre-Lorente et al., 2023), the study aims to bridge policy and practice, offering actionable insights for hotel managers to enhance privacy strategies. Considering these methodological approaches and research aims, this study was in particular designed to 1) investigate the influence of data privacy on customer trust, 2) explore the role of data privacy and customer trust in regards to increase/decrease the willingness to accept personal information collection in the lodging industry, 3) develop causal recipes, which is an optimum combination, of data privacy and customer trust factors by utilizing a fsQCA, and 4) identify the necessary conditions that lead to willingness to accept personal information collection.

2. Literature review

2.1. Data privacy management

The hotel industry is progressively relying on data-driven technologies in order to tailor the guest's experiences and boost the overall efficiency. Hotels are increasingly applying robust cybersecurity measures, implementing strict access controls, and providing employee training programs in order to stay competitive and protected against unauthorized exposure of personal information (Moon *et al*., 2022). The instances of harm persist despite their diligent efforts in order to comprehensively oversee customer data and safeguard personal details. For example, a security breach occurred in the InterContinental Hotels Group that affected over 1,200 hotels, which included popular brands, such as Holiday Inn and Crowne Plaza. Malware infected front desk cash registers between September and December 2016, which

resulted in the theft of customer debit and credit card data (Siteminder, 2023). These examples show how the significance of the effective customer data management is, and they highlight the necessity for a more secure system.

According to Chen and Jan (2021), achieving absolute safety for customer information is nearly an unreachable goal, suggesting that perfect privacy protection may be more theoretical than practical. This raises a debate on whether privacy management practices aim for robust security or simply mitigate risks to an acceptable level. On one side, Van Alstyne and Lenart (2020) caution about third-party data transfer and advocate for exploring approaches that ensure lawful and ethical usage of customer data. They propose the need for comprehensive strategies that balance compliance with practical data usage. Conversely, this position raises a critical challenge—how do hotels effectively ensure such compliance across all data management stages, especially considering the potential complexities and vulnerabilities involved in third-party data sharing.

Mohd et al. (2019) contributed to the conversation by emphasizing the role of regulatory measures for safeguarding personal information. They identified key principles for compliance, including obtaining consent, providing notifications, protecting data, and ensuring its accuracy and timely disposal. These principles, while foundational, reveal a gap that there is limited insight into how such principles are operationalized in the real-world hotel context, particularly in the interplay between regulatory standards and day-to-day privacy practices (Balsalobre-Lorente et al., 2023b).

Building on these foundational concepts, Yu et al. (2022) categorize data privacy attributes in the hotel industry as ethical, lawful, secure, and general usage, echoing Mohd et al. (2019). Secure usage refers to safely managing sensitive information (e.g., passwords), lawful usage concerns adherence to legal standards, ethical usage emphasizes responsible

data handling for education and moral considerations, and general usage pertains to standard procedures for managing customer information. While this categorization is insightful, a debate arises, particularly how these categories are sufficient to capture the complexities of data privacy practices in hotels, especially when considering varied customer expectations and potential vulnerabilities across different data-handling processes.

In this study, we measure the concept of data privacy through these data usage categories because they directly contribute to the main goal of protecting personal information. Data usage practices are not separate from data privacy; rather, they are the mechanisms through which data privacy is maintained (Mohd et al., 2019). Data privacy refers to the appropriate handling, processing, storage, and protection of personal information to ensure confidentiality, integrity, and availability while allowing authorized access in compliance with relevant regulations (Mohd et al., 2019; Van Alstyne & Lenart, 2020). The primary goal of data privacy is to protect individuals' personal information from unauthorized access and misuse while respecting their consent and legal standards. Data usage, on the other hand, encompasses the specific practices and processes through which customer data is collected, stored, managed, and utilized within an organization (Mohd et al., 2019). While data usage practices are integral to maintaining data privacy, they are distinct in focus—data privacy is the overarching concept aimed at protection, whereas data usage refers to the practical implementation of privacy principles. Thus, although they are interconnected, it is crucial to understand that data usage practices are the mechanisms by which the broader goals of data privacy are achieved. By ensuring that data is used securely, lawfully, ethically, and generally managed according to best practices, hotels can effectively protect customer privacy. Therefore, the alignment between data privacy and data usage in this study is

justified by the role that specific data usage practices play in safeguarding personal information and ensuring compliance with privacy standards.

While these frameworks provide a comprehensive categorization of privacy practices, there is limited empirical research examining the direct impact of these practices on customer trust within the hotel context. This leads to a key debate in the literature, for example regarding how current data privacy practices genuinely safeguard customer information, or they are simply focused on meeting regulatory compliance. Wong et al. (2020) bring attention to a related issue, particularly in the context of Online Travel Agencies (OTAs) that share customer data with hotels. While this study primarily focuses on data privacy practices within hotels, it acknowledges that customer data is often initially handled by OTAs during the booking process before being transferred to hotels. The dual responsibility for data management between OTAs and hotels is a critical issue in the broader context of data privacy (Buhalis and Law, 2008). However, the scope of this study is directed specifically toward understanding how hotels manage customer data once it is transferred from the OTA. This focus was chosen for several reasons.

Firstly, the study centers on the hotel's control over data, as hotels assume direct responsibility for processing, storing, and protecting personal information once it is received from an OTA (Piccoli et al., 2017). Therefore, the primary objective is to analyze the privacy practices under the hotel's purview beyond regulatory compliance, evaluating how these practices foster trust with guests. While OTAs play a significant role in the flow of customer data, the emphasis here is on the privacy measures managed directly by hotels.

Secondly, there is a legal distinction between OTAs and hotels regarding their responsibilities for data management. Hotels, upon receiving customer information, are considered "data controllers, whereas OTAs act as "data processors" during the booking

phase (European Union, 2016). This distinction is relevant under privacy regulations such as the Personal Information Protection Act (PIPA) in South Korea and GDPR in the European context (European Union, 2016). Hotels, as data controllers, carry distinct legal obligations, including secure storage, ethical usage, and proactive data protection. By focusing on these obligations, the study seeks to understand the impact of hotels' privacy management on consumer trust, independent of the initial data processing conducted by OTAs. This study contributes to the ongoing debate by assessing how specific privacy practices (secure, lawful, ethical, and general usage) influence customer trust and willingness to share information within hotel operations. By doing so, it provides critical insights into the real-world application of privacy principles and addresses the gap between regulatory intentions and operational practices in safeguarding customer data.

2.2. Customers' cognitive and affective trust

The PTI model is frequently employed in order to forecast the trust and behavioral intentions of online consumers (Wang and Huff, 2007). According to this model, an individual's behavioral intentions are influenced by their perception of the service provider's honesty, commitment to safeguarding the customers' personal information, and the overall trustworthiness (Liu *et al.*, 2005). The parties involved are perceived as trustworthy when monitoring systems demonstrate strength and reliability (Lindenberg, 2000). This positive perception fosters a willingness on their part to share personal information, because confidence in the reliability and effectiveness of regulatory measures instills a sense of security (Moon *et al.*, 2022). This research, which is based on the PTI model, examines the concept of trust via the lens of two distinct forms, which include cognitive trust and affective trust (Johnson and Grayson, 2005)

Cognitive trust is characterized as a specific level of confidence in a counterpart, which stems from knowledge and past interactions with that party (Wang and Huff, 2007). Cognitive trust evolves as individuals gather enough information about the other party from various sources, which include internal and external (Akrout, 2015). This accumulation of information enables individuals to more accurately foresee the behaviors of the other party in accordance with their duties (Johnson and Grayson, 2005). For example, a frequent hotel guest shares personal information during reservations that builds cognitive trust as the hotel consistently demonstrates robust data privacy measures, which involves staff education and transparent policies. This trust, which is rooted in positive experiences and the hotel's track record, allows the guest to confidently anticipate the continued responsible handling of their data in compliance with privacy obligations.

