Data vulnerability and privacy risk among hotel guests who share personal data

Abstract

This research explores the guests' perception toward data vulnerability and its impact on the privacy risk, privacy concern, and the perceived benefits of sharing personal data with hotels, which is in response to rising concerns about the personal data collection for service facilitation in hotels. A proposed research framework that explains the antecedents and outcomes of hotel guests' privacy risk and privacy concern that is related to personal data sharing was examined using the generalized structured component analysis with measurement errors incorporated (GSCA$_M$), the necessary condition analysis (NCA), and a fuzzy-set qualitative comparative analysis (fsQCA). The results expand the antecedents → privacy concerns → outcomes (APCO) model by determining a set of salient variables, such as data access, data breach vulnerabilities, privacy risk, and concern in regards to determining hotel guests' perceived benefits of sharing personal data. This study provides valuable insights into privacy dynamics, enabling hotel professionals to develop targeted marketing strategies prioritizing both data utilization and guest privacy. It also suggests enhancing data security measures to mitigate concerns and foster trust among guests.

Keywords: Data vulnerability, data access, data breach, privacy risk, privacy concern, hotel, benefits of sharing personal data, the APCO model, privacy calculus theory

1. Introduction

The hospitality industry has undergone a transformative shift in its operations with the integration of advanced technologies in order to enhance customer experiences in an era that is dominated by digital connectivity (Lee et al., 2021; Yu et al., 2024). One of the integral components of this transformation is the collection and utilization of personal data from hotel guests. The benefits of leveraging guest data, which include from personalised recommendations to check-in processes, are undeniable. Hotels extensively collect substantial volumes of data from both existing and prospective guests. This is a practice that plays a pivotal role in regards to reinforcing their competitive advantage via the refinement of products, services, and overall customer experiences (Moon et al., 2022). Martin et al. (2017) asserted that actively leveraging customer data allows business firms to outperform competitors. Their study indicated a potential profit increase of approximately 6% compared to businesses that do not employ customer data management strategies. Effectively utilizing customer data can offer considerable benefits (Yu et al., 2022), but this modern approach has given rise to a critical concern, which includes data vulnerability and the privacy risks (Martin et al., 2017).

The recent studies, such as Yu et al. (2022) investigated how weaknesses in regards to managing customer data can lead to privacy concerns. Another study by Kritzinger and Smith (2008) explored what makes customers perceive risk when they share their personal information. A common finding in these studies is the crucial need to protect customer data in order to prevent harm. Despite this focus, most of the research has concentrated on problems related to data vulnerability and the complexities of handling information. Numerous studies show that these types of vulnerabilities usually have negative impacts on businesses (Degirmenci, 2020; Ioannou et al., 2020; Jozani et al., 2020). However, a notable gap in the research exists. Specifically, there is a need to understand how consumer perception of these risks introduces a negative balance to the benefits associated with sharing personal data (Dogra and Adil, 2024). Most studies did not clearly consider how data vulnerability and privacy concerns, such as fears of data breaches, misuse of information, insufficient transparency, and lack of control over data, directly impact customers' likelihood of sharing personal data. In other words, it is essential to identify how the perceptions of privacy risk and concern diminish the perceived benefits of sharing data, making people hesitant to share their personal information. This is especially important for the hospitality sector, where personalizing the customer experience is essential. Thus, it is crucial to discover elements that influence the concerns of hotel customers in regards to data privacy, and how these factors affect cost–benefit trade-offs in customers' privacy decisions and behaviours.

Ryu and Park (2020) stated that the consumers' willingness to share personal information can vary depending on their evaluation of the benefits and costs that are involved. Perceived benefits are related to what customers think they will gain from consenting to the collection of their personal information in the hotel context. Hotels often entice consumers to share personal data in exchange for benefit offers, such as discounts, financial incentives, and personalised services (Yu et al., 2022). The previous research literature emphasised the importance of consumers' privacy concerns (Degirmenci, 2020), but empirical studies that thoroughly examine the factors that lead to privacy concerns and the subsequent outcomes in the hotel industry are scarce (Moon et al., 2022). Consumer concern generally refers to the anxiety or unease customers feel about the potential misuse of their personal information (Jozani et al., 2020). Privacy risk, on the other hand, is more specific and can be defined as the perceived likelihood that their personal data might be lost, stolen, or misused (van der Schyff et al., 2020). Data vulnerability, from a consumer's perspective, pertains to the inherent weaknesses in how their personal information is managed, stored, and shared, making it vulnerable to unauthorized access or breaches (Mohd et al., 2019; van der Schyff et al., 2020). How data vulnerability might influence hotel customers' perceived privacy risk and concern and how these factors introduce a negative balance to the perceived benefits of sharing personal information are not widely investigated. Specifically, data vulnerability involves customers' fears about the structural and procedural weaknesses in data handling that could lead to unauthorized access or exposure of their information. Addressing this gap not only contributes to academic knowledge but also provides valuable insights for hotel professionals to develop targeted marketing strategies that balance data utilisation with guest privacy concerns, as well as promote the perceived benefits of data sharing.

The privacy calculus theory and the antecedents → privacy concerns → outcomes (APCO) framework are applied in this research. Smith et al. (2011) asserted that there is a need for an in-depth exploration of the APCO model in order to verify its effectiveness in regards to addressing privacy concerns and outcomes across various contexts particularly in situations that are characterised by contextual variations. The hotel sector stands out as a focal point for investigation by considering the contextual complexities of the hotel environment (Moon et al., 2022). As a result, the present study was designed to a) unearth the effect of data vulnerability on hotel guests' perceived privacy risk and concern, b) uncover the role of data vulnerability and perceived privacy risk and concern in regards to reducing perceived benefits of sharing personal data, c) build causal recipes, which include the optimum combination of data vulnerability and perceived privacy risk and concern with the use of a fuzzy-set qualitative comparative analysis (fsQCA), and d) explore the necessary conditions that lead to hotel guests' perceived benefits of sharing personal data.

2. Literature review

2.1. Customer data vulnerability in the hotel sector

Service-oriented companies, which include hotels, are actively collecting customer data in order to improve their overall performance (Kim et al., 2024). This strategic effort can have positive impacts on businesses, but it raises concerns among customers who fear their information may be misused. Martin et al. (2017) stated that data vulnerability involves the various challenges and weaknesses in the protection of customer data that can arise when firms utilize this information. This can be further delineated into data breach vulnerability and data access vulnerability. A customer data breach entails the unauthorised expose of customer information in insecure environments, whereas data access vulnerability involves companies' extensively sharing customer data across different groups using digital documents (Gashami et al., 2015). Customers remain unaware of the permissions that are granted to specific users for data breach or access as well as the methods and procedures that are involved despite customers expecting their data to be well-managed. This lack of awareness extends to potential data leaks by employees or relevant stakeholders (Moon et al., 2022). Given these challenges, addressing data vulnerability in managing customer information is crucial due to the potential for both data breaches and data access issues.

Several studies pay attention to the effectiveness of customer data management and its impact on businesses given the significant damages that result from the leakage of sensitive information. For instance, Yu et al. (2022) found that in the hotel context, customers often feel anxious when they consider the potential harm of data leaks, prompting them to react sensitively. Degirmenci (2022) stated that issues that are related to a customer data breach or improper data access can amplify a customer's unfavourable perceptions, erode trust, and adversely impact their support intentions. Moon et al. (2022) further elucidated that the leakage or misuse of customer data poses a financial risk and damages the reputation as well as also triggers significant psychological anxiety, which includes switching to another hotel. Vulnerabilities in customer data management can arguably exert a detrimental impact on the relationships between customers and hotels, which potentially causes substantial financial and non-financial losses. Hotels must acknowledge its negative repercussions particularly the factors that reduce the customer's perceived benefits of sharing personal data by recognizing the gravity of customer data leakage.

