Understanding Privacy Perceptions on Hospitality Apps

Karen Gonzalez Cifuentes, Carlos Mahecha, Anwaya Wadnerkar, Yiyao Wang

Abstract

This study examines user perceptions of privacy and security in mobile hospitality apps, focusing on data collection, policy transparency, and regulatory compliance. Through a survey of U.S. residents, the research identifies significant concerns regarding biometric data collection, location tracking, and smart device usage in hotel rooms. Findings reveal that users prefer clear disclosures and opt-out options, indicating a need for enhanced transparency to build trust. The study highlights user's discomfort with excessive data retention and unauthorized data sharing, emphasizing the importance of robust privacy policies. Insights from this research aim to guide the hospitality industry in implementing better data practices and fostering user confidence. Ultimately, the study contributes to the broader discussion on improving privacy standards and regulatory frameworks in digital hospitality services.

Introduction

The hospitality industry has created various apps to facilitate booking of spaces that require the collection of various user data for certain functionalities. Privacy policies and privacy labels, which are found in app stores, have provided users with information regarding how data is treated and what is collected. Usage of hospitality apps have consistently increased due to their convenience and wide use, however questions regarding user's awareness of data treatment remained as hospitality apps collected sensitive information. With new technology available to better facilitate business processes and guest's needs, more data is being collected. For example, biometric data can now be used for identity verification, which was not possible in the past. Thus, it is important for user's to understand what data is being collected and how it is treated as their expectation of data privacy might be different compared to what new technology has allowed for. By understanding possible misconceptions users have regarding data privacy, areas of weakness in how hospitality apps present privacy information can be identified to be able to provide recommendations for both industry and policy makers. While there has been significant research on the adoption and use of mobile technology by travelers, there is a need for more studies on the long-term impacts of these technologies on travel behavior and experiences (Chen *et al*, 2021) . The literature review performed reveals several key gaps and research opportunities in privacy and data protection within hospitality apps, like the opportunity for clarity in privacy policies regarding newer technologies like AI / IoT devices and applications of biometric data collection, the need for better understanding of user awareness regarding data collection practices and their ability to control their data. The review also highlights concerns about long-term data retention and associated risks, as well as the increasing use of biometric data in hospitality settings, giving us the opportunity to conduct research around the impact of clear disclosure on user comfort levels, the effectiveness of current or potential opt-out mechanisms, the relationship between perceived transparency and user privacy behaviors, and exploring user perceptions of risk related to extended data collection and retention.

Consequently, this study was conducted to analyze and inquire about users' privacy concerns regarding the collection, use, and management of personal data in hospitality apps, focusing on biometric, identifier, geographic, and behavioral data. We want to investigate users' awareness of data collection practices, knowledge of control over their data, and the potential risks associated with excessive data retention and improper access. Thus the following **research questions were posed:**

- **Research question 1:** *How does the clarity of disclosure regarding the use and storage of data in hospitality apps affect users' comfort levels with providing such data?*
- **Research question 2:** *What factors influence users' perceptions of risk associated with long-term data retention by hospitality apps, and how do these perceptions drive opt-out preferences?*
- **Research question 3:** *To what extent does perceived transparency in data management and stronger opt-out preferences correlate with proactive privacy protection behaviors among users of hospitality apps?*

This report discusses in the literature review section the current research that has been done to identify privacy concerns in hospitality apps. The methods section then discusses how the survey was designed and deployed based on the literature review findings to address the research questions identified. The results section will then delve into the findings from the data analysis done on the survey responses, and how the findings answer the research questions. The key findings and inferences section then addresses and highlights interesting points from our results to derive interpretations. The conclusion then discusses what hospitality apps should do in regards to how data is treated.

Literature Review

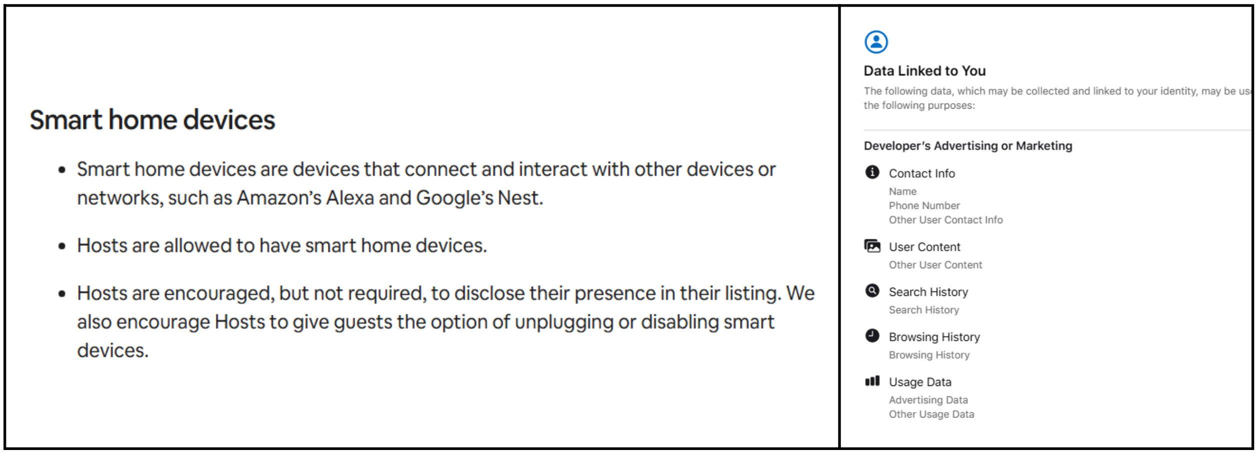
The emergence and impact of hospitality mobile applications have been significant since the rise of smartphones and increasing digitalization of the hospitality industry, where major hospitality companies quickly recognized the potential of mobile apps to reach customers and provide services (Kwon et al, 2013). The impact of these apps on customer experience has been substantial, while also having a great impact from a businesses perspective, bringing improvements over marketing efforts and costs, customer reach, and brand visibility. However, the increased use of mobile technology in tourism has also raised significant privacy concerns. As travelers rely more on mobile devices and apps they generate vast amounts of personal data, including location information, preferences, and behaviors, leading to growing concerns about user security and privacy protection (Chen *et al*, 2021, p.5) and their effects on users' awareness of regulations, potential threats and their impact on user willingness to engage with hospitality mobile technologies, something even more relevant when numerous apps collect sensitive or personal data without sufficient justification or disclosure (Surma et al, 2024, p.21).

Around 2020 Apple introduced in its App Store to help understand an app's privacy practices, mitigate policy ambiguities, and inform users (Surma *et al,* 2024, Zhang *et al,* 2022). Consequently, privacy labels and policies have become a critical aspect of mobile app ecosystems, yet research indicates significant issues with their implementation and effectiveness. A study by Rodriguez *et al.* (2023) revealed substantial discrepancies between privacy label disclosures for iOS and Android versions of the same apps, with 66.5% of analyzed apps showing potential inconsistencies, suggesting a concerning mismatch between what apps disclose in their privacy labels and their actual data collection practices (Rodriguez et al., 2023) and also raising concerns about the apps policies, the depth with which certain topics are addressed (like newer technologies and use case scenarios), and why these are not reflected in the channels provided for that purpose. Krämer (2024) review on apps stores enforcement of privacy policies thro labels suggest how while app stores seem to have significant influence on policy compliance "the privacy labels enforced by app stores partly do not comply with the requirements of the GDPR", consequently non reflecting potential risks and undermining any attempt for transparency. An antecedent of this issue can also be found in Fong (2017) discussing the role of developers and businesses and the responsibility they have to integrate privacy protection principles and standards, sometimes compromised due to the lack of solid requirements by intermediaries and regulation enforcers, like app stores, or the primacy of business related motivations.