Affective trust is conversely characterized by a sense of emotional connection and attachment to the other party, which is where an individual perceives genuine care (Johnson and Grayson, 2005; Wang and Huff, 2007). This type of trust is rooted in positive emotions and reciprocal interactions between a company and a customer, which foster a robust bond between the two parties. It is plausible that they are shaped by distinct antecedents and exert varying influences on the outcome variables given the unique attributes of each trust form. For example, if a hotel staff member takes the time to explain the hotel's rigorous data protection measures, ensures transparent communication about how guest data is handled, and promptly addresses any privacy concerns, it can contribute to the development of affective trust. The guest may feel a sense of security and care by knowing that their privacy is a priority for the hotel. This proactive approach to data privacy can strengthen the emotional connection between the guest and the hotel, which fosters a positive and trusting relationship

While the distinction between cognitive and affective trust is well-acknowledged, the literature lacks consensus on how these trust dimensions are influenced by data privacy practices (Moon et al., 2022). On the one hand, cognitive trust may be more directly shaped by observable actions, such as adherence to privacy regulations and transparent communication. On the other hand, affective trust may be more affected by relational and emotional factors, like staff empathy and efforts to personally reassure customers (Johnson and Grayson, 2005; Wang and Huff, 2007). This debate leads to a critical question regarding how data privacy practices primarily influence cognitive trust through rational assurances, or do they also significantly shape affective trust by fostering emotional security and connection. This gap is crucial to understand for the lodging industry, where both rational evaluations and emotional bonds play significant roles in customer relationships.

Given the hospitality industry's unique nature, where personalized interactions and guest experiences are central, it is essential to investigate how data privacy practices influence both cognitive and affective trust. This insightful understanding can reveal how privacy practices not only secure rational assurances about data handling (cognitive trust) but also foster emotional connections and perceptions of care (affective trust). The current literature does not adequately explore how privacy practices shape these distinct dimensions of trust and the implications for guests' willingness to share personal data. Hence, this study posits that ensuring data privacy in terms of (a) ethical, (b) general, (c) secure, and (d) lawful data usage will bolster both cognitive and affective trust among customers by building upon the literature review and the principles that are outlined in the PTI model within the context of hotel privacy management.

H1a-d: Data privacy significantly affects cognitive trust.

H2a-d: Data privacy significantly affects affective trust.

2.3. Outcome variable: willingness to accept personal information collection

This study explores the fundamental aspect of guests' intentions rooted in trust, specifically within the framework of the Perceived Trust in Information (PTI) model, focusing on their willingness to accept the collection of personal information by hotels. Trust, which encompasses both cognitive and affective dimensions, is a crucial determinant of human behavior (Wang and Huff, 2007). Individuals with a high level of trust in an interaction tend to exhibit positive behaviors, such as openness and cooperation, whereas uncertainty or perceived risks can prompt unfavorable actions, including resistance or reluctance to share information (Moon et al., 2022). In the hospitality context, hotel guests are more inclined to share personal information when they have confidence not only in the property's reputation but also in its data security and privacy management systems (Morosan and DeFranco, 2015). This trust is often built through consistent and transparent communication, the demonstration of ethical practices in data handling, and the overall perception of the hotel's commitment to safeguarding guest information. The strength of this trust relationship plays a pivotal role in determining guests' willingness to engage with the hotel on a deeper level, thereby enhancing their overall experience and loyalty to the brand. As such, understanding and fostering trust is essential for hotels seeking to enhance guest satisfaction and build long-term relationships.

Also, travelers using online travel agencies are more willing to disclose personal information when trust is established based on their judgments of how these providers handle such information (Ioannou *et al*., 2021). A hotel enhances its guests' confidence, which is cognitive trust, by fostering a greater willingness to share personal information during the reservation process when a hotel effectively communicates its advanced cybersecurity

measures. Affective trust, which is rooted in emotional connections, is consequently nurtured via positive experiences and personalized services. Guests who establish emotional bonds with a hotel, which is possibly due to consistent personalized interactions, are more likely to entrust the hotel with their personal information. This emotional connection contributes to an increased inclination to accept data collection. The existing research suggests that trust in service providers within the hospitality and tourism sector is shaped by assessment of privacy management, which impact the customers' intentions to share personal information (Moon *et al*., 2022; Morosan and Defranco, 2015). This study consequently posits that the customers' cognitive (a) and affective (b) trust will heighten their inclination to agree the collection of personal data by hotels.

H3a-b: Customer trust significantly affects willingness to accept personal information collection.

2.4. Configuration effects and hypotheses for fsQCA

Previous studies have established that interactions among variables in complex systems are intricate, and favorable outcomes are typically the result of a combination of variables, often referred to as configurations or causal recipes (Woodside, 2014). These configurations, derived via fsQCA provide insights into the complex relationships between causal conditions and outcome constructs (Wattanacharoensil et al., 2023; 2024; Woodside 2014). In fsQCA, the role of predictors is determined by the attributes of other indicators, meaning that each element may exert either a positive or negative influence on the desired outcome, depending on the characteristics of the other indicators.

This approach exemplifies the principle of equifinality, which suggests that multiple pathways, or configurations, can lead to the same outcome (Woodside, 2014). The complexity of these relationships is particularly relevant in the context of hotel privacy management and customer trust, where various interacting factors contribute to customer behavior, such as the willingness to accept personal information collection (Yu et al., 2022). Traditional symmetric analyses often result in overidentified estimation models that may not adequately address predictive validity. Therefore, in this study, fsQCA is employed following model evaluation and Necessary Condition Analysis (NCA) to explore the optimal combinations of antecedents—such as data privacy and trust factors—that lead to the desired outcome of willingness to accept personal information collection.

The relationships between variables in this study are inherently complex due to the multifaceted nature of both data privacy practices and customer trust dimensions (Moon et al., 2022). Privacy management in hotels involves various aspects, including ethical, lawful, secure, and general data usage, each of which can interact differently with cognitive and affective trust (Yu et al., 2022). The combination of these elements creates a web of interactions where certain configurations of privacy practices may significantly enhance or diminish trust and, consequently, the willingness to share personal information. This complexity cannot be fully captured by traditional symmetric methods (Wattanacharoensil et al., 2023), making fsQCA particularly suitable for this study.

To articulate the complexity and relevance of the configurations examined, we present three models that reflect different potential pathways to the desired outcome. Figure 1 illustrates these models, showing the distinct configurations of data privacy and trust factors that contribute to customers' willingness to share personal information. Each model

represents a unique combination of variables, demonstrating how different pathways can achieve similar outcomes:

Model 1 (H4): The data privacy factors, which include ethical data usage, general data usage, secure data usage, and lawful data usage have a significant effect on willingness to accept personal information collection.

Model 2 (H5): Customer trust, which includes cognitive trust and affective trust, has a significant effect on willingness to accept personal information collection.

Model 3 (H6): Data privacy factors, which include ethical data usage, general data usage, secure data usage, and lawful data usage, and customer trust, which includes cognitive trust and affective trust, has an optimum combination influence on willingness to accept personal information collection.

2.5 Necessary condition analysis

In the realm of hospitality and tourism, there has been a noticeable trend in the adoption of the NCA (Dul, 2022). The NCA represents a forward-thinking methodology that utilizes the necessity logic in order to pinpoint critical conditions that are essential in regards to achieving a desired outcome. The necessary conditions are pivotal for the establishment of desired outcome, but their mere presence does not ensure success (Richter *et al.,* 2020). Meeprom *et al*. (2023) clarified that all necessary conditions should be simultaneously fulfilled in any conditions that lead to the outcomes. Hauff *et al*. (2021) labeled these conditions as *must-have* elements.