2.2 Privacy calculus theory

The privacy calculus theory has been extensively used in order to scrutinise the trade-off between costs and benefits in regards to information disclosure in the information privacy research (Jozani et al., 2020; Laufer and Wolfe, 1977). Costs typically involve the potential loss of privacy, whereas benefits encompass specific advantages that customers obtain when they expose personal information (Ioannou et al., 2020). The privacy calculus theory suggests that customers engage in a cost-benefit analysis when they are requested to reveal personal information by considering privacy in the economic aspect. The disclosure typically occurs when perceived benefits outweigh privacy risks (Smith et al., 2011). People often place a higher value on benefits and discard the value of their privacy despite reports of an undesirable impact of privacy concerns (Jiang et al., 2013). Privacy calculus serves as a robust framework in the context of hospitality and tourism. Ioannou et al. (2020) asserted that the theory highlights personalization, rewards, costs, and relevant benefits as the major considerations of information disclosure.

The evolving dynamics of personalization and data collection challenge simplistic views of customer behaviour in the hospitality industry. Assessing the costs of data sharing becomes increasingly complex for customers, because consequences are hard to predict (Yu et al., 2022). The relevant parties who deal with customer data also find difficulties regarding privacy issues (Degirmenci, 2022). Privacy studies in hospitality and tourism typically concentrate on initial actions, such as booking and switching intentions. There is a limited amount of exploration in regards to the customer's perceived benefits of sharing personal information while staying at hotels (Ioannou et al., 2020; Moon et al., 2022). On the one hand, customers are wary of data vulnerability; therefore, they hesitate to share extensive personal information, which impacts their privacy risk, concern, and experience during their stay. On the other hand, there could be a trade-off between the perceived benefits of sharing personal information and the risks associated with data vulnerability (Xu et al., 2011). In this trade-off, customers may weigh the advantages of personalized services and enhanced experiences against concerns about information disclosure. This dynamic illustrates the complex decision-making process customers face when deciding whether to share their personal information with hotels. As a result, hotels are shifting focus from data collection to ensuring the secure handling of customer information while offering special benefits to their guests (Ryu and Park, 2020; Yu et al., 2022). This study explores the implications of data vulnerability within the privacy calculus theory instead of solely addressing the initial concerns about information disclosure. A conceptual model was developed in order to understand the influence how data vulnerabilities affect privacy risk and concern and subsequently the hotel guests perceived benefits of sharing personal data.

3. Hypotheses and research model

3.1. Impacts of data vulnerability on privacy risk and concern

The APCO model was adopted in order to investigate the impact of data vulnerability and privacy risk and concern on perceived benefits of hotel customers in this research. Dinev et al. (2015) stated that the APCO framework offers a comprehensive macro perspective that outlines the relationships between the antecedents and outcomes of privacy concerns. Smith et al. (2011) suggested that the framework should be continually refined in order to verify its generalizability across various study contexts. Scholars can consider incorporating an expanding set of antecedents and outcomes into a model applicable. We have developed and introduced a modified APCO framework specifically tailored to address the context of hotel data privacy (Figure 1). This framework focuses on key antecedents such as data access and data breach vulnerabilities, perceived privacy concern, and associated risks as mediators. The outcome is measured in terms of the perceived benefits of sharing personal data within the hotel industry.

Data vulnerability is considered as a stimulus that leads to the emergence of privacy risk and concern in the hotel industry (Yu et al., 2022). If a hotel's reservation system is not well-managed, a customer's personal details may be unlawful accessed. This fosters customers to have a certain concern about identity theft. A widespread data breach can also expose extensive amount of customer data, which can heighten privacy risk and concern (Moon et al., 2022). In this study, perceived privacy risk refers to the subjective assessment that individuals make regarding the potential negative consequences or harm that may result from the unauthorized access or misuse of their personal information (van der Schyff et al., 2020). It involves evaluating the likelihood and severity of these potential consequences. On the other hand, privacy concern is defined as anxiety customers feel about the potential misuse of their personal information (Jozani et al., 2020). It reflects individuals' cognitive response and feelings of unease about the collection, use, and disclosure of their personal information. The customer's perceived risks or concerns about information privacy intensify in situations where hotel customers become aware of the misuse of their personal information or are informed about data leakage incidents from hotels. This heightened awareness in conjunction with the perception of being potential victims of personal information misuse contributes to an increased level of perceived privacy risk and concern among hotel customers (Degirmenci, 2020; Jozani et al., 2020). The following hypotheses are proposed, which consider the discussion above.

H1a: Data access vulnerability significantly influences perceived privacy risk.
H1b: Data breach vulnerability significantly influences perceived privacy risk.
H2a: Data access vulnerability significantly influences perceived privacy concern.
H2b: Data breach vulnerability significantly influences perceived privacy concern.

3.2. Impacts of privacy risk and concern on perceived benefits of sharing personal data

This research explores how the hotel customer's perceptions of privacy risk and concern shape the perceived benefits that are associated with sharing personal information by adhering to the APCO framework. Privacy risk within the hotel privacy context is defined as the potential and severity of personal information loss that stems from the opportunistic actions of external entities (Moon et al., 2022). For example, a hotel guest's credit card information that is exposed to unauthorised access by malicious actors who intend to exploit it for fraudulent transactions embodies a tangible privacy risk, which introduces a real possibility and significant severity of financial harm to an individual.

Privacy concern within the hotel context also introduces unique considerations that warrant a comprehensive examination given the specific type of information that is requested, such as biometric data and the methods that are employed for its collection, such as via reservation systems (Yu et al., 2022). This encapsulates the customer's concerns or perceptions in regards to the personal information that they provide to various hotel services (Mousavia et al., 2020). For example, a hotel that uses a facial recognition system for check-in purposes may activate privacy concerns among their customers. The collection of biometric data via this type of technology raises questions about how the information will be stored, who will have access to it, and the potential for unauthorised use (Ioannou et al., 2020). Customers may express a certain degree of anxiety that is related to the security and privacy implications of having their facial features stored in the hotel's database. These concerns can influence their willingness to share this type of personal information, which consequently impacts their overall experience and satisfaction with the hotel's services (Degirmenci, 2020).

The privacy paradox highlights a crucial gap between an individual's concern and perceived risk about privacy and their actual behaviour when sharing personal data, which is in contrast to the privacy calculus theory (Gerber et al., 2018). Consumers sometimes take minimal actions in order to safeguard it despite expressing substantial worries about the privacy of their information (Choe and Ki, 2021). Some studies revealed examples where individuals are willing to share their personal information in return of insignificant incentives, such as a piece of chocolate (Happ et al., 2016). Nevertheless, the existence of the privacy paradox has been a subject of debate. For instance, Baruh et al.'s (2017) study indicated that users who express higher privacy concerns were in fact less inclined to share their personal information online and revealed less information in the online privacy management context. This fact generally aligns with the predictions of the privacy calculus theory. This research seeks to predict the hotel customer's evaluations of the benefits that concern sharing personal information by building upon the privacy calculus theory and the APCO model. We present the following hypotheses in the hotel privacy management context, which is consistent with the previous research in the privacy domain (Jozani et al., 2020; Ryu and Park, 2020).

> H3a: Perceived privacy risk exerts a significant influence on the perceived benefits of sharing personal data.
>
> H3b: Perceived privacy concern exerts a significant influence on the perceived benefits of sharing personal data.

3.3. Hypotheses for the configuration model

Woodside (2014) introduced an insightful perspective in regards to examining relationships among various factors in the research. He proposed that the researchers can uncover meaningful outcomes by strategically combining different constructs, which are also known as *configurations* or *causal recipes*. This study attempts to investigate the intricate interplay between certain causal conditions specifically the vulnerability of data and the associated risks and concerns in regards to privacy when customers stay at hotels by building on this foundation. We are particularly interested in understanding how these factors influence what customers perceive as the benefits of sharing their personal data.

Each antecedent or contributing factor is defined by the characteristics of other predictors in the analysis in the framework of fsQCA (Woodside, 2014). This means that any given factor can either positively or negatively impact the desired outcome, and this effect depends on the specific nature of other factors that it interacts with (Wattanacharoensil et al., 2024). For example, data breach vulnerability and data access vulnerability in combination may significantly affect a hotel guest's benefits of sharing personal data (Yu et al., 2022). The combination of data vulnerability factors will possibly diminish the perception of benefits in regards to exposing personal data considering this. This characteristic reflects the equifinality principle by signifying that achieving desired outcomes is possible via various potential means or the combinations of causal factors (Woodside, 2017). We propose the following hypotheses in order to explore the configuration effects given the literature that is mentioned above and arguments on the fsQCA. Figure 1 also visually represents the proposed net effect and the configurational models.