Furthermore, a subsequent study by Rodriguez et al. (2024) found that over half of the examined app privacy policies were potentially non-compliant with transparency regulations (GDPR), with some of them for example, explicitly allowing indefinite data retention. These findings highlight the relevance of enhanced regulatory oversight to ensure privacy policies are compliant, clear, and accessible to users (Rodriguez et al., 2024). If these privacy policies and labels, which should be in theory a way to enforce regulations over aspects such as the collection and handling of consumer-related information, contain gaps that could potentially impact user privacy, we must first ask and asses the level of impact of these grey areas, and second, how we might begin to drive change in this regard, largely justifying the nature of this study: understanding user perceptions of applications in one specific sector—hospitality—that highlights the multifaceted nature of the problem and could provide insights for users, policy enforcers, businesses, developers and academics.

Now to start our reflection on users perceptions, seems necessary to state how the complexity and opacity of privacy policies and gaps in regulation present additional challenges, more if we think about the hospitality business, where the collection of personal data is due to operations, regulatory requirements, to understand customer expectations and provide a better experience, as well as to guide marketing campaigns either in-house or through third parties.

Consider, for example, the policies and labels of Airbnb as a case study in privacy challenges within hospitality apps. The platform's community policy, not the policy directly available and referenced in the Apple app store, but an extended policy disclosed on their website, makes no reference to AI-powered devices or technologies and is broad regarding data collection and management by Smart/IoT devices, leaving a significant gap in addressing potential privacy implications for users. This omission/lack of specificity extends to privacy labels, which provide no indication of data that might be collected by AI or IoT devices related to users for purposes like advertising or marketing, raising questions about the comprehensiveness of their data governance framework and the transparency provided to users.



Smart home devices

- Smart home devices are devices that connect and interact with other devices or networks, such as Amazon's Alexa and Google's Nest.
- Hosts are allowed to have smart home devices.
- Hosts are encouraged, but not required, to disclose their presence in their listing. We also encourage Hosts to give guests the option of unplugging or disabling smart devices.

Data Linked to You

The following data, which may be collected and linked to your identity, may be us
the following purposes:

Developer's Advertising or Marketing

Contact Info
Name
Phone Number
Other User Contact Info

User Content
Other User Content

Search History
Search History

Browsing History
Browsing History

Usage Data
Advertising Data
Other Usage Data

Airbnb extended Community policy (left) and Ios privacy labels related to personal data (right)

Given these gaps, we began to recognize the need to better understand the major areas of privacy concern and define the specific criteria that would guide our study around hospitality apps. Significant omissions related to newer technologies, news about personal data exposure, and excessive third-party data usage highlighted the lack of transparency and the importance of focusing our research on the broader issues of data collection, user awareness, and the need for clear disclosures. The following table summarizes the review performed around major areas of privacy concern:

Identifying major areas of concern:

Nema *et al.* 2022	Discussed dominant privacy concerns across multiple app categories: unnecessary permissions, personal information collection, tracking, privacy controls, selling of personal data
Ioannou *et al* (2020)	The authors propose a theoretical model to conceptualize the effect antecedents on travelers' online privacy concerns. This model includes "individual or psychological factors (i.e., disposition to privacy, privacy

	awareness, perceived privacy control, trust), knowledge and experience (i.e., privacy knowledge, privacy experience), (3) contextual factors (i.e., information sensitivity, perceived personalization benefits) and (4) macro-environmental factors (i.e.,privacy protection regulation).” (p.2)
Neo & Teo (2022, p.1843)	The authors discussed four dimensions of information privacy around biometric technology: collection, errors, secondary use, and unauthorized access, and reduced judgement based on the Concern for Information Privacy (CFIP) instrument developed by (Smith, Milberg, & Burke, 1996)
Li (2011, p.466)	Reviews Concerns for Information Privacy (General CFIP) and Specific Concerns for Information Privacy (Specific CFIP) and proposes an integrative framework that includes individual factors such as computer anxiety, need for privacy, personality traits, other factors related to the environment such as culture, government regulations and social norms, and some more specific concerns related to behavioral intentions, perceived privacy risks and benefits and trust.

Going through academic literature, it was possible to identify how consequences of privacy concerns include impacts on personal beliefs (e.g. trust, risk perceptions), attitudes, behavioral intentions, and actual behaviors (Lin, 2011,p.454). However, the relationship between privacy concerns and actual behavior is complex, making it hard to relate aspects like privacy concerns, trust, and risk perceptions with information disclosure, underlining with this several areas in need of further research, like the moderating effects involving privacy concerns (Lin, 2011,p.465).

Despite these complexities, several authors have been able to identify relevant categories to guide their own studies. Nema et al. (2022) identified five dominant privacy concerns across multiple app categories: unnecessary permissions, personal information collection, tracking, privacy controls, and selling of personal data, while Ioannou et al. (2020) identified several individual factors shaping travelers' online privacy concerns, including disposition to privacy, privacy awareness, perceived control, trust, and prior privacy knowledge/experiences, using these concerns to provide comprehensive takes on privacy behavior in digital environments.

Following some of the most relevant concerns identified in academic literature allowed us to consider general and specific perspectives on privacy concerns and reflect on issues like transparency in data collection, adequacy of privacy policies, user awareness of data usage practices, risks associated with long-term data retention, and the effectiveness of opt-out mechanisms. Some of the studies have emphasized how the lack of clear communication and regulatory oversight can difficult user trust and increase perceived risks, particularly with sensitive data like biometrics and geographic location tracking. Drawing from these insights, as a way of defining an inquiry horizon and methodological guideline, we proposed the following categories of concern:

- **Data Collection Concerns:** focusing on the breadth and sensitivity of data collected, including unnecessary permissions, personal information collection, tracking, and lack of transparency about what is being gathered and why.
- **Data Retention and Access:** examining risks associated with long term storage of data, access to it, and how securely it is managed, including concerns about unauthorized access, secondary uses, and insufficient regulatory oversight.
- **User Control and Normative Awareness:** relating to users' ability to manage their data through clear privacy controls, opt-out mechanisms, and understanding of how their data is used, shaped by trust, privacy awareness, and alignment with social and regulatory norms.

Once these categories were defined, we proceeded by identifying and refining specific scenarios on which we would develop our concerns regarding user behavior and understanding of privacy in hospitality apps, and the hypothesis that would guide our research.

Identifying scenarios of inquiry:

Ioannou *et al* (2020, 2021)	Collection of biometric and behavioral data for travel, collection and storage of identifiers, biographic information, and behavioral data.
Liyanaarachchi *et al* (2023)	Collection of biometric data imbalances related to the reduction of individual control impacting consumers' willingness to share information, while also influencing their decisions regarding hotel selection and service access
Neo & Teo (2022)	Physical biometrical privacy, ethical issue regarding the tourist usage of biometrics, information privacy regarding biometric data collection,
Kim et al, 2024	Voice AI, intention to use this technology in hotels, influence on customer intention to stay and compromise of customer control
Sia *et al,* 2023	Geolocation tracking services in mobile travel apps for personalization, user engagement, user trust and acceptability and concerns regarding location accuracy and data misuse.
de Camargo Silva *et al*, 2019	Smart locks, physical locks supported by Iot technologies, the use of blockchain-based systems for smart door locks, potential privacy concerns connecting IoT infrastructure to the blockchain network.
Surma et al, 2024	Excessive data gathering (related to collection of data related to health and fitness privacy labels category) related to potential to misuse of sensitive health information, identity theft, fraud and unwanted exposure of private data

Following on this, Kim et al. (2024) examined the adoption of voice AI in hotel guestrooms, highlighting the need for clear communication about data collection practices in such contexts, and remarking on how while trust plays a crucial role in technology adoption, privacy concerns significantly impact users' intentions to use these services. However, despite known risks, or the possibility of exposure, user attitudes towards privacy and data sharing exhibit a complex and context-dependent nature. Ioannou et al. (2020) found that while travelers express concerns about information privacy, they are often still willing to share behavioral data with travel providers and interestingly, for biometric information, the decision to disclose is more dependent on expected benefits rather than privacy concerns (Ioannou et al., 2020, p.12). Additionally, as suggested by Lehto *et al.* (2023), some regulatory contexts could make it hard for users to opt-out of some data collection procedures, leading to users acceptance of their loss of control in situations related to their stays in hotels and rentals (Kim et al, 2024).