Traditional symmetric quantitative methods in contrast use sufficient logic in order to examine causal relationships. Methods, such as regression obtain the net effects of

antecedents in order to elucidate the impact of independent constructs on the outcome construct. Liehr and Hauff (2022) deduced that these indicators significantly enhance the dependent variable, which is not obligatory, as *nice-to-have* factors. Ethical data usage and lawful data usage in regards to the data privacy management in hotels may be crucial, but they are not necessarily adequate as sufficient conditions. On the other hand, the effect of cognitive and affective trusts may only be realized when customers explicitly recognize this particular condition. Employing necessity logic, which was elucidated by Dul (2022) via the NCA, hypotheses are framed as *X is a prerequisite for Y to occur*, which implies that *Y cannot exist if X is absent*. Accordingly, we propose the following.

H7: Data privacy factors are the necessary conditions for the customers' willingness to accept personal data collection.

H8: Trust factors are the necessary conditions for the customers' willingness to accept personal data collection.

2.6 Theoretical foundation and the empirical model development

The empirical model proposed in this study is developed through a systematic integration of key constructs related to data privacy management and customer trust within the hotel industry (Johnson and Grayson, 2005; Mohd et al., 2019; Moon et al., 2022; Yu et al., 2022). The foundation of this model rests on the premise that effective data privacy practices are pivotal in fostering both cognitive and affective trust among hotel guests, which in turn influences their willingness to share personal information.

The empirical model posits that data privacy management directly influences both dimensions of trust. Effective data privacy practices enhance cognitive trust by demonstrating

the hotel's competence and reliability in handling personal information. Simultaneously, these practices contribute to affective trust by fostering an environment where guests feel emotionally secure and valued. In turn, both cognitive and affective trust are hypothesized to positively impact guests' willingness to accept the collection of personal information. Cognitive trust encourages guests to share information based on their rational assessment of the hotel's data protection capabilities. Affective trust motivates information sharing through the emotional assurance that the hotel genuinely cares about their privacy and well-being.

Recognizing the multifaceted nature of data privacy and trust, the model adopts a configurational approach to capture the interplay between various factors (Woodside, 2014). This approach allows for the identification of different combinations of data privacy practices and trust dimensions that can lead to the desired outcome of increased willingness to share personal information. By exploring these configurations, the model acknowledges that there is no single pathway to achieving high levels of trust and willingness to share data, but rather multiple viable combinations that can effectively produce the same positive outcome.

In sum, the empirical model is derived from the logical integration of data privacy management and trust dimensions. It illustrates how comprehensive data privacy practices serve as the foundation for building both cognitive and affective trust, which are critical drivers of guests' willingness to share personal information. This logical framework sets the stage for the subsequent empirical analysis, where the relationships and configurations proposed will be tested to validate their effectiveness in the context of hotel privacy management.

Insert Figure 1 here

3. Methodology

3.1. Composition of measurement items and research methods

The measurement items were composed based on a set of measurements where the validity and reliability were established in the prior research. First, the measurement items for secure data usage, which included 6 items, lawful data usage, which included 5 items, ethical data usage, which included 4 items, and general data usage, which included 4 items, were extracted from Yu *et al.* (2022) in order to measure the data privacy components. Next, cognitive trust and affective trust were each measured using five items that were borrowed from Johnson and Grayson (2005). Lastly, four items were used in order to assess willingness to accept personal data collection, based on the study by (Degirmenci, 2020). All the measurement items were modified in order to fit the hotel privacy management, and they were rated using a seven-point Likert's scale. All the measurement items are shown in the Appendix.

3.2. Data collection procedures and study samples

This study employed an online survey created by a research firm, which is the Embrain, in South Korea. The data collection was conducted over a four-week period from October 1, 2023, to October 31, 2023. The decision to focus on a Korean sample for this study was guided by several key considerations. First, South Korea is recognized as a leader in technology adoption and has one of the highest internet penetration rates in the world, making it a relevant context for examining data privacy issues (Kemp, 2021). This digital environment heightens the importance of privacy management, especially in industries like hospitality, where customer data is frequently collected and processed. Moreover, South Korea has a robust legal framework for data protection, including the Personal Information Protection Act (PIPA), which mandates strict standards for the collection, storage, and use of

personal data (Korea Legislation Research Institute, 2020). This regulatory environment makes South Korea an appropriate setting for studying how privacy management practices impact trust among consumers who are highly aware of privacy concerns.

The sample was randomly recruited from Embrain's extensive panel database, ensuring a diverse pool of South Korean residents. Survey invitations were disseminated via email to maximize reach and participation rates. To qualify for the study, respondents had to meet specific eligibility criteria: they must have stayed at a hotel within the past two years and preferably have experience with international chain hotels. International chain hotels were defined as those operating in multiple countries and adhering to international data privacy standards and regulations, with examples including Marriott, Hilton, and InterContinental. International chain hotels are often at the forefront of implementing comprehensive data privacy measures due to their global presence and adherence to international standards and regulations, making them a critical context for examining the impact of these practices on customer trust (El-Said et al., 2024). Local chain hotels were identified as those primarily operating within South Korea and complying with local data privacy laws (e.g., Lotte Hotels & Resorts), which could have different approaches to data privacy management due to domestic regulations and customer expectations. This distinction was clearly communicated in the survey to capture different privacy management practices and perceptions among hotel users.

Additionally, while the study primarily targeted experiences in international chain hotels, it also considered respondents who stayed at local-chain hotels if they met the recent stay criterion. Including respondents with experience in local-chain hotels was important to capture variations in privacy management practices that may differ due to local regulations, resources, or customer expectations. This approach allowed the study to not only focus on the

established practices of international chains but also to explore the practices of local chains, thereby ensuring that the findings are applicable to the broader hotel industry, and minimizing potential latent sample bias.

Furthermore, for the purpose of this study, which focuses on data privacy management within hotels, respondents were selected based on their experiences with chain hotels in the past two years. It is assumed that these respondents are aware of the role that hotels play in managing and protecting their personal information, regardless of the booking channel. While OTAs may facilitate the initial booking decision, our focus is on how hotels handle customer data once it is in their possession. According to privacy regulations such as the European Union's General Data Protection Regulation (GDPR) (European Union, 2016), hotels, upon receiving customer information, are considered "data controllers," whereas OTAs act as "data processors" during the booking phase. This distinction places primary responsibility on hotels for secure, lawful, ethical, and appropriate usage of personal data—key elements of data privacy management. By framing the study in this way, we ensure that respondents' understanding of data privacy issues aligns specifically with hotel data management practices. We used a couple of attention check questions and ensured that our respondents read each question carefully as an effort to yield the best data quality. For example, to prompt the memory cues of respondents, they were also requested to provide hotel names that they recently stayed. The survey design and content were reviewed by a panel of experts, including three manager-level hoteliers with 10 years practical experience in the hotel industry and three academics specializing in hospitality research. Their combined insights ensured that the questions were contextually appropriate, aligned with industry practices, and academically sound, thereby enhancing the questionnaire's validity and ensuring its relevance to the study's focus on data privacy management in hotels. The experts

suggested minor revisions before finalizing the questionnaire. After the survey was completed, we identified some invalid answers, such as responses with one serial number and removed them after collecting all the responses. As a result, 429 responses were secured for the data analysis.

The respondents included 217 female (50.6%) and 212 male (49.4%) respondents. 23.3% out of the 429 respondents were in their twenties, 25.6% were in their thirties, 24.7% were in their forties, and 26.3% were in their fifties and above. Nearly 70% of the respondents held a bachelor degree, 17% held a postgraduate degree, and 13% held a high school and college degree in regards to education. Finally, 38.9% of the respondents earned between $3,000-5,000 per month, which was followed by 28% earning less than $3,000, 23.3% earning between $5,000 and $8,000, and 9.8% earning $8,000 or more per month.