> H4 (model A): Data vulnerability, which includes data access vulnerability, has a significant effect on the perceived benefits of sharing personal data.
>
> H5 (model B): Perceived privacy risk and concern, which includes perceived privacy risk and perceived privacy concern, have a significant effect on the perceived benefits of sharing personal data.
>
> H6 (model C): Data vulnerability, which includes data access vulnerability, and perceived privacy risk and concern, which includes perceived privacy risk and perceived privacy concern, have an optimum combination effect on the perceived benefits of sharing personal data.

Insert Figure 1 here

3.4. Necessary condition analysis (NCA)

Dul (2022a) stated that there has been a notable surge in the adoption of the NCA within the field of tourism and hospitality research. The NCA, which is an innovative methodology that is grounded in necessity logic, aims to pinpoint indispensable conditions that must be satisfied for a desired outcome to materialise. According to Meeprom et al. (2023), the presence of these necessary conditions is pivotal for the desired outcome, but their mere existence does not ensure success. Success is instead contingent upon the simultaneous presence of all necessary conditions within a specific configuration (Richter et al., 2020). Hauff et al. (2021) aptly characterise necessary conditions as *essential* or *must have* factors.

Necessary logic asserts that an outcome or a specific level of an outcome can be attained only if the requisite determinant is present or available to a particular degree, which differs from sufficiency logic (Fakfare et al., 2024; Meeprom et al., 2023). For instance, the vulnerability of data access may be deemed necessary, which is not invariably sufficient, for customers to perceive benefits in a hotel setting. Less privacy concern can contribute to a hotel customer's benefit perception if they perceive this condition. Achieving a specific outcome requires the satisfaction of a necessary factor, which is in contrast to sufficiency logic, whereas other elements can compensate if certain conditions cannot be met. The previous studies, such as Richter et al. (2020) and Wattacharoensil et al. (2024) expressed necessity logic via the NCA by stating that 'X is a prerequisite for Y' or 'Y needs X to occur.' In other words, Y cannot be achieved as a desired outcome if X is not present. We propose the following hypotheses in the context of hotel data privacy management, which are based on the literature and the discussion in regards to the NCA that are mentioned above.

> H7: Data vulnerability is a necessary condition for perceived privacy risk and concern.
> H8: Privacy risk and concern is not a prerequisite for the perceived benefits of sharing personal data to occur.

3. Methodology

3.1. Composition of the measurement items and data collection procedures

The measurement items that were utilised in this research were derived from the existing literature on hotel privacy and customer data management. Data access vulnerability and data breach vulnerability were each assessed using three items, which were based on Martin et al.'s (2017) study. Perceived privacy risk was evaluated using four items that were adapted from Xu et al. (2011), whereas perceived privacy concern was measured using five items that were modified from Mousavi et al. (2020). Finally, the perceived benefits of sharing personal data were developed based on six items that were verified by Ryu and Park (2020). All measurement items were derived from the existing literature; thus, their validity and reliability were established. However, they were further tested in the hotel privacy management context. A 7-point Likert's scale, which ranged from (1) *strongly disagree* to (7) *strongly agree*, was employed.

The target population of our study was South Korean travelers who have stayed at a chain hotel within the past two years. An online survey was conducted for the data collection by using a professional research firm in South Korea. The company distributed the survey invitations by email to their panels based on the random sampling method. Only individuals who were qualified via a series of screening questions were led to participate in the survey. The survey was specifically designed to collect the responses from people who answered yes to the following 2 questions. *Have you stayed at a chain hotel? When was the last time you stayed at a chain hotel?* We retained 429 responses for our data analysis after ruling out responses that were useless due to missing values and short response times.

The descriptive results reveal that the gender ratio is well balanced, which included 49% male respondents and 51% female respondents. Most of the respondents (70%) attained an undergraduate degree, which was followed a postgraduate degree (17%), and an associate degree and lower (13%). The majority of the respondents were between 51 years old and above (26.3%), which was followed by 31-40 years old (25.6%), 41-50 years old (24.7%), and 21-30 years old (23.3%). The majority of respondents earned between $3,000-$5,000 (38.9%) in regards to their monthly incomes, which was followed by the respondents who earn less than $3,000 (28%), $5,000 and $8,000 (23.3%), and $8,000 or higher (9.8%).

3.2 Analytical processes

This study used multi-approaches in order to verify the research hypotheses. We followed Manosuthi et al.'s (2022) suggestion and divided the dataset into two portions, which included a training sample (80%) and a testing sample (20%). The training data was utilised for the model's estimation, whereas the testing set was utilised for model's evaluation in regards to its usability. Second, we opted for a composite-based SEM; hence, the Generalized Structured Component Analysis (GSCA$_M$) was employed. This method allows for an in-depth examination of the individual components and its validity within our study, which takes the shared and unique parts of the measurement items, such as how the factor-based SEM deals with measurement errors into account (Hwang et al., 2017). The validity and reliability measures that were obtained from the GSCA$_M$ were also used in order to assess the reliability and validity for the NCA (Richter et al., 2020). Third, the linear combination scores were calibrated using the standardised scale, and they were used across the analysis processes. Next, a single necessary condition analysis was conducted using R with the NCA Package (Dul, 2022b). The fsQCA was subsequently implemented in order to further explore how various precursors collectively contribute to the outcome. The QCA Package in the R programming environment was used in order to perform the fsQCA (Dusa, 2019). We removed the maximum ambiguity cases, and the membership score = 0.5. The adoption of these multi-procedures is vital, because it enables us to gain a comprehensive understanding of the multifaceted relationships among data vulnerability and perceived risk/concern in regards to influencing the perceived benefits of sharing personal data in the hotel privacy management context.

4. Results

4.1 Model assessment and the results of net-effect analysis

The GSCA$_M$ was adopted as a primary estimator in order to assessment the measurement model. The findings showed that all factor loadings and the AVE scores were above the threshold of 0.5, which thereby verify convergent validity. As the reliability values, which included Cronbach's alpha and Dijkstra-Henselers rho_A, were greater than 0.7. This confirmed the model's internal consistency, which is illustrated in Table 1. The discriminant validity was further assessed, and the advanced heterotrait-monotrait ratio of the correlations (HTMT2) values were generally found to be below the recommended edge (0.85), which thereby validated discriminant validity. No major collinearity issues were found, which considered that the VIF scores were generally below 5 (Hair et al., 2011). The following values were revealed by assessing the model's fit. ($\chi 2$/df = 2.287, RMSEA = 0.066, CFI = 0.966, and NNFI = 0.960). We can summarise that the measurement is valid and reliable as a result of this.

A structural model analysis was performed in order to achieve H1-H3. The results, which are shown in Table 2, revealed that the customer's perceived privacy risk was strongly influenced by data breach vulnerability (b = 0.692), whereas perceived privacy concern was affected by both data access (b = 0.213) and data breach (b = 0.530) vulnerabilities. The results partially support H1 and fully verify H2. We found no significant effects between the relationships between these constructs when we investigated the net-effects of perceived privacy risk and privacy concern on the perceived benefits of sharing personal data; therefore, H3 was not supported.

Insert Table 1 and 2 here

4.2. NCA results

We tested whether the predictors are a necessary condition for the desired outcomes by following Dul's (2016) recommendation for performing a single NCA. First, the data vulnerability factors were included in the model in order to find whether they are necessary parts for perceived privacy risk and concern to occur. Table 3 illustrated that data access (DAV) and data breach vulnerabilities (DBV) were identified as the necessary conditions for perceived privacy risk (PPR) and concern (PPC), which are necessary in degree. DAV and DBV are meaningful determinants of PPR and PPC by considering that their necessity effect size (d) estimates and significant values (Karwowski et al., 2016). For example, data access vulnerability must reach the trigger point of 4.2% and data breach vulnerability must reach 6.1% for the hotel customers to perceived privacy risk at 40.6%. Hence, H7 was fully supported. We found non-significant estimates and a zero necessity effect size when examining whether PPR and PPC are a prerequisite for the perceived benefits of sharing personal data, H8 was therefore supported. Figure 2 displays the scatter plots for each identified relationship.