The academic literature we reviewed discussed major privacy concerns in hospitality apps and helped us identify critical issues that informed the development of five scenarios (biometric data collection, room security, location data color lection, IoT smart IA powered devices data collection and extended data retention for marketing) explored in subsequent sections.

With both categories of inquiry and scenarios in mind, we were able to propose three hypotheses that address key aspects of user privacy concerns in hospitality apps. First, regarding transparency and comfort with biometric data collection Lehto *et al*, (2023) suggests how “a significant segment of consumers is concerned about protecting the privacy of their personal data used in biometrics-based hotel services” supporting Ioannou *et al* (2020, p.12) study where it was found that “perceived expected benefits outweigh privacy concerns when travelers are faced with such privacy decisions” making relevant to understand not only confort regarding the collection of this kind of data, but the impact of having disclosure on the way hospitality apps and thirds parties could use data. This, and the previous discussion around led us to the following hypothesis:

- Hypothesis 1: Users are more comfortable with data collection when hospitality apps provide clear disclosure about its use and storage

Second, considering data retention and Opt-Out preferences DeGiulio *et al* (2021) discuss opt-in user consent for tracking in mobile apps, exposing the prevalence of third party trackers in apps and finding how App Tracking Transparency “is less subject to dark patterns and other privacy-diminishing effect than other types of preference settings." (DeGiulio et al, 2021, p.164) while also suggesting the need for further research in other scenarios and contexts. As data collection and retention is a concern discussed by several authors (Ioannou et al 2020; Liyanaarachchi et al 2023, Neo & Teo, 2022; Nema et al, 2022), it poses the opportunity to relate data practices with opt-out preferences, therefore, we propose the following hypothesis:

- Hypothesis 2: Users are more likely to perceive long-term data retention as risky and opt out if they are uncomfortable with how hospitality apps manage data access.

As summarized by Ioannou *et al* (2021, p.1513), while travelers value the benefits of personalization that hospitality apps may offer, like products and proactive convenience, it also raises privacy concerns about they way information is used, as travelers become more aware of the extensive personal and behavioral data collected to create these kind of experiences, even more when the option to opt-out does not seem clear. This aligns with the findings of Lehto et al. (2023), who observed a strong risk education effect on consumer decision-making regarding the commercial use of AI technology in services and discussed how a significant segment of consumers is concerned about protecting the privacy of their personal data used in biometrics-based hotel services, highlighting the value of providing information about risks and benefits as it can significantly influence attitudes (Lehto et al., 2023, p.88). This led us to a third hypothesis, aiming to inquiry around perceived transparency and privacy protection behaviors.

- Hypothesis 3: Individuals with more perceived transparency and stronger preferences for opt-out are more likely to take proactive measures to protect their privacy.

These hypotheses will serve as a foundation for systematically examining how users interact with hospitality apps and the extent to which privacy policies and practices influence their trust and engagement. The subsequent sections are structured to detail the methodology, analyze the results, and engage in a comprehensive discussion.

Methods

Study Design

A survey was conducted for this study to better understand user's privacy perceptions of hospitality apps. The survey presented respondents with these five scenarios: biometric data collection, room security concerns, location data sharing and advertising, data collection by smart devices in rooms, and data retention for marketing. Each scenario had roughly 5 questions each, thus the survey had a total of 25 scenario-based questions. Based on the literature review, the survey questions in each scenario were aimed at further investigating user's concerns regarding data collection, data retention, and control and normative awareness in hospitality apps. Some questions in the scenarios asked about the respondents' about their comfortability with data collection. Other questions asked respondents about their level of concern when unnecessary data is being retained. The rest of the questions were mainly used to understand whether respondents would seek control of data collection, and how comfortable they would be with paying for services to potentially enhance data protection. Overall, the scenarios in the survey were designed to understand the respondent's normative awareness of the hospitality app's privacy by presenting them with situations that they may or may have not have known occur. Additionally, screeners were used so that all participants were individuals who reside in the US, are 18 years or older, own iPhones, and have booked a space using a hospitality app in the past. All the questions presented to the respondents in each scenario were answered using a Likert scale, for example some questions asked respondents about their level of comfortability ranging from extremely comfortable to very comfortable.

For the biometric data collection scenario, the survey respondents were tasked with imagining using a hospitality app that requested a picture of their ID where the biometric data collected would be sent to a third party service provider. This scenario was based on Airbnb's process of asking for a government issued ID which the app uses to collect biometric data to send to third party service providers for identity verification. In the privacy policies of other hospitality apps, there is often a vague description of the usage of biometric data used for identifying an individual. Many hospitality apps like Marriot Bonvoy and World of Hyatt mention using biometric data to "uniquely identify an individual" and "to enable access to our services" respectively (Marriott Bonvoy, n.d., sec. Personal Data We Collect; World of Hyatt, n.d., sec. Special Categories).

The second scenario in the survey was regarding room security concerns where respondents were asked to imagine being in a hotel where the door lock had an older keycard system with known vulnerabilities that have been bypassed in the past. According to the research that analyzed the online travel reviews of American travelers of European hotels, "restriction (i.e. the behaviors that people carry out to protect their privacy) and outcome state (i.e. the various behavioral states through which guests achieve privacy and its outcomes)." are the most discussed categories of privacy concerns (D'Acunto et al., 2021). One problem that raised attention is the security of rooms itself, with reviewers emphasizing the weakness of even lack of locks in their rooms (D'Acunto et al., 2021). This public concern is also coupled with the recently discovered flaws in the security systems used by millions of hotels (Anderson, 2024). This raises concerns about the potential privacy and security risks imposed by the door locks. While there are no explicit laws regulating the security of door locks, it remains a potential gray area on how hotels should regulate their safety systems. Specifically, in the example of Airbnb, there's no requirements on security other than just requiring "should be able to lock" (Airbnb, 2024).

The third scenario presented to respondents dealt with location data sharing and advertising, where the hospitality app used by the participant showed targeted ads, content and nearby recommendations based on their location, suggesting the app shared location data with third party advertisers. This is a relevant scenario as hospitality apps like Booking.com, Airbnb, and other hotel chain platforms usually collect and utilize precise location data to personalize services as part of their integrated features. A review performed by a cybersecurity journal around 22 widely used apps found that many collect extensive user data without proper disclosure or apparent necessity, like precise location, camera, microphone, SMS messages, and even system settings. Among these apps, Booking.com, MakeMyTrip, and HotelTonight were identified as top data collectors (Cybernews, 2023). This finding also supports the lack of transparency in data collection practices concerns and raises ethical questions about the commodification of users' behaviors and data.

The fourth scenario was related to data collection in rooms by smart devices, and it had respondents imagine being in a high-tech hotel where smart devices were used to personalize their experience. The data tracked was later used to send them promotions based on their preferences. This is relevant considering for example, how the release of Alexa for hospitality raised major concerns. Jelski (2019) discussed Western Hotels & Resorts report on the pilot program of Alexa for hospitality, referring to many guests disconnecting Alexa devices due to concerns about being listened to in their rooms, highlighting mistrust from recent privacy breaches involving smart devices, news about Alexa recording private conversations, and underscoring the need of an easily accessible privacy policies regarding data collection and storage from these devices in hotel rooms. Authors like Buhalis & Moldavska (2022) have continued discussions on the matter, primarily exploring voice assistants advantages and challenges around hotel operations and customer service, while others have pointed out the need of addressing concerns regarding data collection instigated by major third parties like Amazon and Google (Bittendorfer et al, 2019)

The fifth scenario was about data retention for marketing, where respondents imagined that their usage of hotel services was stored on their account without their knowledge and later used to send marketing emails based on those services. This scenario reflects real-life practices outlined in policies like Marriott Bonvoy's and World of Hyatt's privacy statements, which mention using customer data for targeted advertising and personalization but provide little transparency about data retention durations. For example, Marriott’s policy explicitly states that collected data is utilized to tailor advertising efforts, aligning closely with the described scenario where users were uncomfortable with unconsented retention and usage of service history (Marriott Bonvoy, n.d). These examples highlight how vague disclosures in privacy policies may lead to user mistrust regarding data retention practices.

The scenarios allowed for the research questions to be addressed, and the exact questions and scenarios are available in Appendix 1.