3.3. Analytical procedures

The main purpose of this research was to apply both sufficiency and necessity logics in order to investigate the effects of data privacy on customer trust and the subsequently willingness to accept personal information collection. The cSEM and QCA packages with the R programming environment were used, which followed Dusa's (2019) suggestion. The formal set-theoretic methods were performed in order to test the hypotheses via the fsQCA. Firstly, the analysis began with the validation of the measurement model. This study adopted the generalized structured component analysis with measurement errors incorporated ($GSCA_M$) in order to derive scores for seven factors, which included secure data usage (SDU), lawful data usage (LDU), ethical data usage (EDU), general data usage (GDU), cognitive trust (CT), affective trust (AT), and willingness to accept personal information collection (WAP). According to Hwang *et al.* (2017), $GSCA_M$ is a modern approach that includes the shared and

distinct elements of the indicators. Our analysis revealed that the measurement model theoretically fit with the data. The analysis also shows the reliability estimates, which include Dijkstra–Henselers rho_A for all variables surpassed 0.7. The results strongly indicate the internal consistency of the measurement model. All factor loadings and AVEs exceeded 0.5, which shows vigorous evidence for the convergent validity. Discriminant validity was verified by considering the advanced heterotrait–monotrait ratio of the correlations were below the accepted value of 0.85. Next, we calibrated the dataset and compute the membership scores, which considered the threshold values of 0.05 (full exclusion), 0.5 (maximum uncertainty), and 0.95 (full inclusion). The derived scores were then used for a sufficient condition analysis (SCA) and the NCA.

4. Research results

4.1. SCA results

We determined whether each study variable is sufficient in order to enhance the outcome by using traditional sufficient logic, which is regression (See Table 1). We can see that the primary factors in the PTI framework can sufficiently enhance the level of the cognitive trust and affective trust of hotel customers, especially ethical data usage (b = 0.317) and lawful data usage (b = 0.250). These findings partially supported H1 and H2. We found that both cognitive (b = 0.302) and affective trust (b = 0.256) have a critical role in regards to explaining the enhancement of the customers' WAP when the net effects between the trust factors and the customers' willingness to accept personal information collection are considered, which therefore fully supported H3.

Insert Table 1 here

4.2. NCA results

All the necessary conditions for the occurrence of the WAP were identified by using the necessity logic. As displayed in Table 2, all trust factors, which include cognitive and affective trust appears to be necessary factors in kind ($d > 0.1$, $p < 0.01$), whereas all the data privacy factors, which include ethical data usage, secure data usage, lawful data usage, and general data usage, are considered necessary factors in degree, which thus support H7 and H8. We discovered that the hotel customers' willingness to accept personal information collection is enabled when their level of ethical data usage, secure data usage, lawful data usage, and general data usage reach these trigger scores.

Insert Table 2 here

4.3. fsQCA results based on the formal set-theoretic approach

This study adopted three parameters for the fsQCA, which include sufficiency inclusion (inclS), proportional reduction in inconsistency (PRI), and raw coverage (covS) for the assessment of the model. All the sufficiency indices were found to be above the established threshold of 0.7, which indicates that all the solutions derived from the fsQCA analysis meet the criteria for sufficiency and prove to be valid across the training and testing datasets (Pappas and Woodside, 2021). We identified one possible configuration for H4, which includes the combination of EDU*GDU*SDU*LDU. This configuration collectively accounted for 91.2% for the manifestation of the WAP. The disjunction of CT was found for the occurrence of WAP in regards to H5. This solution explains 93.5% with a PRI score of 57.5%. H6 was examined next, and we found the possible combination of hotel data privacy

and trust factors, which included EDU*GDU*SDU*LDU*CT. This solution sufficiently explained 88.5% with a PRI score of 59.4%.

We further evaluated the configuration based on empirical solutions derived from the fsQCA, the presence/absence of the proposed theory, and the occurrence or nonoccurrence of the results by using the formal set-theoretic approach (Schneider and Wagemann, 2012). Eight possible models were composed, and Table 3 and Table 4 provide a summary of the findings. The respective percentages relative to the total number of cases (CT1) and the percentage relative to the total number of conditional cases, which included Y or ~Y (CT2), were also included.

Insert Table 3 & 4 here

5. Discussion and implications

5.1 Research implications

This research successfully verified the theoretical framework, which includes data privacy factors, customer trust, and willingness to accept personal information collection, via the utilization of stringent methodological approaches, such as the $GSCA_M$, SCA, fsQCA and NCA. Specifically, it extends the Privacy-Trust-Intention (PTI) model within the context of hotel privacy management, providing a more comprehensive understanding of how data privacy practices influence different dimensions of customer trust (Moon et al., 2022). By empirically demonstrating that data privacy factors influence both cognitive and affective trust, this research enriches the theoretical literature by highlighting the multifaceted nature of trust in the hospitality context. This aligns with recent theoretical advancements that advocate for a dual-trust approach in service management (Janotta and Hogreve, 2024).

This research verifies four critical elements under the privacy construct to gain insights into the data privacy factors that affect customer trust and willingness to accept personal information collection, which include secure data usage, lawful data usage, ethical data usage, and general data usage. These factors are essential for building a comprehensive privacy management strategy that aligns with both regulatory requirements and customer expectations. Our results contribute theoretical implications for scholars in the hospitality field by adopting sufficiency and necessity logic. For example, this study confirms the value of four data privacy variables in the lodging context (Buhalis and Moldavska, 2022; Yu *et al*., 2022). These variables are analyzed before examining their roles in regards to forming a customer's cognitive and affective trust and subsequently WAP. By employing a configurational approach, this study demonstrates the interplay between different data privacy factors and their collective impact on trust and WAP, offering a more holistic view compared to traditional linear models. We successfully introduce a more robust PTI framework in regards to predicting the customers' WAP when they stay at hotels by integrating data privacy factors, customer trust, which included cognitive and affective, and WAP (Moon *et al*., 2022; Wang and Huff, 2007). Moreover, the NCA technique provides an extra layer of results beyond traditional net-effect or sufficient condition analysis. This study could pinpoint the necessary components that are essential for the occurrence of WAP, which thereby significantly contribute to the existing knowledge on customer behavior and hotel data privacy management.

The data privacy factors particularly in terms of ethical data usage and lawful data usage had a significant effect on customer trust, which is based on the SCA results. Ethical data usage was found to be a statistically significant factor in regards to determining cognitive trust (b = 0.317), but lawful data usage was discovered to meaningfully affect

affective trust (b = 0.25). The results partially supported H1 and H2 by showing the significance of data privacy management in the hotel sector in regards to formulating customer trust. Ethical data usage, which is influenced by both external and internal forces, can significantly shape the cognitive trust of hotel customers, which is consistent with the study by Moon *et al.* (2022). This is primarily important because the foundation of trust is solidified, when hotels prioritize transparency and cultivate a sense of reliability that aligns with the customers' expectations for ethical data usage (Wang and Huff, 2007), which thereby develops the customers' cognitive trust. Van Alstyne and Lenart (2020) affirmed that there is a need for business organizations to prioritize lawful and ethical utilization and management of customer data. Customers develop a sense of confidence and an emotional connection with an organization when affective trust is determined, which thereby exhibits their willingness to share personal information (Johnson and Grayson, 2005). Our results align with the prior research.