The simultaneous analysis of the net-effects and the NCA further revealed intriguing results. Table 4 depicts that the four possible conditions that were not identified in the earlier SEM studies were exposed. These conditions are necessary but insufficient, necessary and sufficient, unnecessary but sufficient, and unnecessary and insufficient. The DBV was found to be the variable that was necessary and sufficient for the PPR, which means that that the DBV must be present, and the increase in the DBV also enhances the chances for the PPR to develop. The DAV becomes the variable that is necessary for the PPR, but it is an insufficient condition. The result implies that the DAV must be available for the PPR to occur, but the increase in the DAV will not influence affect the level of the PPR. The DBV and DAV were found to be necessary and sufficient conditions for the PPC to occur and develop. The PPR and PPC were surprisingly found to be unnecessary and insufficient conditions for the PB. The results are further discussed in the discussion and implication section.

Insert Table 3 and 4 here

Insert Figure 2 here

4.3. Results of configuration effects

The fsQCA was performed in order to determine the causal relationships (configurations) that develop the desired outcomes in order to achieve H4-H6. We followed Ragin's (2008) suggestion and used intermediate solutions, because they are most interpretable. The possible configurations that present the same outcomes were determined by means of the truth table and applying logical minimization to the table. We followed Pappas and Woodside's (2021) technical note on the fsQCA and set the inclusion of sufficiency (inclS) and the proportional reduction inconsistency (PRI) at a minimum threshold of 0.7. The PRI is an alternative method that improves the clarity and reliability of understanding relationships between data sets. It helps ensure that the observed relationships especially in cause-and-effect scenarios are consistent and meaningful by reducing confusion from overlapping or contradictory information (Pappas and Woodside, 2021).

We created the truth table in this research in order to show the combination of the presence and absence conditions for the hypothesised models. Table 4 illustrates all possible configurations for the development of the PB. The findings show that intricate combinations among data vulnerability and perceived privacy risk and concern exist beyond what was exposed from the result of a traditional net-effect analysis for hotel customers to perceive the benefits of sharing personal data. Model A shows that the DAV should be present, which is recipe 1, for the PB to develop, whereas the DBV is not required, which is recipe 2. Model B illustrates the combination of the presence of the PPC and the absence of the PPR for the PB to enhance. Moreover, three recipes were found when identifying the optimal solution using all data vulnerability and perceived privacy risk and concern factors. The fsQCA results provide the enrichment to the net-effect analysis and the NCA results, which were previously obtained, given that the combined variables can enhance the ultimate outcome of the PB. Table 5 shows that the overall consistency and solution coverage for each hypothesised model reveal that a significant proportion of the outcome was covered by each configuration.

Insert Table 5 here

5. Discussion and implications

This research aims to clarify the role of the data vulnerability factors and perceived privacy risk and concern that affect the perceived benefits of sharing the personal data of hotel guests by adhering to the APCO model. The results of the $GSCA_M$ analysis indicated that the data vulnerability antecedents influence perceived privacy risk and concern, and the data breach vulnerability (DBV) factor has a strong impact on perceived privacy concern. Our research verifies the importance of data vulnerabilities based on the APCO model, which is similar to the previous studies on privacy (Degirmenci, 2020; Ioannou et al., 2020; Jozani et al., 2020; Martin et al., 2017), even though it is within the hotel context. In contrast, while the literature suggests that weaknesses in managing customer data, such as data access vulnerability (DAV) can increase perceived privacy risk (PPR) (van der Schyff et al., 2020; Xu et al., 2011), our study did not find DAV to be a primary antecedent leading to PPR. The DBV was instead found to significantly affect the PPR. One possible reason to explain this finding is that highly sensitive data, within the hotel sector, such as credit card details and personal identification are typically handled by the hotel staff (Yu et al., 2022), the consequences of breaches can therefore be perceived as severe. The severity of perceived losses when staff handle personal data stems from several factors (Mohd et al., 2019). Human error can result in significant breaches that expose sensitive information to unauthorized parties, leading to financial loss, identity theft, and legal consequences (Yu et al., 2022). Furthermore, intentional misuse or theft by employees can cause direct harm to customers, such as fraudulent transactions or personal identity exploitation (Moon et al., 2022). Automated systems, designed with robust security protocols and monitoring, minimize these risks by ensuring consistent adherence to security measures, thereby reducing the likelihood and impact of breaches (Berezina et al., 2019).

Breaches in the hotel sector also tend to receive a substantial amount of public attention, which increases the perceived risk among customers. Research by Ho et al. (2023) indicates that exposure to media reports about data breaches leads individuals to perceive higher risks and adopt protective behaviours. The hotel industry's regulatory environment also often emphasises the prevention and management of breaches by prioritizing the DBV as a critical area of focus (Elphick, 2024). The sector's technological integration with various online services expands potential vulnerabilities, which makes breaches a more apparent risk and a concern in this study's domain. However, this study further reveals that no significant relationship is found between the PPR, PPC, and perceived benefits of sharing personal information (PB). These findings can be anticipated due to a mix of factors. For example, customers may perceive the benefits of personalised services, financial offers, and convenience that come with sharing personal data as outweighing the privacy risks/concerns. This trade-off can lead to a weaker connection between their privacy risk, privacy concern and the perceived benefits of data sharing, which is based on the privacy calculus theory (Jozani et al., 2020). In addition, hotel guests might see data sharing as an inevitable part of modern services. Sharing personal information is often mandatory when making hotel reservations or checking in, which thereby contributes to a weakened link between privacy risk, privacy concern and the PB.

This research identified the antecedents that are required for the occurrence of the PPR and PPC via the NCA analysis. Both data vulnerability factors, which included the DAV and DBV, were interestingly determined as being necessary conditions for the development of perceived privacy risk and concern, even though they are necessary in degree. The DBV was found to be necessary and sufficient for the occurrence of the PPR and PPC. The guest's perception in regards to the DBV may arise from a lack of confidence in the security policies or data privacy management (Moon et al., 2022). Transparent communication about customer data protection procedures could be emphasised in order to overcome this issue. The DAV is a necessary condition, but it alone is insufficient in order to develop the PPR. The result implies that the DAV is indispensable, but it is not the sole element in regards to determining the perception of privacy risk. Other threat perceptions concerning data security must also be present in order to create a privacy risk perception. In this context, a threat refers to the subjective assessment of the probability a harmful event, which influences individuals' intentions and behaviours to protect themselves (Vacondio et al., 2021). On the other hand, risk is the possibility of harm or loss (Tiwari and Omar, 2023). Therefore, for the perception of privacy risk (PPR) to be developed, guests must not only be aware of vulnerabilities like DAV but also recognize the presence of other threats that could exploit these vulnerabilities, leading to a perceived potential risk. On the contrary, the DAV is both necessary and sufficient for the PPC to occur. If hotel guests perceive that their personal data is inadequately accessed, this perception alone is enough to produce substantial privacy concerns. Furthermore, the PPR and PPC were discovered as being unnecessary and insufficient for the PB. The result implies that hotel guests might recognise the rewards of data sharing, which is regardless of their privacy concerns or risk perceptions. This is consistent with the results of the net-effect analysis that was presented earlier in this study.

The net-effect analysis and NCA findings offer comprehensive insights into the antecedents → privacy concerns → outcomes (APCO) in the hotel data management context, but the combination of the data vulnerability and privacy risk and privacy concern factors can yield meaningful results. The findings from the fsQCA substantiate the idea of equifinality, which shows that certain core conditions can contribute to the desired outcomes (PB). The intermediate configurations identified by the fsQCA shed light on the complex relationships among the constructs within the APCO model. The presence of the DAV in conjunction with the absence of the DBV emerge as the key determinants that drive the PB, which is illustrated in model A. Individuals are likely to appreciate the benefits of data sharing when they feel that their personal data is accessible but secure from breaches. These results are in line with the previous privacy research, such as Martin et al. (2017) and Moon et al. (2022). The presence of PPC alongside with the negation of the PPR were found to enhance the PB, which is shown in model B. Hotel guests might be more proactive in regards to sharing data under the belief that it is being safely and responsibly handled when they are concerned about their privacy but do not perceive a direct or significant risk with it. These identified elements additionally emerged from the previous hotel privacy studies (Moon et al., 2022; Yu et al., 2022), which therefore reinforce our understanding of the factors that affect the guest's PB in the hotel privacy domain.