Study Deployment

The Prolific platform was used to recruit 50 respondents which answered the survey questions on the Qualtrics platform where the survey was created and hosted. The time taken to complete the survey was around 15 minutes. The protocols for the IRB were followed, so each respondent was shown a consent form at the beginning of the survey discussing respondent participation before being shown the scenarios. The survey responses were then used to answer the research listed earlier.

Data Analysis

In regards to the first research question which discussed how disclosure of use and storage in hospitality apps affects user's comfort levels with providing data, a pairwise t-test was conducted to assess respondent's answers to relevant data collection questions in the survey scenarios. The fifth scenario regarding marketing data retention is an exception as a one-sided t-test was used to compare respondent's comfort level with full disclosure and no disclosure of use and storage of data. To assess user's perception of data retention and access in the second research question, the answers to data retention questions in the relevant survey scenarios were used to perform a one-sided t-test. The survey responses were analyzed using a one-sided t-test to address the third research question about user control, such as opt-out preferences and other proactive privacy protection behaviors. However, a pairwise t-test was used for analyzing answers to the fifth scenario regarding marketing data retention. Additionally a regression model was created to compare how transparency and opt-out preferences predict proactive personal data deletion behavior in the fourth scenario with smart devices data collection and the fifth scenario with marketing data retention. The full data analysis conducted can be seen in Appendix 2.

Results

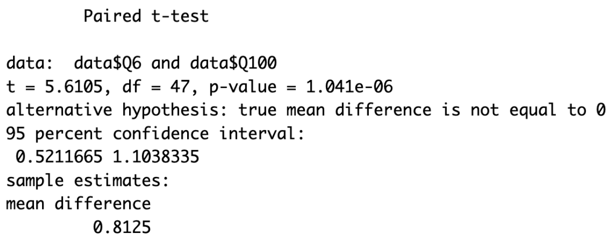
For our results, we conducted paired t-test, one sided t-test, and regression analysis on all of our scenarios in each category.

Category 1: Data Collection Concerns

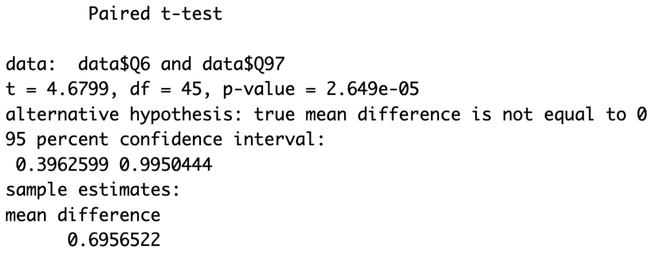
Hypothesis: Transparency and Comfort with Biometric Data Collection

Users are more comfortable with biometric data collection when hospitality apps provide clear disclosure about its use and storage.

Analysis: We can compare responses to Q6 (comfort with disclosed biometric data collection) and Q100 (comfort with undisclosed biometric data collection), and Q97(comfort with undisclosed biometric data use).



```
        Paired t-test

data:  data$Q6 and data$Q100
t = 5.6105, df = 47, p-value = 1.041e-06
alternative hypothesis: true mean difference is not equal to 0
95 percent confidence interval:
 0.5211665 1.1038335
sample estimates:
mean difference
         0.8125
```



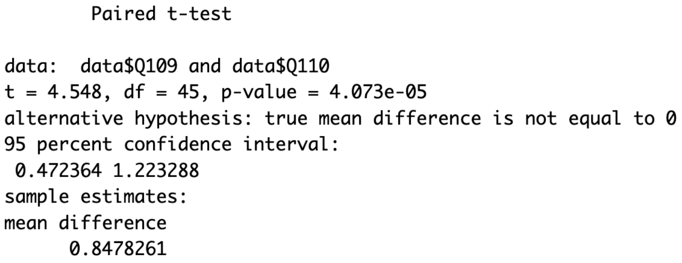
```
        Paired t-test

data:  data$Q6 and data$Q97
t = 4.6799, df = 45, p-value = 2.649e-05
alternative hypothesis: true mean difference is not equal to 0
95 percent confidence interval:
 0.3962599 0.9950444
sample estimates:
mean difference
      0.6956522
```

These significant p-values show that users are more comfortable with disclosed data collection than undisclosed ones.

Hypothesis: Transparency and Comfort with Location Data Collection

Users are more comfortable with smart device data collection when hospitality apps provide clear disclosure about its use and storage.

Analysis: We can compare responses to Q109 (comfort with disclosed location data collection) and Q100 (comfort with undisclosed location data use).



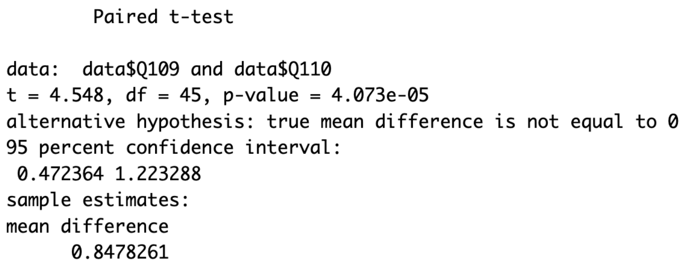
```
        Paired t-test

data:  data$Q109 and data$Q110
t = 4.548, df = 45, p-value = 4.073e-05
alternative hypothesis: true mean difference is not equal to 0
95 percent confidence interval:
 0.472364 1.223288
sample estimates:
mean difference
      0.8478261
```

Similarly, in location data collection, the significant p-value also shows that users prefer clear disclosure about data collection and use.

Hypothesis: Transparency and Comfort with Smart Device Data Collection

Users are more comfortable with location data collection when hospitality apps provide clear disclosure about its use and storage.

Analysis: We can compare responses to Q109 (comfort with disclosed smart device data collection) and Q100 (comfort with undisclosed smart device data use).



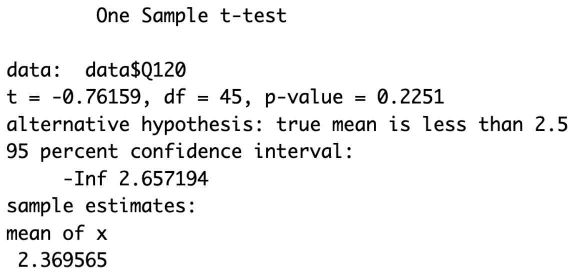
```
        Paired t-test

data:  data$Q109 and data$Q110
t = 4.548, df = 45, p-value = 4.073e-05
alternative hypothesis: true mean difference is not equal to 0
95 percent confidence interval:
 0.472364 1.223288
sample estimates:
mean difference 
      0.8478261 
```

Similarly, in smart device data collection, the significant p-value also shows that users prefer clear disclosure about data collection and use.

Hypothesis: Transparency and Comfort with Personal Service Records Data Collection

Users are more comfortable with personal service records with clear disclosure and consent

Analysis: We can compare responses to Q120 (comfort with undisclosed personal service records data collection) and the average value of 2.5.



```
        One Sample t-test

data:  data$Q120
t = -0.76159, df = 45, p-value = 0.2251
alternative hypothesis: true mean is less than 2.5
95 percent confidence interval:
     -Inf 2.657194
sample estimates:
mean of x 
 2.369565 
```

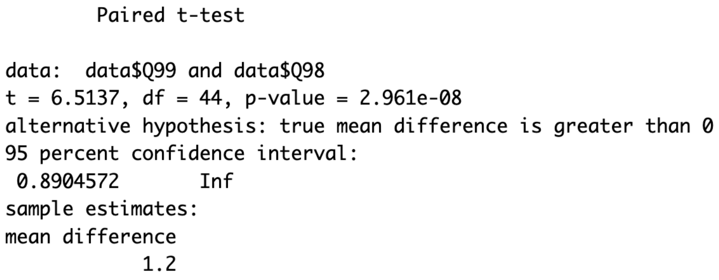
Similarly, in personal service records data collection, the significant p-value also shows that users prefer clear disclosure about data collection and use.

Category 2: Data Retention and Access

Hypothesis: User Concern for Biometric Data Retention

Users are more concerned about security breaches in biometric data retention than average hospitality biometric data use for business purposes.