This study further adopted the necessity logic via the NCA in order to attain the desired outcome (WAP), which is unlike the traditional analysis that applies the sufficiency logic. The results interestingly shed light on the factors of data privacy and trust that are necessary for the occurrence of WAP. Our results generally align with the empirical results from the SCA analysis (H3), and studies that were previously conducted in the field of hotel privacy and customer trust (Yu *et al*., 2022), which were in different research settings. Cognitive trust and affective trust especially emerge as indispensable prerequisites for the manifestation of WAP, which highlights the significance of cultivating customer trust via the well handling of data and ethical data usage. Hotels need to ensure the implementation of robust data privacy measures and transparent practices in order to foster these essential components of trust (Moon *et al*., 2022). Moreover, all data privacy factors are essential for

the occurrence of WAP, but they are necessary in degree. In other words, the WAP of hotel customers is triggered when the customers' level of EDU (0.160), GDU (0.147), SDU (0.196), and LDU (0.229) reach these trigger points. Data privacy and trust factors are crucial in order to cultivate WAP in regards to personal information sharing in the lodging industry, which emphasizes their substantial impact on the overall experience when hotels collect personal data. The NCA results identified in this research offer fresh perspectives in regards to forming a solid ground for the development of a comprehensive understanding of the dynamics of the customers' perception of privacy management and trust (Martin *et al*., 2017; Wang and Huff, 2007), which is particularly in the lodging sector.

We followed Schneider and Wagemann's (2012) recommendation and implemented a formal set-theoretic technique in order to investigate a causal recipe for an outcome (WAP) and test the hypotheses (H4-H6), which therefore enhanced knowledge and improved the methodology within the lodging and hospitality field. This study verified the formal set-theoretic theory of the fsQCA model via the tests of eight possible combinations. As such, the validity of the fsQCA model was confirmed. For H4, an analysis via logical minimization by means of Boolean logic indicates interesting results in regards to the hypothesis results. When the solutions were identified based on the *covered most likely* (CML) cases or when the proposed model lines up with the established theory, the findings confirm our expectations (EDU*GDU*SDU*LDU). This result signifies a strong indication for the use of data privacy factors in regards to developing WAP, which confirms the study by Yu *et al.* (2022). An empty set was interestingly found when aligning the model based on the *covered least likely* (CLL) cases and *uncovered most likely* (UML), which implies that no surprised solutions were found when examining these particular cases. Next, we found the one distinct solution (EDU + ~GDU + ~SDU + ~LDU) when examining the model based on *uncovered least*

likely (ULL) cases. This solution indicates that the presence of EDU, which is combined with the negation of GDU, SDU, and LDU, is what we neither expected nor found in the occurrence of WAP. Further investigation into these cases may offer theoretical insights into the limitations or exceptions within the context of the study. Furthermore, an investigation of IML, cML, ILL, and CLL cases exhibit very limited or no cases at the intersection between the theory and the proposed models. This therefore proves the validity of the identification of the data privacy configuration, such as EDU*GDU*SDU*LDU.

Then, we derived one distinct solution by comprising the disjunction of CT in order to achieve H5 by using a Boolean expression. This result is consistent with the earlier SCA analysis, which implies that cognitive trust plays a vital role in regards to cultivating WAP. The finding confirms our expectations by validating the relationship between the combined impact of the trust factors (AT*CT) in regards to influencing WAP when the proposed model is compared with the established theory (Model * Theory * WAP) (Martin *et al*., 2017; Moon *et al*., 2022). However, one unexpected solution occurred, which is CT*~AT, when analyzing solutions based on the CLL cases (Model * ~Theory * WAP). The solution suggests that in certain scenarios where the established theory is not followed or applied, cognitive trust is impactful, but an affective trust toward a hotel firm is not. The combination of CT and AT is not necessary in these specific cases. The number of cases identified in this category was not high, but the exclusion of AT should be noted and investigated further in order to obtain valuable insights. The assessment of other models, such as the non-occurrence of WAP under the set-theoretic analysis demonstrates few to no cases, which verifies the significance of trust factors (CT*AT) combined in regards to influencing WAP in the hotel privacy management context.

Next, H6 was verified in order establish the most effective recipes of data privacy and trust factors that affect WAP. We obtained one possible configuration by using a Boolean expression, which comprised of five dimensions. The result affirms our expectation by validating the relationship between the combined impact of data privacy and trust factors (EDU*GDU*SDU*LDU*CT) and their effect on WAP by aligning the proposed model with the established theory (Model * Theory * WAP) (Mutimukwe *et al*., 2020). The configuration collectively shows the overall solution values in the acceptable level, without the inclusion of affective trust. An empty set was found when attempting to identify solutions based on CLL cases (Model * ~Theory). No unexpected variables therefore exist for the occurrence of WAP under these particular cases. However, five recipes exist, when analyzing the solutions based on UML (~Model * Theory). It is noteworthy that the analysis of these particular cases revealed variations in the configurations but with a modest occurrence (CT1 = 5.73%). These findings suggest that researchers may consider exploring the refinements of these configurations when evaluating the WAP in hotel customers in the future, because they could offer valuable insights into the intricate relationships among data privacy components, trust factors, and their effects on WAP. For example, the absence of ethical data usage in conjunction with the inclusion of cognitive and affective trust might introduce complexities in regards to the development of WAP in the hotel setting. This fresh perspective may offer useful implications for academics in future investigations. Furthermore, the evaluation of other models under the set-theoretic analysis particular from the aspect of the non-occurrence of WAP show few to no cases. This outcome validates the efficacy of the fsQCA solution in regards to formulating WAP, which is derived from the combination of data privacy and trust factors, such as EDU*GDU*LDU*SDU*CT. This study successfully extends the PTI framework and enhances the methodology into the context of hotel privacy management by

employing a multi-procedural approach that includes GSCA$_M$, SCA, NCA, and the set-theoretic theory analysis via the fsQCA.

5.2 Practical implications

This study also provides meaningful for practitioners in the lodging sector. First, from an economic perspective, fostering customer trust through robust data privacy practices can lead to enhanced customer loyalty and increased revenue. Trust reduces the perceived risk associated with sharing personal information, thereby encouraging more frequent and higher-value transactions. Additionally, preventing data breaches through effective privacy management can save hotels from significant financial losses related to legal penalties, remediation costs, and reputational damage. Therefore, investing in comprehensive data privacy measures is not only a regulatory requirement but also a sound economic strategy that can drive long-term profitability and competitiveness in the hospitality market. This is consistent with the resource-based view of the firm, which emphasizes the strategic importance of data as a competitive asset (Barney, 1991).

Secondly, external privacy management should be implemented to showcase privacy policies to customers. This involves establishing robust regulatory frameworks that pertain to data privacy policies and facilitates customers' understanding of privacy-related regulations. The SCA findings revealed that ethical data usage could enhance cognitive trust (b = 0.317). This differentiated impact of data privacy practices on the dimensions of trust—cognitive and affective—is a key discovery that challenges the traditional PTI model, which typically treats trust as a singular construct. Hotels, therefore, need to place a strong emphasis on ethical data usage practices, such as being transparent about how customer data will be used and ensuring that it aligns with ethical standards when collecting customers' personal data. By tailoring their privacy management strategies based on whether they aim to build cognitive or affective

trust, hotels can more effectively foster trust. For example, while ethical data usage significantly enhances cognitive trust, lawful data usage was discovered to meaningfully affect affective trust. Moreover, Mohd et al. (2019) suggested that obtaining consent and providing clarification on how data will be used and how long it will be retained are essential in maintaining ethical data practices. The study findings further suggest that lawful data usage is crucial for fostering affective trust, which is another aspect of trust-building that has practical implications. Managers should, therefore, emphasize their commitment to legal data usage practices when collecting customers' information.

Furthermore, the NCA results imply that managers can highlight the importance of four data privacy factors by considering their specific trigger points. For instance, general data usage must reach 14.7%, and secure data usage must reach 19.6% to foster customers' willingness to accept information collection. This introduction of necessity logic represents a novel approach, as it identifies critical thresholds that are essential for achieving WAP, extending the PTI framework beyond sufficiency logic. These findings provide practitioners with clear benchmarks for their privacy practices, ensuring that they meet the minimum requirements necessary to build trust and encourage data sharing.