Lastly, three configurations that affect the PB were revealed, which are shown in model C. Configuration 1 (~DBV*~PPR*~PPC) indicates that the absence of DBV, PPR, and PPC can collectively foster the PB. This implies a situation where a lack of general sense of perceived risk and privacy concern encourages the guests to share their personal data. Hotel guests may take it for granted that hotels will deliberately protect their personal data while accepting benefit offers from a hotel. Configuration 2 (~DAV*~DBV*PPR*PPC) suggests the absence of both types of vulnerabilities, which include the DAV and DBV, along with the presence of perceived risk and concern possibly will lead to the PB. This configuration suggests that even in the absence of direct vulnerabilities, the ongoing concern and perceived risks that are related to privacy can motivate individuals to engage in behaviours that protect their privacy. There is a need to address their concerns and promote the transparency of privacy practices beyond ensuring robust security measures. Finally, configuration 3 (DAV*DBV*PPR*PPC) reflects a complex scenario where individuals might still perceive benefits when all data vulnerability and perceived privacy risk and perceived privacy concern factors exist in the APCO framework. This might occur when hotel guests recognise robust risk mitigation efforts and weigh the value of personalised services against potential threats, which leads to a decision to share data (Happ et al., 2016). The decisive factor is often the individual's assessment of an organization's commitment to safeguarding their privacy over their data in a situation where the PPR and PPC are realised. The fsQCA results indicate that the data vulnerability, perceived privacy risk, and perceived privacy concern drivers can lead to developing the PB in the hotel context, which is aligned with the previous findings (Moon et al., 2022). In summary, the fsQCA solutions that result from the three models further support the integration particularly the antecedents → privacy constructs→ outcome and the privacy calculus theory as fundamental grounds (Ioannou et al., 2022), even though not all factors are necessary for the manifestation of the PB.

5.1. Implications for theory

This research offers significant contributions to the body of knowledge in the hotel privacy management context. First, this study successfully conceptualises the antecedents, which include data breach and data access vulnerabilities, for privacy risk, privacy concern, and it explores the relationships among the constructs that lead to the desired outcome (PB) by applying the APCO framework (Smith et al., 2011). This study contributes to the privacy-related literature within the hotel industry context by adopting the privacy calculus theory as a theoretical ground (Jozani et al., 2020; Laufer and Wolfe, 1977). It highlights the elements that hotel guests *must* and *should* consider in the trade-off between the costs and benefits of sharing personal information. The guests' perceptions in regards to privacy risk and concern are increased when they lack confidence about data privacy management in hotels (Yu et al., 2022). The study's findings demonstrate that increased privacy risks/concerns weaken the connection between the perceived privacy risk and privacy concern and the benefits of sharing personal data. This study provides an insightful understanding into hotel privacy dynamics by applying the privacy calculus theory and the APCO framework.

Second, this research adopted the $\mathrm{GSCA_M}$ as a main estimator, which is due to its robust procedures in regards to controlling measurement errors, in order to perform the net-effect analysis (Hwang et al., 2017). The latent scores were also calculated and used in the subsequent analysis. Furthermore, this study follows the study by Dul (2016) in regards to conducting a new NCA in order to determine the single necessary condition(s) for the occurrence of the outcome (PB). This advanced method offers greater explanatory power for the essential elements by specifying whether condition X is necessary in kind or in degree, whereas the necessary conditions that were obtained from the fsQCA revealed only the necessary conditions in kind. The necessary conditions in degree for perceived privacy risk and privacy concern were identified, which included data access and data breach vulnerabilities, in this research. The simultaneous analysis of the net-effect and NCA additionally allows us to determine what conditions are necessary and/or sufficient in order to achieve the PB outcome. This research identified four possible categories of conditions for the PB to manifest, which included necessary but insufficient, necessary and sufficient, unnecessary but sufficient, and unnecessary and insufficient. This advanced approach provides a new angle for the research findings as well as offers a distinction between the variable types, such as necessary and/or sufficient in regards to influencing the PB outcome.

Another significant contribution in this research is the in-depth exploration of the complexity theory in the hotel data privacy context and the examination of alternative paths to the outcome via the fsQCA. The desired outcome (PB) can be formulated based on the complex interaction of the antecedents/constructs; therefore, this study identified certain fsQCA configurations as potential solutions, which are shown in Table 5. The results verify the importance of the data vulnerability factors, privacy risk, and concern for the PB. Hence, these findings determine the necessary and sufficient constructs in regards to establishing the PB as well as also enhance the APCO framework (Smith et al., 2011) and the privacy calculus theory (Jozani et al., 2020; Laufer and Wolfe, 1977). These elements are crucial whether individually or combined in regards to promoting the PB within the hotel data privacy context.

5.2 Implications for practice

This study identifies how data vulnerability affects privacy risk and the perceived benefits of sharing personal data using robust frameworks from a practical perspective, which include the APCO and privacy calculus theory, and it provides tangible benefits to hands-on workers in the hotel industry. First, the complacent information management can lead to an exposure to crime; thus, it is necessary for hotel establishments to thoroughly educate their employees about personal information protection and establish reliable systems in order to prevent potential breaches. It was revealed in this study that weaknesses in data management can result in the heightened perceived risk/concern of hotel guests. If a proper security system is not in place, it raises the customer's perceived privacy risk and privacy concern and subsequently affects a hotel's reputation. A comprehensive approach that encompasses education and robust security measures is therefore crucial.

Second, the privacy calculus theory suggests that customers are often willing to share personal information if they gain benefits in exchange even without fully understanding how their data will be used or misused. Thus, hotel executives should develop strict policies on consent management, which hotel guests can decide on what aspects of personal information they would like to share (Mohd et al., 2019). A clear explanation should be provided regarding how each piece of information is utilised and for what purpose in the process of personal data collection (Guo and Li, 2022). This practice can be visually demonstrated in the form of detailed privacy notices or interactive consent forms, such as a short virtual film and/or an online link to hotel privacy regulations. The goal is to ensure transparency and build trust with the guests. Privacy and regulations can be more effectively communicated by implementing these policies, which thereby benefit both the practitioners and guests in the hotel industry.

Third, the NCA results revealed in this research offer a new perspective into the hotel data privacy context. For example, the NCA findings revealed that for hotel guests to realise a privacy concern at 68.9%, their perception in regards to data access must reach 4.2% and 6.1% for data breach vulnerabilities. These findings demonstrate a very low tolerance among hotel guests in regards to data privacy and security risks. The guest's sensitivity to data vulnerabilities highlights the need for hotels to adopt firm data protection measures and effectively communicate the privacy policies in order to maintain trust (Park and Lehto, 2021). These recommendations provide practical guidelines for hotel professionals to manage data privacy in an efficient way.

Fourth, the joint analysis between net-effect and NCA offers valuable insights for hotel marketing managers and executives. The study's findings highlight that data breach vulnerability has an essential role in the manifestation and enhancement of perceived privacy concern. Marketing strategies can emphasize robust data security measures, such as encryption protocols and secure payment systems to instil confidence in potential guests. As Martin and Murphy (2017) claimed, transparent communication about data protection practices, including how guest information is collected, stored, and utilised, can build trust and loyalty. Recognizing that hotel guests expect a risk-free experience from data breaches, hotels can go the extra mile by highlighting initiatives focused on offering benefits that prioritize guest privacy and security. These initiatives may include functional incentives, such as access to additional features in a hotel app (e.g., early check-in/late check-out options, room upgrades, personalized travel itineraries), which enhance the convenience and personalization of the guest experience. Additionally, psychological incentives, such as exclusive services (e.g., dedicated concierge access, private lounges, VIP event invitations), can create a sense of privilege and exclusivity. As Shoemaker and Lewis (1999) stated, these non-monetary incentives not only enhance the guest experience but also foster a deeper emotional connection and loyalty to the brand. Incorporating value-adding strategies that move beyond financial incentives aligns with the literature and effectively enhances guest loyalty (Chang and Wong, 2018).