Analysis: We can examine the differences between Q98 (concern about security breach in biometric data) and Q99(concern about general business use in biometric data).



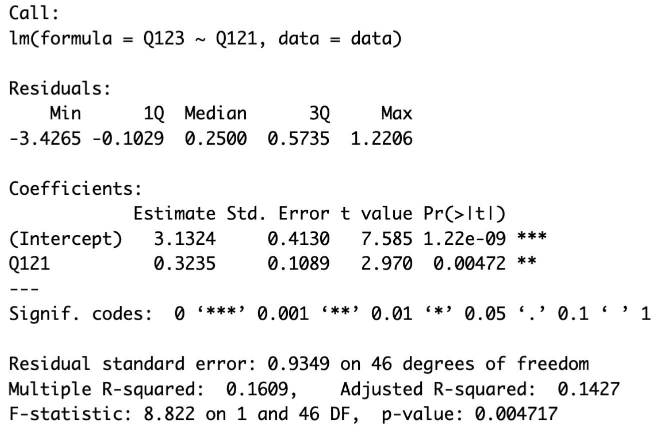
```
        Paired t-test

data:  data$Q99 and data$Q98
t = 6.5137, df = 44, p-value = 2.961e-08
alternative hypothesis: true mean difference is greater than 0
95 percent confidence interval:
 0.8904572       Inf
sample estimates:
mean difference 
            1.2 
```

The significant p-value results indicate that users are more concerned about potential security risks in biometric data retention than normal business use.

Hypothesis: User Concern for Personal Records Data Retention

Users are more likely to perceive long-term data retention as risky and opt out if they are uncomfortable with hospitality personal records data use.

Analysis: We can examine the correlation between Q121 (concern about excessive data collection) and Q123 (likelihood to opt-out of data collection).



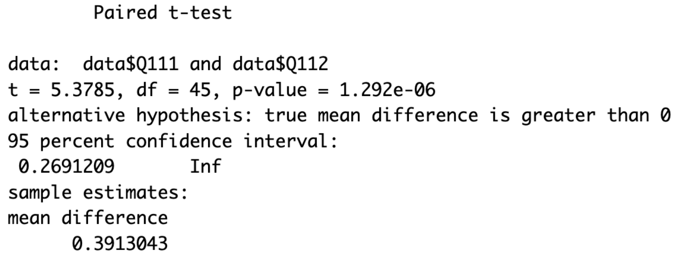
```
Call:
lm(formula = Q123 ~ Q121, data = data)

Residuals:
    Min      1Q  Median      3Q     Max 
-3.4265 -0.1029  0.2500  0.5735  1.2206 

Coefficients:
            Estimate Std. Error t value Pr(>|t|)    
(Intercept)   3.1324     0.4130   7.585 1.22e-09 ***
Q121          0.3235     0.1089   2.970  0.00472 ** 
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.9349 on 46 degrees of freedom
Multiple R-squared:  0.1609,	Adjusted R-squared:  0.1427 
F-statistic: 8.822 on 1 and 46 DF,  p-value: 0.004717
```

The significant p-value results indicate that users are more likely to perceive data retention as risky when they are more concerned about personal records data use.

Hypothesis: User Concern for Location Data Retention

Users are more concerned about length of data retention than sharing of data for location data.

Analysis: We can examine the differences between Q111 (concern about length of data retention in location data) and Q112 (concern about sharing of data retention in location data).



```
	Paired t-test

data:  data$Q111 and data$Q112
t = 5.3785, df = 45, p-value = 1.292e-06
alternative hypothesis: true mean difference is greater than 0
95 percent confidence interval:
 0.2691209       Inf
sample estimates:
mean difference 
      0.3913043 
```

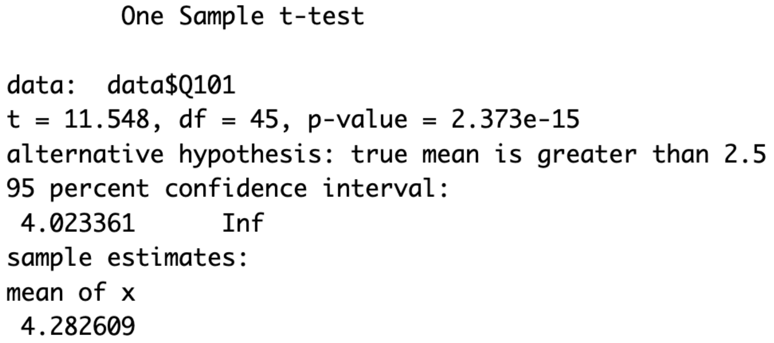
The significant p-value results indicate that users are more concerned about length of data than sharing of data.

Category 3: User Control and Normative Awareness

Hypothesis: In Person vs Online Preferences with Biometric Data

Users generally prefer verification involving biometric data in person rather than online.

Analysis: We can compare responses to Q101 (preferences for in person verification) and the average value of 2.5.



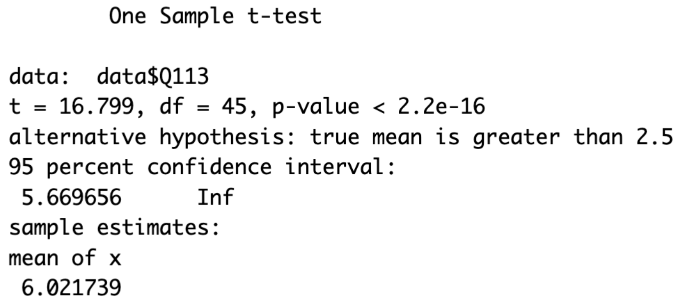
```
        One Sample t-test

data:  data$Q101
t = 11.548, df = 45, p-value = 2.373e-15
alternative hypothesis: true mean is greater than 2.5
95 percent confidence interval:
 4.023361      Inf
sample estimates:
mean of x
 4.282609
```

The results show that users' preferences are greater than average value, 2.5, which means that users generally prefer to verify in person than online.

Hypothesis: Opt Out Preferences with Location Data

Users generally prefer to opt out in location data tracking.

Analysis: We can compare responses to Q113 (preferences for data collection opt out) and average value, 2.5



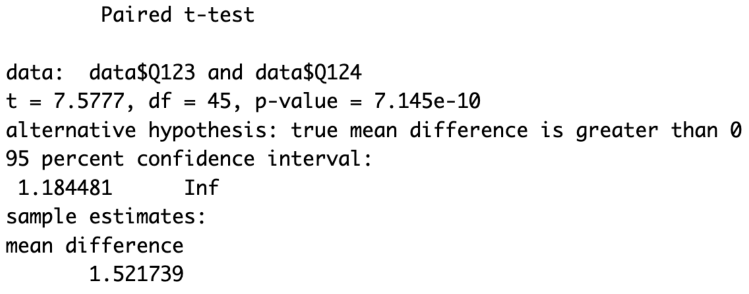
```
        One Sample t-test

data:  data$Q113
t = 16.799, df = 45, p-value < 2.2e-16
alternative hypothesis: true mean is greater than 2.5
95 percent confidence interval:
 5.669656      Inf
sample estimates:
mean of x
 6.021739
```

The results show that users' preferences are greater than average value, 2.5, which means that users generally prefer to opt out.

Hypothesis: User Preferences vs Actual Action Involving Cost with Personal Records Data

Users who prefer to delete their data will choose to pay a small fee to ensure all data is deleted.