Third, hotel executives should extend their privacy management efforts to internal privacy management apart from external privacy management. Employees should be encouraged to adhere to established ethical guidelines and best practices when handling sensitive information. For example, all staff members should be committed to upholding the highest standards of data protection within the organization, which includes regular updating passwords and adopting secure authentication measures. Hotels can create an additional layer of accountability and security within the organization by monitoring who accesses sensitive data and when. Hotel executives should therefore be equally attentive to privacy measures

that concerns employee data. This involves implementing internal privacy management strategies in order to safeguard the sensitive information of staff members.

Finally, five underlying factors, including ethical data usage, secure data usage, lawful data usage, general data usage, and cognitive trust appear in the three fsQCA configurations to foster customers' willingness to accept personal information collection. The study validates that there are multiple, equally valid pathways or configurations of these factors that can lead to WAP, which aligns with the principle of equifinality (Woodside, 2014). This finding challenges the linear relationships often implied by the PTI model. The results from configuration 1 highlight the importance of all four privacy factors (EDU, SDU, LDU, GDU) in shaping hotel customers' inclination to accept personal data collection. The results for configuration 2 show that cognitive trust alone can foster the increment of customers' WAP. Interestingly, the study found that cognitive trust could be sufficient on its own to influence WAP in certain scenarios, without the need for affective trust. This discovery suggests that in some contexts, focusing efforts on building cognitive trust might be more effective, especially where emotional engagement (affective trust) is less critical. The findings revealed that the five underlying components, when combined with data privacy and trust factors (configuration 3), significantly influence hotel customers' willingness to accept personal data collection. Hotel executives should, therefore, promote data privacy and trust factors either individually or combined, as they are sufficient variables in inducing WAP.

5.3 Policy implications

In terms of policy recommendations, the study highlights the persistent gap between data privacy regulations and their practical implementation within the hotel industry. It is crucial for policymakers in the lodging sector to establish clear guidelines that mandate

transparency and accountability in data privacy management. These policies should not only require hotels to disclose how personal information is collected, stored, and used but also ensure that customers are informed about their rights concerning data privacy (Fakfare et al., 2024). For instance, regulations could mandate that hotels obtain explicit consent from guests before collecting their personal information, provide options for data portability, and allow for the deletion of personal data upon request. Furthermore, policymakers should advocate for regular audits and assessments of hotels' data privacy practices, potentially involving third-party evaluations to ensure compliance with legal and ethical standards. This will reinforce customer trust and ensure that hotels maintain high standards of data protection both externally with guests and internally with employees. Effective implementation support can enhance compliance rates and overall data protection standards across the industry (Brown & Duguid, 2000).

Additionally, training and development programs focusing on data privacy should be integrated into the professional development of hotel staff (Balsalobre-Lorente et al., 2024). Policymakers could collaborate with industry associations to create standardized training modules that emphasize the importance of ethical data usage, legal compliance, and the role of cognitive and affective trust in customer relationships. Establishing a centralized privacy management framework that all hotels can adopt would further standardize best practices across the industry, ensuring a consistent approach to data privacy. Efforts to raise awareness among consumers regarding their data privacy rights should be prioritized through educational campaigns at both the industry and government levels (Esmaeili et al., 2023). Empowering customers with this knowledge will lead to more informed decisions and foster a culture of trust between hotels and their guests.

Furthermore, policymakers and industry bodies should collaborate to establish standardized best practices for data privacy management in hotels. These standards should encompass ethical, secure, lawful, and general data usage, providing a comprehensive blueprint for hotels to follow. For example, the adoption of ISO/IEC 27001:2022 standards for information security management systems can provide hotels with a structured framework to manage and protect customer data systematically (International Organization for Standardization, 2022). By following these internationally recognized standards, hotels can ensure consistent data privacy practices, thereby enhancing trust among customers and ensuring compliance with legal requirements. Standardization can help reduce inconsistencies in privacy practices across different hotels, enhancing overall industry trust and compliance. Such standardization efforts are crucial for maintaining a level playing field and ensuring that all hotels meet high privacy standards (Tari et al., 2019).

Additionally, to support the implementation of robust data privacy practices, policymakers should encourage technological innovations that enhance data security and privacy (Jahanger et al., 2022). This could involve funding research into advanced cybersecurity measures or incentivizing the adoption of cutting-edge data protection technologies within the hospitality sector. Technological advancements can provide hotels with the tools needed to proactively address emerging privacy threats and enhance data protection capabilities (Nadkarni et al., 2020).

6. Limitations and future research avenues

While this research provides meaningful insights into the relationship between data privacy factors, customer trust, and willingness to accept personal information collection in hotels, it is not without limitations. One limitation is that the study did not account for

differences in privacy policies across various hotel categories (e.g., luxury vs. budget hotels, independent hotels, and boutique hotels). As privacy expectations and practices may vary significantly among different types of hotels, future research should consider examining these categories as potential moderating variables to assess if and how privacy perceptions differ across different hotel segments. Another limitation lies in the scope of the methodological approaches used. While the current study employed rigorous techniques like GSCA$_M$, SCA, fsQCA, and NCA, future studies could benefit from exploring alternative methods such as prioritization techniques, deep learning models, or best-worst scaling. These approaches could offer deeper insights into customer intentions and behaviors, particularly in the complex and evolving context of privacy management in the hospitality industry. Moreover, future research might also consider longitudinal studies to observe changes in privacy perceptions and trust over time, providing a more dynamic understanding of these critical factors in hotel privacy management.

References

Akrout, H. (2015), "A process perspective on trust in buyer–supplier relationships: 'calculus' an intrinsic component of trust evolution," *European Business Review*, Vol. 27 No. 1, pp. 17-33.

Balsalobre-Lorente, D., Mohammed, K. S., Cifuentes-Faura, J., and Shahzad, U. (2023a), "Dynamic connectedness among climate change index, green financial assets and renewable energy markets: Novel evidence from sustainable development perspective," *Renewable Energy,* Vol. 204*,* pp.94-105.

Balsalobre-Lorente, D., dos Santos Parente, C. C., Leitão, N. C., & Cantos-Cantos, J. M. (2023b). The influence of economic complexity processes and renewable energy on CO2 emissions of BRICS. What about industry 4.0?. *Resources Policy, 82,* 103547.

Balsalobre-Lorente, D., Nur, T., Topaloglu, E. E., & Evcimen, C. (2024a). The dampening effect of geopolitical risk and economic policy uncertainty in the linkage between economic complexity and environmental degradation in the G-20. *Journal of Environmental Management, 351,* 119679.

Balsalobre-Lorente, D., Nur, T., Topaloglu, E. E. and Evcimen, C. (2024b), "Assessing the impact of the economic complexity on the ecological footprint in G7 countries: Fresh evidence under human development and energy innovation processes," *Gondwana Research*, Vol. 127, pp. 226-245.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of management, 17*(1), 99-120.

Brown, J. S., and Duguid, P. (2001), "The social life of information", *Harvard Educational Review*, Vol.71 No.1, pp.151-152.

Buhalis, D. and Moldavska, I. (2022), "Voice assistants in hospitality: using artificial intelligence for customer service," *Journal of Hospitality and Tourism Technology*, Vol. 13 No. 3, pp. 386-403.

Camilleri, M. A., Troise, C. and Kozak, M. (2023), "Functionality and usability features of ubiquitous mobile technologies: the acceptance of interactive travel apps," *Journal of Hospitality and Tourism Technology*, Vol. 14 No. 2, pp. 188-207.

Chen, H. S. and Jai, T. M. (2021), "Trust fall: data breach perceptions from loyalty and non-loyalty customers," *The Service Industries Journal*, Vol. 41 Nos. 13-14, pp. 947-963.

Choi, K., Wang, Y., Sparks, B. A. and Choi, S. M. (2023), "Privacy or security: does it matter for continued use intention of travel applications?," *Cornell Hospitality Quarterly*, Vol. 64 No. 2, pp. 267-282.