Finally, the fsQCA findings provide crucial marketing implications for hotel managers to navigate the complex landscape of data management and privacy concerns. For instance, considering the results of the optimal solution of configuration 1 (~DBV*~PPR*~PPC), hotels can emphasize their commitment to privacy protection by highlighting transparent data handling practices to mitigate concerns and enhance benefits of sharing data. For example, hotels can implement comprehensive privacy policies and display them on their websites, showcasing their dedication to safeguarding guest data, while offering attractive incentives for guests who share personal data. In Configuration 2 (~DAV*~DBV*PPR*PPC), where ongoing privacy concerns motivate guest behaviours, hotels can implement initiatives that actively address and alleviate these concerns, such as establishing a ‘Privacy Information Centre’. This information centre within the hotel premises provides guests with access to comprehensive resources about data privacy, including informative brochures, FAQs, and contact details for privacy support staff, offering a transparent and easily accessible channel for addressing privacy risks and concerns. Additionally, Configuration 3 (DAV*DBV*PPR*PPC) highlights the importance of enhancing the value proposition while ensuring data security. Hotels can achieve this by implementing transparent communication strategies to assure guests of their commitment to data privacy and security, such as providing opt-in/opt-out options for data sharing for any personalised service offered. For example, mobile apps that allow guests to customize their stay preferences, such as housekeeping schedules or restaurant reservations, can be developed to offer a personalised guest experience, while ensuring data security through encryption and authentication measures. Overall, leveraging insights from fsQCA allows hotels to develop targeted marketing strategies that prioritize security measures, while navigating the complexities of data privacy management that enhances guests’ perceived benefits in the hospitality industry.

6. Research limitations and future agenda

This research is subject to certain limitations. First, this study investigated the effect of a set of antecedents particularly in terms of data access and data breach vulnerabilities on hotel guests perceived privacy risk and privacy concern. However, several antecedents were identified in the extant privacy-related literature, which included hospitality and tourism as potential factors that affect privacy concerns (Tiwari and Omar, 2023). Hence, the future studies are encouraged to explore the effects of other antecedents, such privacy awareness, privacy knowledge, and different types of trust on perceived privacy risk and privacy concern by adhering the APCO model (Darabi et al., 2023). Second, the data privacy policies and regulations of hotels may vary across different regions/countries and hotel types. Comparing the privacy policies in different regions/countries and/or hotel types would be an interesting agenda. Lastly, this study adopted the $\mathrm{GSCA_M}$ as a principal estimator in regards to obtaining results for the net-effect analysis and calculating the latent scores in order to perform the

NCA. The $GSCA_M$ is considered a valid and robust approach (Hwang et al., 2017), but the future research may attempt to compare results by using other estimators, such as maximum likelihood or partial least squares in order to verify the model's predictive validity.

References

Ajzen I and Fishbein M (1980) *Understanding Attitudes and Predicting Social Beha*vior, Prentice-Hall Inc., Englewood Cliffs, NJ.

Baruh L, Secinti E and Cemalcilar Z (2017) Online privacy concerns and privacy management: A meta-analytical review. *The Journal of Communication* 67(1): 26–53.

Berezina, K., Ciftci, O., & Cobanoglu, C. (2019), "Robots, artificial intelligence, and service automation in restaurants. In *Robots, artificial intelligence, and service automation in travel, tourism and hospitality* (pp. 185-219). Emerald Publishing Limited.

Chang H H and Wong K H (2018) Consumer psychological reactance to coalition loyalty program: price-consciousness as a moderator. *Service Business, 12:* 379-402.

Choe Y and Ki H (2021) Risk perception and visit intention on Olympic destination: Symmetric and asymmetric approaches. *Journal of Vacation Marketing* 27(3): 314-329.

Culnan MJ and Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10: 104–115.

Darabi H, Rasoli-dehkharghani P and Kordani H (2023) Iran's destination image, incremental analysis of safety and security. *Journal of Vacation Marketing.*

Dinev T, McConnell AR and Smith HJ (2015) Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research* 26(4): 639–655.

Dogra N and Adil M (2024) Should we or should we not? Examining travelers' perceived privacy, perceived security and actual behavior in online travel purchases. *Journal of Vacation Marketing* 30(1): 123-142.

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

Dul J (2022b) Necessary condition analysis (NCA) with R. R package. Version 3.2.1 Ed.

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

Elphick D (2024) What is cyber security in the hospitality industry?. *SiteMinder.* Retrieved from https://www.siteminder.com/r/cyber-security-hospitality-industry/

Fakfare P, Manosuthi N, Lee J S, Promsivapallop P, Kang H and Han H (2024) Eliciting small island tourists' ecological protection, water conservation, and waste reduction behaviours. *Journal of Destination Marketing & Management, 32*: 100900.

Gashami JPG, Chang Y, Rho JJ and Park MC (2016) Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Information Development* 32(4): 837-852.

Guo R and Li H (2022) Can the amount of information and information presentation reduce choice overload? An empirical study of online hotel booking. *Journal of Travel and Tourism Marketing* 39(1): 87-108.

Hair JF, Ringle CM and Sarstedt M (2011) PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice 19*(2): 139–152.

Happ C, Melzer A and Steffgen G (2016) Trick with treat - Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior* 61: 372–377.

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* 31(1): 18-36.

Ho F N, Ho-Dac N and Huang J S (2023) The effects of privacy and data breaches on consumers' online self-disclosure, Protection Behavior, and Message Valence. *SAGE Open* 13(3). https://doi.org/10.1177/21582440231181395

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

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

Jiang Z, Heng CS and Choi BCF (2013) Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research* 24: 579–595.

Jozani M, Ayaburi E, Ko M and Choo KKR (2020) Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior* 107: 106260.

Karwowski M, Dul J, Gralewski J, Jauk E, Jankowska DM, Gajda A, et al. (2016) Is creativity without intelligence possible? A necessary condition analysis. *Intelligence* 57: 105–117.

Kim J J and Han H (2022) Redefining in-room amenities for hotel staycationers in the new era of tourism: A deep dive into guest well-being and intentions. *International Journal of Hospitality Management* 102: 103168.

Kim, J., Weldesenbet, E.G.,, Sam, K., Gedecho, E.K., Han, H., & Hong, J. (2024). Re-assessing hotel room performances before and during the pandemic. *Journal of Vacation Marketing*, https://doi.org/10.1177/13567667231211349

Kritzinger E and Smith E (2008) Information security management: An information security retrieval and awareness model for industry. *Computers and Security* 27(5-6): 224-231.

Laufer RS and Wolfe M (1977) Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33: 22–42.

Lee M, Ahn J, Shin M, Kwon W and Back K J (2021) Integrating technology to service innovation: Key issues and future research directions in hospitality and tourism. *Journal of Hospitality and Tourism Technology* 12(1): 19-38.

Manosuthi N, Lee JS and Han H (2022) Investigating residents' support for Muslim tourism: The application of IGSCA-SEM. *Journal of Travel & Tourism Marketing.*

Martin K D, Borah A and Palmatier RW (2017) Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81(1): 36-58.

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

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 AZA, Anuar N, and Ahmad SAPS (2019) Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security* 27(1): 81–100.

Moon H, Yu J, Chua, BL and Han H (2022) Hotel privacy management and guest trust building: A relational signaling perspective. I*nternational Journal of Hospitality Management* 102: 103171.

Mousavi R, Chen R, Kim DJ and Chen K (2020) Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems* 135: 113323.

Pappas IO and Woodside AG (2021) Fuzzy-set qualitative comparative analysis (fsQCA): Guidelines for research practice in information systems and marketing. *International Journal of Information Management* 58: 102310.

Park S and Lehto X (2021) Understanding the opaque priority of safety measures and hotel customer choices after the COVID-19 pandemic: an application of discrete choice analysis. *Journal of Travel & Tourism Marketing* 38(7): 653-665.

Richter NF, Schubring S, Hauff S, Ringle CM and Sarstedt M (2020) When predictors of outcomes are necessary: Guidelines for the combined use of PLS-SEM and NCA. *Industrial Management & Data Systems* 120(12): 2243–2267.