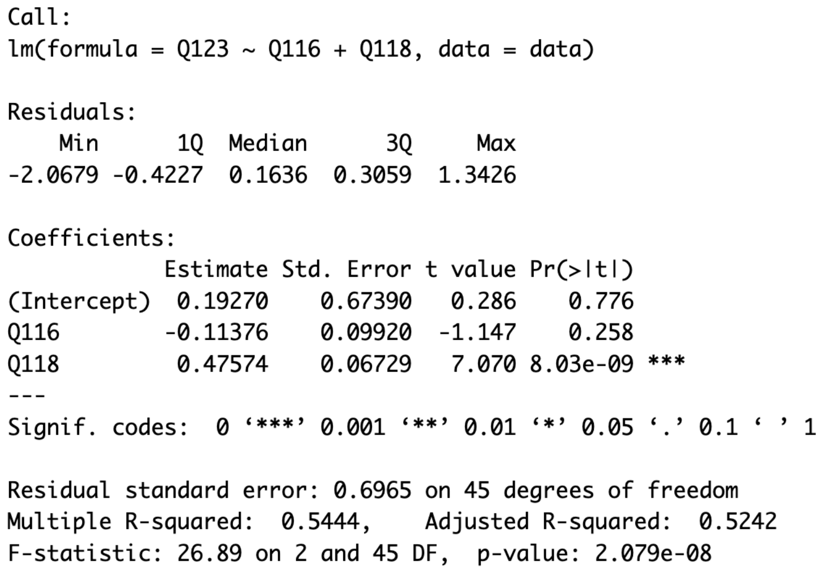
Analysis: We can compare responses to Q123 (preferences for data deletion) and Q124 (willingness to pay for deletion).



```
        Paired t-test

data:  data$Q123 and data$Q124
t = 7.5777, df = 45, p-value = 7.145e-10
alternative hypothesis: true mean difference is greater than 0
95 percent confidence interval:
 1.184481      Inf
sample estimates:
mean difference
       1.521739
```

The results show that users who prefer to delete data are not willing to pay for their deletion, which rejects our hypothesis.

Hypothesis: Users Proactive Behavior Prediction Model with Data Across Scenarios
Individuals with more perceived transparency and stronger preferences for opt out are more likely to take proactive measures to protect their privacy.
Analysis: A regression model was created to assess how transparency (Q116) and opt-out preferences (Q118) predict proactive behaviors, such as data deletion (Q123).



```
Call:
lm(formula = Q123 ~ Q116 + Q118, data = data)

Residuals:
    Min      1Q  Median      3Q     Max 
-2.0679 -0.4227  0.1636  0.3059  1.3426 

Coefficients:
            Estimate Std. Error t value Pr(>|t|)    
(Intercept)  0.19270    0.67390   0.286    0.776    
Q116        -0.11376    0.09920  -1.147    0.258    
Q118         0.47574    0.06729   7.070 8.03e-09 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.6965 on 45 degrees of freedom
Multiple R-squared:  0.5444,	Adjusted R-squared:  0.5242 
F-statistic: 26.89 on 2 and 45 DF,  p-value: 2.079e-08
```

Conclusion:

Users exhibit a strong preference for detailed disclosures regarding data collection and usage, particularly for sensitive information like biometrics and location data. The study identified a significant difference in comfort levels between disclosed and undisclosed biometric data practices ($p < 0.05$), underscoring the critical importance of transparency in fostering trust and confidence among users (Ioannou et al., 2020). Hospitality apps that prioritize clear and accessible communication about their data handling practices are better equipped to build and sustain user trust, which is essential for long-term engagement.

The research also highlighted a strong correlation between user concerns about excessive data retention and their likelihood to opt out when given the option ($r = 0.68$, $p < 0.001$). Apps that offer clear and user-friendly opt-out mechanisms, particularly for sensitive data like location tracking or smart device interactions, can significantly enhance user satisfaction and trust. This demonstrates the importance of empowering users with intuitive privacy controls to address their concerns effectively while ensuring regulatory compliance (DeGiulio et al., 2021).

However, a notable gap exists between user preferences for privacy protection and their willingness to take actionable steps when monetary incentives are involved. While 65% of users expressed a preference for deleting their data, only 45% were willing to pay for this feature. This disconnect suggests a need for cost-free and user-friendly options for managing personal data. Apps that offer non-monetary solutions, such as automatic data deletion or easy-to-use deletion tools, are likely to align more closely with user expectations and encourage proactive privacy management (Kim et al., 2024).

Security concerns also play a significant role in shaping user preferences, with users demonstrating a willingness to pay for enhanced security features when their room safety is perceived as inadequate ($r = 0.45$, $p < 0.001$). This insight points to an opportunity for hospitality providers to offer tiered security options, such as upgraded locks or advanced room security systems, which could cater to users with heightened security needs and simultaneously improve overall satisfaction.

Concerns about excessive data collection by smart devices were strongly correlated with a higher likelihood of opting out of such practices ($r = 0.68$, $p < 0.001$). Hospitality apps can address these concerns by providing granular control over IoT device data collection, balancing the benefits of personalized experiences with respect for user privacy. This approach is critical for alleviating discomfort and ensuring a positive user experience.

Data retention practices for marketing purposes also emerged as a significant source of discomfort, particularly when conducted without explicit consent. Users expressed a clear need for apps to implement transparent data retention policies and align with privacy regulations like General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Ensuring clear communication about how and why user data is retained is essential for rebuilding trust and mitigating concerns.

Biometric data handling remains one of the most sensitive areas of concern, with users expressing discomfort over undisclosed practices related to biometric information. Hospitality apps must implement robust security measures and provide detailed explanations of how such data is stored and protected. By prioritizing transparency and demonstrating a commitment to safeguarding sensitive information, these platforms can effectively address user concerns and build a reputation as trustworthy services.

Limitations

This study, while offering valuable insights into user perceptions of privacy in hospitality apps, has several limitations that merit consideration. Firstly, the survey's sample size of 50 respondents, though sufficient for initial analysis, limits the generalizability of the findings. A larger and more demographically diverse participant pool would provide stronger statistical power and capture variations across different user groups, particularly regarding geographic and cultural contexts (D’Acunto et al., 2021).

The use of a scenario-based approach, while effective for eliciting targeted insights, does not fully reflect real-world complexities. Hypothetical responses may differ significantly from actual user behavior during live interactions with hospitality apps, potentially leading to over- or underestimations of privacy concerns (Ioannou et al., 2020). Furthermore, the study focused on specific technologies such as biometric verification, IoT devices, and location tracking. This narrow scope, though intentional, overlooks broader and emerging privacy challenges, such as the integration of blockchain systems or advanced AI-driven personalization features (De Camargo Silva et al., 2019).

Another limitation is the focus on existing privacy practices in well-known apps like Airbnb and Marriott Bonvoy. While this approach provided relevant insights, it might not account for cutting-edge innovations or the implications of upcoming regulatory changes, such as stricter enforcement under evolving GDPR or CCPA guidelines. Lastly, the analysis of user behavior in scenarios involving monetary incentives for privacy protections highlighted a preference-action gap but did not explore alternative motivators. Non-monetary factors such as loyalty rewards or trust-based incentives might offer additional pathways to encourage proactive privacy behaviors, which remain unexamined.

Future Research

Building on these findings, future research should adopt a longitudinal design to observe how user perceptions and behaviors change over time, particularly as privacy regulations and app functionalities evolve. By tracking trends and responses longitudinally, researchers could better capture the dynamic nature of user concerns and preferences (Jung and Park, 2018).

Expanding the participant base to include a larger and more demographically diverse sample would enhance the reliability of findings and help identify cultural and regional differences in privacy concerns (D’Acunto et al., 2021). Furthermore, comparing privacy perceptions in the hospitality sector with those in other app-intensive industries, such as healthcare or retail, could provide a broader perspective on user expectations and trust across sectors (Chen et al., 2021).

Future studies should also incorporate experimental methodologies to validate the preferences identified in this survey. Observing actual user behavior in live app environments would address potential hypothetical biases inherent in scenario-based approaches. Additionally, exploring non-monetary incentives such as gamification, rewards, or reputation-based systems could provide alternative pathways to encourage privacy-protective behaviors without imposing financial burdens on users.

There is also a need to analyze the implications of emerging technologies, such as blockchain-based systems, decentralized identity platforms, and advanced AI-driven personalization. These technologies introduce new dimensions to privacy and data governance, which may not be adequately addressed by current frameworks (De Camargo Silva et al., 2019). Lastly, as regulatory landscapes evolve, future research should examine the impact of new privacy laws and directives on user trust and app compliance. By focusing on these areas, subsequent studies can provide a more comprehensive understanding of privacy dynamics in the digital hospitality ecosystem.