Dul, J. (2022), "Problematic applications of necessary condition analysis (NCA) in tourism and hospitality research," *Tourism Management*, Vol. 93, 104616.

Dusa, A. (2019), *QCA with R: A Comprehensive Resource*, Springer International Publishing, Cham, Switzerland.

El-Said, O.A., Elhoushy, S., Smith, M. and Youssif, M., 2024, "Crisis-driven innovation in hospitality: How do international hotel chains innovate to recover from a global crisis?", *International Journal of Hospitality Management,* Vol.120, 103758.

Esmaeili, P., Rafei, M., Balsalobre-Lorente, D. and Adedoyin, F. F. (2023), "The role of economic policy uncertainty and social welfare in the view of ecological footprint: evidence from the traditional and novel platform in panel ARDL approaches," *Environmental Science and Pollution Research*, Vol. 30 No. 5, pp. 13048-13066.

European Commission. (2024), "*Guidelines for the implementation of the General Data Protection Regulation (GDPR) by archive services*", Available at https://commission.europa.eu/documents_en?f%5B0%5D=document_title%3Adata%20protection

European Union. (2016), "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)",* available at https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fakfare, P., Manosuthi, N., Lee, J.-S., Jin, M., Han, H. and Kim, J.J. (2024), "Data vulnerability and privacy risk among hotel guests who share personal data," *Journal of Vacation Marketing*. https://doi.org/10.1177/13567667241276

Han, H., Kim, S., Hailu, T. B., Al-Ansi, A., Lee, J. and Kim, J. J. (2024), "Effects of cognitive, affective and normative drivers of artificial intelligence ChatGPT on continuous use intention," *Journal of Hospitality and Tourism Technology*, ahead-of-print, doi: 10.1108/JHTT-11-2023-0363.

Hauff, S., Guerci, M., Dul, J. and van Rhee, H. (2021), "Exploring necessary conditions in HRM research: Fundamental issues and methodological implications," *Human Resource Management Journal*, Vol. 31 No. 1, pp. 18–36.

Hwang, H., Takane, Y. and Jung, K. (2017), "Generalized structured component analysis with uniqueness terms for accommodating measurement error," *Frontiers in Psychology*, Vol. 8, 2137.

International Organization for Standardization (2022), *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements,* available at: https://www.iso.org/standard/27001

Ioannou, A., Tussyadiah, I. and Miller, G. (2021), "That's private! Understanding travelers' privacy concerns and online data disclosure," *Journal of Travel Research*, Vol. 60 No. 7, pp. 1510-1526.

Jahanger, A., Yu, Y., Hossain, M. R., Murshed, M., Balsalobre-Lorente, D., and Khan, U. (2022), "Going away or going green in NAFTA nations? Linking natural resources, energy utilization, and environmental sustainability through the lens of the EKC hypothesis", *Resources Policy,* Vol.79, 103091.

Jaspers, E. D. and Pearson, E. (2022), "Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns," *Journal of Business Research*, Vol. 142, pp. 255-265.

Johnson, D. and Grayson, K. (2005), "Cognitive and affective trust in service relationships," *Journal of Business Research*, Vol. 58 No. 4, pp. 500-507.

Janotta, F., and Hogreve, J. (2024), "Ready for take-off? The dual role of affective and cognitive evaluations in the adoption of Urban Air Mobility services", *Transportation Research Part A: Policy and Practice*, Vol.185, 104122.

Kemp, S. (2021), "Digital 2021: South Korea. DataReportal – Global Digital Insights" Available at https://datareportal.com/reports/digital-2021-south-korea (accessed 15 August 2024).

Korea Legislation Research Institute (2020), "Personal Information Protection Act", available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (accessed 15 August 2024).

Liehr, J. and Hauff, S. (2022), "Must have or nice to have? Necessary leadership competencies to enable employees' innovative behavior," *International Journal of Innovation Management*, Vol. 26 No. 10, 2250070.

Liu, C., Marchewka, J. T., Lu, J. and Yu, C. S. (2005), "Beyond concern: a privacy–trust–behavioral intention model of electronic commerce," *Information & Management*, Vol. 42 No. 1, pp. 127-142.

Martin, K. D., Borah, A. and Palmatier, R. W. (2017), "Data privacy: Effect on customer and firm performance," *Journal of Marketing*, Vol. 18 No. 1, pp. 36–58.

Meeprom, S., Sathatip, P., Leruksa, C., Manosuthi, N. and Fakfare, P. (2023), "Cannabis-infused food: Uncovering effective conditions for achieving well-being perception and choice behavior among young adult consumers," *Food Quality and Preference*, 104915.

Mohd, A. Z. A., Anuar, N. and Ahmad, S. A. P. S. (2019), "Customer data security and theft: A Malaysian organization's experience," *Information and Computer Security*, Vol. 27 No. 1, pp. 81–100.

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, 103171.

Morosan, C. and DeFranco, A. (2015), "Disclosing personal information via hotel apps: A privacy calculus perspective," *International Journal of Hospitality Management*, Vol. 47, pp. 120-130.

Mutimukwe, C., Kolkowska, E. and Grönlund, Å. (2020), "Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior," *Government Information Quarterly*, Vol. 37 No. 1, 101413.

Nadkarni, S., Kriechbaumer, F., Rothenberger, M., and Christodoulidou, N. (2020), "The path to the Hotel of Things: Internet of Things and Big Data converging in hospitality", *Journal of Hospitality and Tourism Technology,* Vol.11 No.1, pp.93-107.

Pappas, I. O. and Woodside, A. G. (2021), "Fuzzy-set Qualitative Comparative Analysis (fsQCA): Guidelines for research practice in Information Systems and marketing," *International Journal of Information Management*, Vol. 58, 102310.

Petrosyan, A. (2023), "Number of internet and social media users worldwide as of October 2023," available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed 3 March 2024).

Rafei, M., Esmaeili, P., and Balsalobre-Lorente, D. (2022), "A step towards environmental mitigation: How do economic complexity and natural resources matter? Focusing on different institutional quality level countries", *Resources Policy,* Vo.78, 102848.

Richter, N. F., Schubring, S., Hauff, S., Ringle, C. M. and Sarstedt, M. (2020), "When predictors of outcomes are necessary: Guidelines for the combined use of PLS-SEM and NCA," *Industrial Management & Data Systems*, Vol. 120 No. 12, pp. 2243–2267.

Schneider, C. Q. and Wagemann, C. (2012), *Set-theoretic methods for the social sciences: A guide to qualitative comparative analysis*, Cambridge University Press, Cambridge.

Siteminder (2023), "Hotel data breaches: What independent hoteliers need to know about data security," available at: https://www.siteminder.com/r/hotel-data-breaches/ (accessed 5 January 2024).

Tarí, J. J., Pereira-Moliner, J., Molina-Azorín, J. F., and López-Gamero, M. D. (2019), "Heterogeneous adoption of quality standards in the hotel industry: drivers and effects", *International Journal of Contemporary Hospitality Management*, Vol.31 No.3, 1122-1140.

Van Alstyne, M. W. and Lenart, A. (2020), "Economic and business dimensions using data and respecting users: Three technical and legal approaches that create value from data and foster user trust," *Communications of the ACM*, Vol. 63 No. 11, pp. 28–30.

Wang, S. and Huff, L. C. (2007), "Explaining buyers' responses to sellers' violation of trust," *European Journal of Marketing*, Vol. 41 Nos. 9/10, pp. 1033-1052.

Wattanacharoensil, W., Lee, J. S., Fakfare, P. and Manosuthi, N. (2023), "The multi-method approach to analyzing motivations and perceived travel risks: impacts on domestic tourists' adaptive behaviors and tourism destination advocacy," *Journal of Travel & Tourism Marketing*, Vol. 40 No. 2, pp. 109-130.