Ryu S and Park Y (2020) How consumers cope with location-based advertising (LBA) and personal information disclosure: The mediating role of persuasion knowledge, perceived benefits and harms, and attitudes toward LBA. *Computers in Human Behavior* 112: 106450.

Shoemaker S and Lewis R C (1999) Customer loyalty: the future of hospitality marketing. *International Journal of Hospitality Management 18* (4): 345–370.

Smith HJ, Dinev T and Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quarterly* 35: 989–1016.

Tiwari V and Omar A (2023) The impact of the hotel star rating system on tourists' health safety and risk perceptions: Study based on tourists' vacation experiences. *Journal of Vacation Marketing.*

van der Schyff K, Flowerday S and Furnell S (2020) Privacy risk and the use of Facebook Apps: A gender-focused vulnerability assessment. *Computers & Security* 96: 101866.

Vacondio M, Priolo G, Dickert S and Bonini, N (2021) Worry, perceived threat and media communication as predictors of self-protective behaviors during the COVID-19 outbreak in Europe. *Frontiers in Psychology, 12:* 577992.

Wattanacharoensil W, Lee JS, 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* 40(2): 109-130.

Wattanacharoensil W, Fakfare P, Manosuthi N, Lee JS, 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* 100: 104823.

Woodside AG (2017) Solving the core theoretical issues in consumer behavior in tourism. In Consumer behavior in tourism and hospitality research (Vol. 13, pp. 141-168). Emerald Publishing Limited.

Xu H, Dinev T, Smith J and Hart P (2011) Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems 12*(12): 798-824.

Yu, J., Moon, H., Chua, B. L., & Han, H. (2022). Hotel data privacy: strategies to reduce customers' emotional violations, privacy concerns, and switching intention. *Journal of Travel & Tourism Marketing, 39*(2), 215-227.

Yu, J., Moon, H., Chua, B., & Han, H. (2024). A new tourism paradigm in the marketplace: Armchair travel and destination experiences. *Journal of Vacation Marketing 30*(1), 58-71.

Table 1: Measurement model assessment

Construct	Indicator	AVE	Reliability (alpha)	$\hat{\lambda}_t$	*t*-value
DAV	I feel anxious about all possible poor management processes of this hotel brand in regards to other people's access to my personal information, such as email address, mobile phone number, company address, and home address that it has collected.	0.896	0.962	0.932	N/A
	I feel vulnerable about all possible poor management processes of this hotel brand regarding others' access to my personal information it has collected.			0.955	48.025
	I feel nervous about all possible poor management processes of this hotel brand in regards to other people's access to my personal information it has collected.			0.951	46.097
DBV	This hotel brand has vulnerable customer information management systems.	0.874	0.953	0.908	N/A
	My personal information that is collected by this hotel brand may be leaked.			0.945	0.038
	My personal information that is collected by this hotel brand is not safely managed.			0.95	0.039
PPR	It would generally be risky to give my personal information to this hotel brand.	0.746	0.923	0.785	N/A
	There would be high potential for privacy loss associated with giving my personal information to this hotel brand.			0.925	18.493
	My personal information could be inappropriately used by this hotel brand.			0.923	18.164
	Providing this hotel brand with my personal information would involve many unexpected problems.			0.818	20.457
PPC	I am concerned that this hotel brand is collecting too much information from me.	0.772	0.942	0.79	N/A
	I am concerned that this hotel brand will use my information for other purposes.			0.895	21.168
	I am concerned that this hotel brand will share my information with other parties.			0.919	21.45
	I am concerned that this hotel brand does not protect the privacy of my information.			0.892	19.253
	I am concerned that this hotel brand allows other users to access my information.			0.877	18.501
PB	By sharing my personal information with this hotel brand, I can get the hotel's latest offers by sharing my personal information with this hotel brand.	0.781	0.955	0.823	N/A
	I am able to access the hotel's relevant offers at the right time by sharing my personal information with this hotel brand.			0.897	27.796
	Sharing my personal information with this hotel brand makes it convenient for me to find the hotel's offers that I need.			0.908	25.272

	Sharing my personal information with this hotel brand can provide me with relevant offers that are tailored to my preferences or personal interests.			0.898	23.595
	Sharing my personal information with this hotel brand can provide me with personalized offers that are tailored to my travel activities.			0.897	21.49
	Sharing my personal information with this hotel brand can provide me with the kind of offers that I might like.			0.879	20.722

Note: DAV = data access vulnerability, DBV = data breach vulnerability, PPR = perceived privacy risk, PPC = perceived privacy concern, PB = Perceived benefits of sharing personal data, and $\widehat{\lambda_i}$ = factor loading.

Table 2: Net-effect analysis

Relationship	Estimate	*t*-value	Std. Err
DAV->PPR	0.070	0.049	0.049
DBV->PPR	**0.692**	**10.217**	0.055
DAV->PPC	**0.213**	**2.741**	0.054
DBV->PPC	**0.530**	**6.822**	0.059
PPR->PB	-0.059	-0.596	0.085
PPC->PB	0.008	0.080	0.089

Note: DAV = data access vulnerability, DBV = data breach vulnerability, PPR = perceived privacy risk, PPC = perceived privacy concern, PB = perceived benefits of sharing personal data, and **bold value** = significant.

Table 3: Single necessary condition analysis

Outcome: PPR	**CE-FDH (d)**	**p-value**	**CR-FHD (d)**	**p-value**	**Triggered level**	**Necessary?**
DAV	0.04	0.000	0.04	0.001	0.042 ->0.406*PPR	**In degree**
DBV	0.04	0.000	0.06	0.000	0.061 ->0.594*PPR	**In degree**
Outcome: PPC	**CE-FDH (d)**	**p-value**	**CR-FHD (d)**	**p-value**	**Triggered level**	**Necessary?**
DAV	0.03	0.025	0.03	0.037	0.042->0.689*PPC	**In degree**
DBV	0.04	0.007	0.03	0.008	0.061->0.689*PPC	**In degree**
Outcome: PB	**CE-FDH (d)**	**p-value**	**CR-FHD (d)**	**p-value**	**Triggered level**	**Necessary?**
PPR	0.00	1.000	0.00	1.000	N/A	No
PPC	0.00	1.000	0.00	1.000	N/A	No

Note: DAV = data access vulnerability, DBV = data breach vulnerability, PPR = perceived privacy risk, PPC = perceived privacy concern, PB = Perceived benefits of sharing personal data, and d = effect size.

Table 4: The four exhaustive conditions of the occurrence and increment of outcomes

Condition/Outcome: PPR	**Sufficient**	**Insufficient**
Necessary	DBV	DAV
Unnecessary	-	-
Condition/Outcome: PPC	**Sufficient**	**Insufficient**
Necessary	DBV, DAV	-
Unnecessary	-	-
Condition/Outcome: PB	**Sufficient**	**Insufficient**
Necessary	-	-
Unnecessary	-	PPR, PPC

Note: DAV = data access vulnerability, DBV = data breach vulnerability, PPR = perceived privacy risk, PPC = perceived privacy concern, and PB = Perceived benefits of sharing personal data.

Table 5: The solution of configuration effect

Outcome: PB	Model A (H4)			Model B (H5)			Model C (H6)			
	Recipe 1	Recipe 2	Full model	Recipe 1	Recipe 2	Full model	Recipe 1	Recipe 2	Recipe 3	Full model
DAV	●		Recipe 1 + Recipe 2					◌	●	Recipe 1 + Recipe 2 + Recipe 3
DBV		◌					◌	◌	●	
PPR				◌		Recipe 1 + Recipe 2	◌	●	●	
PPC					●		◌	●	●	
Consistency	0.889	0.823	0.825	0.857	0.911	0.855	0.890	0.957	0.959	0.879
PRI	0.811	0.721	0.749	0.762	0.836	0.789	0.802	0.764	0.913	0.837
covS	0.571	0.715	0.955	0.695	0.605	0.94	0.592	0.283	0.421	0.839

inclS = Inclusion of Sufficiency, PRI = Proportional Reduction in Inconsistency, covS = Raw Coverage

● = Core condition, ○ = Peripheral condition, ◌ = Absence, Blank = Don’t care, DAV = data access vulnerability, DBV = data breach vulnerability, PPR = perceived privacy risk, PPC = perceived privacy concern, and PB = Perceived benefits of sharing personal data.