References

Airbnb. (2024). Bedroom and bathroom locks for your Room listing - Airbnb Help Center. Airbnb. https://www.airbnb.com/help/article/3412

Anderson, M. (2024, March 22). A Security Flaw in Millions of Hotel Keycard Locks Has Been Found. What Does that Mean for Planners? | Smart Meetings. Smart Meetings. https://www.smartmeetings.com/tips-tools/159860/a-security-flaw-in-millions-of-hotel-keycard-locks-has-been-found-saflok

Bittendorfer, T., Bunt, J., Grunder, L., Riedel, D., Magnus, B., & Salzlecher, T. (2019). Technology in tourism: How voice assistants influence the hospitality industry. Iscontour, 328-338.

Buhalis, D., & Moldavska, I. (2022). Voice assistants in hospitality: using artificial intelligence for customer service. Journal of Hospitality and Tourism Technology, 13(3), 386-403.

Chen, S., Law, R., Zhang, M., & Si, Y. (2021). Mobile communications for tourism and hospitality: a review of historical evolution, present status, and future trends. Electronics, 10(15), 1804.

Cybernews. (2023, June 12). Top travel apps harvesting your data without asking – Cybernews exclusive. https://cybernews.com/privacy/top-travel-apps-privacy/

D'Acunto, D., Volo, S., & Filieri, R. (2021). "Most Americans like their privacy." Exploring privacy concerns through US guests' reviews. International Journal of Contemporary Hospitality Management, 33(8), 2773–2798. https://doi.org/10.1108/ijchm-11-2020-1329

De Camargo Silva, L., Samaniego, M., & Deters, R. (2019, October). IoT and blockchain for smart locks. In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0262-0269). IEEE.

DeGiulio, A., Lee, H., & Birrell, E. (2021, October). "Ask App Not to Track": The Effect of Opt-In Tracking Authorization on Mobile Privacy. In International Workshop on Emerging Technologies for Authorization and Authentication (pp. 152-167). Cham: Springer International Publishing.

Fong, A. (2017). The role of app intermediaries in protecting data privacy. International Journal of Law and Information Technology, 25(2), 85-114.

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

Ioannou, A., Tussyadiah, I., & Miller, G. (2021). That's private! Understanding travelers' privacy concerns and online data disclosure. Journal of Travel Research, 60(7), 1510-1526.

Jelski, C. (2019, February 19). Amazon's Alexa can be an unwelcome hotel roommate. Travel Weekly. https://www.travelweekly.com/Travel-News/Hotel-News/Hotel-guests-uncomfortable-with-Amazon-Alexa

Jung, Y., & Park, J. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. International Journal of Information Management, 43, 15-24.

Kim, J., Erdem, M., & Kim, B. (2024). Hi Alexa, do hotel guests have privacy concerns with you?: A cross-cultural study. Journal of Hospitality Marketing & Management, 33(3), 360-383.

Krämer, J. (2024). The death of privacy policies: How app stores shape GDPR compliance of apps. Internet Policy Review, 13(2). https://doi.org/10.14763/2024.2.1757

Lehto, X. Y., Park, S., Mohamed, M. E., & Lehto, M. R. (2023). Traveler attitudes toward biometric data-enabled hotel services: Can risk education play a role?. Cornell Hospitality Quarterly, 64(1), 74-94.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 28.

Li, Y., Chen, D., Li, T., Agarwal, Y., Cranor, L. F., & Hong, J. I. (2022, April). Understanding ios privacy nutrition labels: An exploratory large-scale analysis of app store data. In CHI Conference on Human Factors in Computing Systems Extended Abstracts (pp. 1-7).

Liyanaarachchi, G., Viglia, G., & Kurtaliqi, F. (2023). Privacy in hospitality: managing biometric and biographic data with immersive technology. International Journal of Contemporary Hospitality Management.

Marriott Bonvoy. (n.d.). California and Colorado Privacy Statement. Marriott. Retrieved December 7, 2024, from https://www.marriott.com/about/ccpa-cpa.mi

Mo Kwon, J., Bae, J. I., & Blum, S. C. (2013). Mobile applications in the hospitality industry. Journal of hospitality and tourism technology, 4(1), 81-92.

Neo, H. F., & Teo, C. C. (2022). Biometrics in Tourism: Issues and Challenges. Handbook of e-Tourism, 1835-1849.

Rodríguez, D., Fernández-Aller, C., Del Alamo, J. M., & Sadeh, N. (2024, July). Data Retention Disclosures in the Google Play Store: Opacity Remains the Norm. In 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 19-23). IEEE.

Rodriguez, D., Jain, A., Del Alamo, J. M., & Sadeh, N. (2023, July). Comparing privacy label disclosures of apps published in both the App Store and Google Play Stores. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 150-157). IEEE.

Sia, P. Y. H., Saidin, S. S., & Iskandar, Y. H. P. (2023). Systematic review of mobile travel apps and their smart features and challenges. Journal of Hospitality and Tourism Insights, 6(5), 2115-2138.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS quarterly, 167-196.

Surma, Z. A., Gowdar, S., & Pandit, H. J. (2024). Examining the Integrity of Apple's Privacy Labels: GDPR Compliance and Unnecessary Data Collection in iOS Apps. Information, 15(9), 551.

World of Hyatt. (n.d.). Privacy policy for guests. Retrieved December 7, 2024, from https://world.hyatt.com/content/gp/en/privacy/guest-policy.html

Zhang, S., Feng, Y., Yao, Y., Cranor, L. F., & Sadeh, N. (2022). How usable are ios app privacy labels?. Proceedings on Privacy Enhancing Technologies. [Original source: https://studycrumb.com/alphabetizer]

Appendix 1: Survey Questions

Demographic questions:

Could you please indicate the age group you belong to? (Single choice)

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

Would you mind sharing the highest level of education you have completed? (Single choice)

- High school
- Bachelor’s degree
- Master’s degree
- PhD
- Other: [Please specify]

May we ask your gender? (Single choice)

- Male
- Female
- Non-binary
- Prefer not to say
- Other: [Please specify]

Have you used any of the following hospitality apps in the past? (Select all that apply)

- Airbnb
- Booking.com
- Marriott Bonvoy
- Expedia
- Hotels.com
- Other: [Please specify]

Scenario questions

Scenario 1: Biometric Data Collection

Imagine you download a hospitality app to book a hotel. The app requests a photo of your government ID for identity verification, allowing it to collect and share your biometric data with third-party service providers for facial recognition purposes. The biometric information collected in this scenario is the information regarding your facial features and other physical characteristics that is generated through facial recognition technology.

How comfortable are you with using a hospitality app that collects and shares your biometric data gathered from a picture of your government issued ID, assuming the app fully discloses how it's used and stored?

Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How comfortable are you with using a hospitality app that does not specify which third party service providers it shares your biometric information with?

Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How comfortable are you with using a hospitality app where your biometric data could be accessed by unauthorized parties due to a security breach after you had submitted a picture of your government issued ID?

Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How comfortable are you with using a hospitality app that states they only use biometric data gathered from your government issued ID for "General Business and Booking/Guest Registration"?

Scale:
1 - Extremely Uncomfortable

2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How comfortable are you with using a hospitality app that does not specify what constitutes the biometric information the app collects?

Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

If offered a choice between using the app's biometric verification or having an in-person employee verify your ID, how likely would you be to choose in-person verification?

Scale:
1 - Extremely Unlikely (Prefer App's Biometric Verification)
2 - Unlikely
3 - Neutral
4 - Likely
5 - Extremely Likely (Prefer In-Person Verification)

Scenario 2: Room Security Concerns

Imagine staying in a hotel where the door lock is an older keycard system without any additional security features. Later, you learn that this lock system has known vulnerabilities and has been bypassed in similar hotels.

How secure would you feel staying in a hotel room that only uses a basic keycard lock without added security mechanisms (e.g., deadbolt or chain latch)?