Wattanacharoensil, W., Fakfare, P., Manosuthi, N., Lee, J. S., Chi, X. and Han, H. (2024), "Determinants of traveler intention toward animal ethics in tourism: Developing a causal recipe combining cognition, affect, and norm factors," *Tourism Management*, Vol. 100, 104823.

Wong, E., Rasoolimanesh, S. M. and Pahlevan Sharif, S. (2020), "Using online travel agent platforms to determine factors influencing hotel guest satisfaction", *Journal of Hospitality and Tourism Technology,* Vol.11 No.3, pp. 425-445.

Woodside, A. G. (2014), "Embrace• perform• model: Complexity theory, contrarian case analysis, and multiple realities," *Journal of Business Research*, Vol. 67 No. 12, pp. 2495–2503.

Yu, J., Moon, H., Chua, B. L. and Han, H. (2022), “Hotel data privacy: Strategies to reduce customers’ emotional violations, privacy concerns, and switching intention,” *Journal of Travel & Tourism Marketing*, Vol. 39 No. 2, pp. 215-227.

Zaki, H. S. and Al-Romeedy, B. S. (2024), “Chatbot symbolic recovery and customer forgiveness: A moderated mediation model,” *Journal of Hospitality and Tourism Technology*, ahead-of-print, doi: 10.1108/JHTT-11-2023-0374.

Table 1.

Sufficient condition analysis

Dependent variable	Constructs	Coefficients	p-value	Sufficient?
CT	EDU	0.317	0.000	Yes**
	GDU	0.170	0.147	No
	SDU	0.129	0.167	No
	LDU	0.086	0.410	No
AT	EDU	0.151	0.126	No
	GDU	0.156	0.231	No
	SDU	0.065	0.528	No
	LDU	0.250	0.075	Yes*
WAP	CT	0.302	0.002	Yes**
	AT	0.256	0.004	Yes**

Note: EDU = ethical data usage, SDU = secure data usage, LDU = lawful data usage, GDU = general data usage, CT = cognitive trust, AT = affective trust, WAP = willingness to accept personal information collection, * = significant at the 90% confidence level, ** = significant at the 95% confidence level, R-square: CT = 32.5%, AT = 22.1%, and WAP = 14%

Table 2.

Single necessary condition analysis

Outcome (WAP)	CE-FDH (d)	p-value	Triggered level	Necessary?
EDU	0.06	0.790	0.160	In degree
GDU	0.06	0.779	0.147	In degree
SDU	0.04	0.927	0.196	In degree
LDU	0.05	0.780	0.229	In degree
CT	0.24	0.000	0.234	**In kind**
AT	0.20	0.000	0.153	**In kind**

Note: CE-FDH = Ceiling Envelopment with Free Disposal Hull, CR-FDH = Ceiling Regression with Free Disposal Hull, EDU = ethical data usage, SDU = secure data usage, LDU = lawful data usage, GDU = general data usage, CT = cognitive trust, AT = affective trust, and WAP = willingness to accept personal information collection, d = effect size

Table 3.

The solution of fsQCA hypotheses

	H4	H5	H6
Variable/Outcome (WAP	Model A	Model B	Model C
EDU	●		●
GDU	●		●
SDU	●		●
LDU	●		●
CT		●	●
AT			
Model's Predictive Power			
inclS	0.703	0.745	0.766
PRI	0.521	0.575	0.594
covS	0.912	0.935	0.885

inclS = Inclusion of Sufficiency, PRI = Proportional Reduction in Inconsistency, covS = Raw Coverage,
● = Core condition, ◌ = Absence, and Blank = Don't care

Table 4.

A summary of the hypothesis testing from earlier fsQCA analysis

Outcome		**H4**	**H5**	**H6**
WAP	Model	EDU*GDU*SDU*LDU	CT	EDU*GDU*SDU*LDU*CT
	Theory	EDU*GDU*SDU*LDU	AT*CT	EDU*GDU*SDU*LDU*CT*AT
	Model * Theory (CML)	EDU*GDU*SDU*LDU	AT*CT	EDU*GDU*LDU*SDU* CT
	inclS	0.703	0.790	0.766
	PRI	0.521	0.624	0.594
	covS	0.912	0.882	0.885
	CT1	52.67%	45.80%	50%
	CT2	87.34%	75.95%	82.91%
	Model * ~Theory (CLL)	-	CT*~AT	-
	inclS	0.924	0.857	0.929
	PRI	0.551	0.496	0.494
	covS	0.370	0.501	0.343
	CT1	0.00%	8.02%	0.00%
	CT2	0.00%	13.29%	0.00%
	~Model * Theory (UML)	-	-	~EDU*CT*AT + ~GDU*CT*AT + ~SDU*CT*AT + ~LDU*CT*AT + EDU*GDU*SDU*LDU*~CT
	inclS	0.924	0.909	0.843
	PRI	0.551	0.488	0.460
	covS	0.370	0.405	0.484
	CT1	0.00%	0.00%	5.73%
	CT2	0.00%	0.00%	9.49%
	~Model * ~Theory (ULL)	EDU + ~GDU + ~SDU + ~LDU	~CT	~EDU*~CT + ~EDU*~AT + ~GDU*~CT + ~GDU*~AT + ~SDU*~CT + ~SDU*~AT + ~LDU*~CT + ~LDU*~AT
	inclS	0.848	0.814	0.873%
	PRI	0.497	0.347	0.458%
	covS	0.421	0.438	0.377%
	CT1	7.63%	6.49%	4.58%
	CT2	12.66%	10.76%	7.59%
	Result of model fit	**Acceptable Fit**	**Acceptable Fit**	**Acceptable Fit**
	Model * Theory (IML)	~EDU*GDU*LDU*SDU	AT*CT	CT*EDU*GDU*LDU*SDU
	inclS	0.703	0.790	0.766
	PRI	0.521	0.624	0.594
	covS	0.912	0.882	0.885
	CT1	0.00%	0.00%	0.00%
	CT2	0.00%	0.00%	0.00%
	Model * ~Theory (ILL)	-	~AT*CT	-
	inclS	0.924	0.857	0.929
	PRI	0.551	0.496	0.494
	covS	0.370	0.501	0.343
	CT1	0.00%	9.16%	0.00%
	CT2	0.00%	23.08%	0.00%

~WAP	**~Model * Theory (cML)**	-	-	~EDU*CT*AT + ~GDU*CT*AT + ~SDU*CT*AT + ~LDU*CT*AT + EDU*GDU*SDU*LDU*~CT
	inclS	0.924	0.909	0.843
	PRI	0.551	0.488	0.460
	covS	0.370	0.405	0.484
	CT1	0.00%	0.00%	8.02%
	CT2	0.00%	0.00%	20.19%
	~Model * ~Theory (CLL)	EDU + ~GDU + ~SDU + ~LDU	~CT	~EDU*~CT + ~EDU*~AT + ~GDU*~CT + ~GDU*~AT + ~SDU*~CT + ~SDU*~AT + ~LDU*~CT + ~LDU*~AT
	inclS	0.848	0.814	0.873%
	PRI	0.497	0.347	0.458%
	covS	0.421	0.438	0.377%
	CT1	6.49%	8.02%	3.82%
	CT2	16.35%	0.00%	9.62%

Note: CML = Covered Most Likely, CLL = Covered Least Likely, UML = Uncovered Most Likely, ULL = Uncovered Least Likely, IML = Inconsistent Most Likely, ILL = Inconsistent Least Likely, cML = Consistent Most Likely, CLL = Consistent Least Likely, CT1 = Cases in the intersection divided by Total number of cases, and CT2 = Cases in the intersection divided by Total number of cases Y > .5

Figure 1.
Conceptual model