Figure 1. Proposed theoretical framework

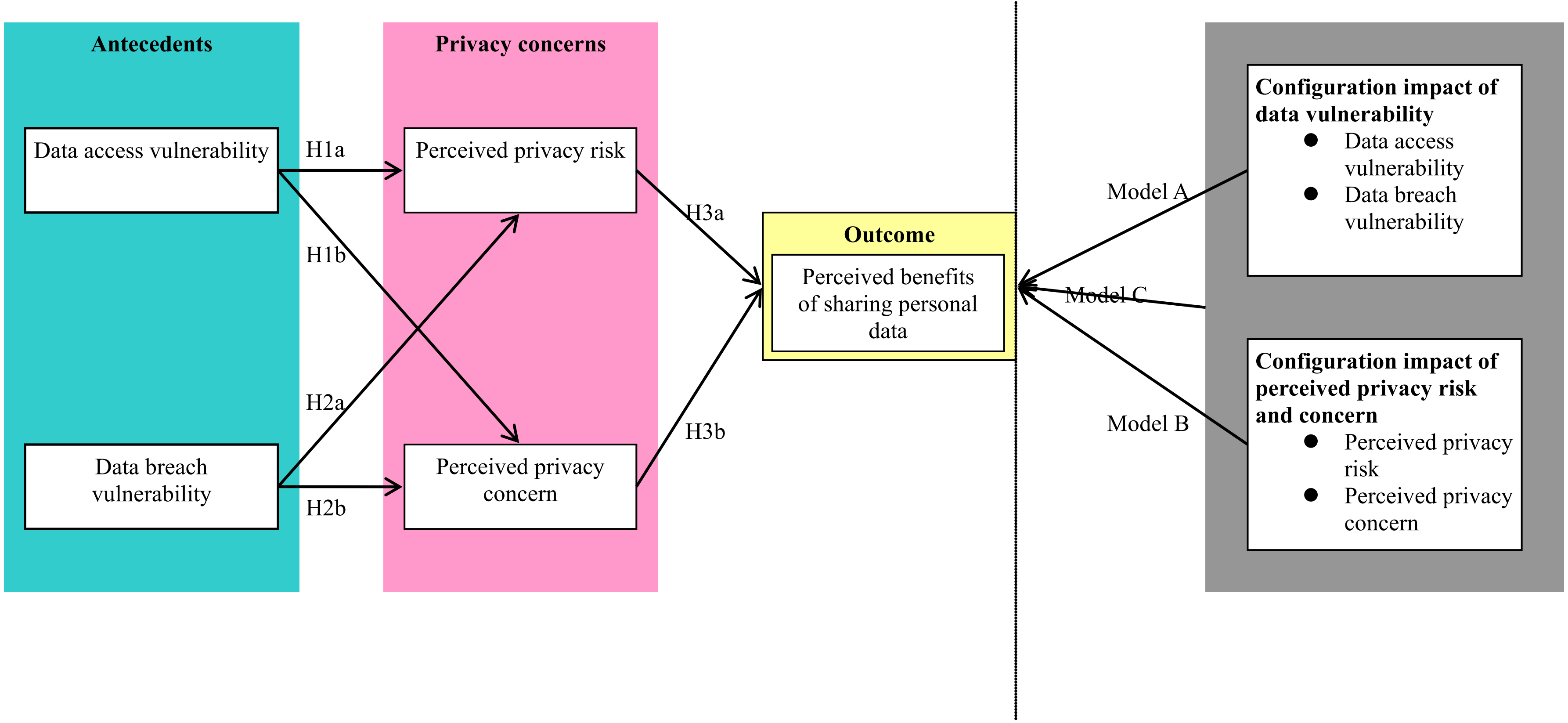
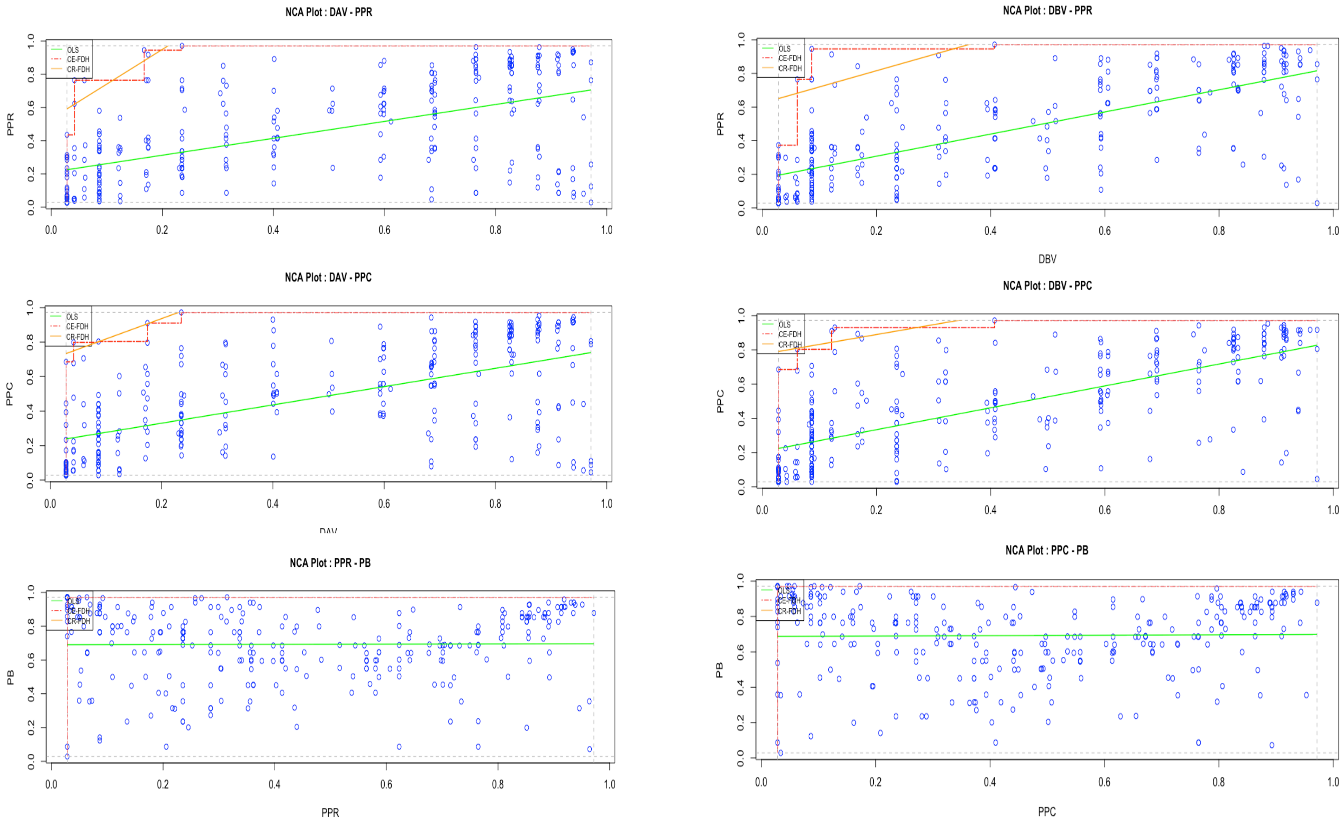

Antecedents
Data access vulnerability
Data breach vulnerability
Privacy concerns
Perceived privacy risk
Perceived privacy concern
H1a
H1b
H2a
H2b
H3a
H3b
Outcome
Perceived benefits of sharing personal data
Model A
Model B
Model C
Configuration impact of data vulnerability
● Data access vulnerability
● Data breach vulnerability
Configuration impact of perceived privacy risk and concern
● Perceived privacy risk
● Perceived privacy concern

Figure 2. NCA plots


NCA Plot : DAV - PPR
NCA Plot : DBV - PPR
NCA Plot : DAV - PPC
NCA Plot : DBV - PPC
NCA Plot : PPR - PB
NCA Plot : PPC - PB
OLS
CE-FDH
CR-FDH
PPR
PPC
PB
DAV
DBV
PPR
PPC