Scale:
1 - Very Secure
2 - Secure
3 - Neutral
4 - Insecure
5 - Very Insecure

How concerned would you be about staying in a hotel with a keycard lock system that has been reported to have potential security flaws?
Scale:
1 - Not Concerned at All
2 - Slightly Concerned
3 - Neutral
4 - Concerned
5 - Extremely Concerned

If you knew a hotel's lock system had security vulnerabilities, how likely would it influence your decision to avoid staying there?
Scale:
1 - Extremely Unlikely
2 - Unlikely
3 - Neutral
4 - Likely
5 - Extremely Likely

How important is it to you that hotels provide detailed information about their room security measures, such as the type of locks or other security features?
Scale:
1 - Not Important at All
2 - Slightly Important
3 - Neutral
4 - Important
5 - Extremely Important

Would you be willing to pay an extra amount (e.g., $5 per night) for a room with enhanced security features, like upgraded locks or additional security devices?
Scale:
1 - Not Willing at All
2 - Slightly Willing
3 - Neutral
4 - Willing
5 - Extremely Willing

Scenario 3: Location Data Sharing and Advertising

Imagine using a hospitality app that tracks your location to offer nearby recommendations. Later, you notice targeted ads for places you visited, suggesting the app shared your location data with third-party advertisers.

How comfortable would you feel about the app sharing your location data with third-party advertisers, assuming the app's information about privacy disclosure is clear?
Scale:
1 - Extremely uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How comfortable would you be if the app collected more location data than necessary (e.g. Keeps collecting location data after your stay is over) without explicitly stating this previously?
Scale:
1 - Not comfortable at all
2 - Slightly comfortable
3 - Neutral
4 - Comfortable
5 - Extremely comfortable

If the app did not specify how long your location data would be stored, how comfortable would this make you feel?
Scale:
1 - Not comfortable at all
2 - Slightly comfortable
3 - Neutral
4 - Comfortable
5 - Extremely comfortable

How comfortable would you be if the app shared your location data with third parties without explicitly mentioning it in advance?
Scale:
1 - Not comfortable at all
2 - Slightly comfortable
3 - Neutral
4 - Comfortable
5 - Extremely comfortable

If the app offered a clear opt-out option for location tracking, to which extent would you rather

opt-out of location tracking, knowing this option is available?
Scale:
1 - Definitely Would Not Opt-Out
2 - Probably Would Not Opt-Out
3 - Unsure / Neutral
4 - Probably Would Opt-Out
5 - Definitely Would Opt-Out

Scenario 4: Data Collection by Smart Devices in Rooms

Imagine staying in a high-tech hotel with smart devices that track your habits to personalize your experience. Later, you receive promotions based on these preferences, realizing your data was recorded and retained.

Regarding this particular scenario, how comfortable would you feel about smart devices collecting data on your habits and preferences, assuming full disclosure of their data use?
Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How transparent do you find the information provided by apps about data collection and use by smart devices in hotel rooms?
Scale:
1 - Not Transparent at All
2 - Slightly Transparent
3 - Neutral
4 - Transparent
5 - Extremely Transparent

How concerned would you be if smart devices in your room collected more behavioral data than necessary (e.g. your daily routine, shows and content by demand, personal requests, night behaviors) without properly telling you?
Scale:
1 - Not Concerned at All
2 - Slightly Concerned

3 - Neutral
4 - Concerned
5 - Extremely Concerned

If you were offered a clear opt-out option for data collection by smart IoT or AI powered devices in your hotel room or stays, to which extent would you rather opt-out, knowing this option is available?

Scale:
1 - Definitely Would Not Opt-Out
2 - Probably Would Not Opt-Out
3 - Unsure / Neutral
4 - Probably Would Opt-Out
5 - Definitely Would Opt-Out

Scenario 5: Data Retention for Marketing

Imagine receiving promotional emails from a hotel after your stay based on specific services you used, like spa treatments, which are still stored in your account without prior knowledge or consent.

How uncomfortable would you feel if hospitality apps retained personal records (e.g., spa treatments, massages, room service, etc) without your consent?
Scale:
1 - Extremely Uncomfortable
2 - Uncomfortable
3 - Neutral
4 - Comfortable
5 - Extremely Comfortable

How concerned would you feel if your personal data was used in marketing campaigns without your explicit consent?
Scale:
1 - Not Concerned at All
2 - Slightly Concerned
3 - Neutral
4 - Concerned
5 - Extremely Concerned

If such personal data were exposed due to a data breach, how vulnerable would you feel?
Scale:
1 - Extremely Vulnerable
2 - Vulnerable
3 - Neutral
4 - Invulnerable
5 - Extremely Invulnerable

How likely are you to choose an option to delete personal service data after your stay?
Scale:
1 - Extremely Unlikely
2 - Unlikely
3 - Neutral
4 - Likely
5 - Extremely Likely

Would you be willing to pay a small fee (e.g., $2) to ensure that all personal service data is erased after your stay?
Scale:
1 - Not Willing at All
2 - Slightly Willing
3 - Neutral
4 - Willing
5 - Extremely Willing

Appendix 2: Data Analysis

```
data <- read.csv("/Users/yiyao/Downloads/Understanding Perceptions of Hospitality Apps_December 2, 2024_20.29.csv", header = TRUE)
data <- data[-c(1, 2), ]
library(ggplot2)

## First category
## Data Collection Concerns: sets the foundation by exploring users' comfort with data sharing, as all scenarios inherently involve data collection.

#First scenario: Biometric data
data$Q6 <- as.numeric(as.character(data$Q6))
data$Q100 <- as.numeric(as.character(data$Q100))
t.test(data$Q6, data$Q100, paired = TRUE)
data$Q6 <- as.numeric(as.character(data$Q6))
data$Q97 <- as.numeric(as.character(data$Q97))
t.test(data$Q6, data$Q97, paired = TRUE)
#comfort with full disclosure vs no disclosure

#Third scenario: Location data
data$Q109 <- as.numeric(as.character(data$Q109))
data$Q110 <- as.numeric(as.character(data$Q110))
t.test(data$Q109, data$Q110, paired = TRUE)
#comfort with full disclosure vs no disclosure

#Fourth scenario: Smart device
data$Q115 <- as.numeric(as.character(data$Q115))
data$Q117 <- as.numeric(as.character(data$Q117))
t.test(data$Q115, data$Q117, paired = TRUE)
#comfort with full disclosure vs no disclosure

#Fifth scenario: Marketing data
data$Q120 <- as.numeric(as.character(data$Q120))
t.test(data$Q120, mu= 2.5, alternative="less")
#comfort with full disclosure vs no disclosure

## Second category
## Data Retention and Access: directly address the hypothesis on excessive data retention and its potential risks.
## First scenario: Biometric data
data$Q98 <- as.numeric(as.character(data$Q98))
data$Q99 <- as.numeric(as.character(data$Q99))
t.test(data$Q99, data$Q98, paired = TRUE, alternative = 'greater')
# test whether users are more concerned with security breach or normal business use
# significant, so it means that users more concerned

## Fifth scenario: Marketing data
data$Q121 <- as.numeric(as.character(data$Q121))
data$Q123 <- as.numeric(as.character(data$Q123))
t.test(data$Q121, data$Q123, paired = TRUE)
model <- lm(Q123 ~ Q121 , data = data)
print(summary(model))

## Third scenario: Location data
data$Q111 <- as.numeric(as.character(data$Q111))
data$Q112 <- as.numeric(as.character(data$Q112))
t.test(data$Q111, data$Q112, alternative= 'greater', paired = TRUE)
# test whether users are more concerned with length of data retention or sharing of data
# results indicate sharing of data is more of concern

## Third category
## User Control and Normative Awareness: focus on user control and their awareness of data
related policies, both of which are critical in data privacy issues across all scenarios.

# First scenario: Biometric data
data$Q101 <- as.numeric(as.character(data$Q101))
t.test(data$Q101, mu = 2.5, alternative= 'greater')
# test whether user prefer in person over app verification
# prefer in person

# Third scenario: Location
data$Q113 <- as.numeric(as.character(data$Q113))
t.test(data$Q113, mu = 2.5, alternative= 'greater')
# test whether people wanna opt out,
# result is they prefer

# Fifth scenario: Marketing data
data$Q123 <- as.numeric(as.character(data$Q123))
data$Q124 <- as.numeric(as.character(data$Q124))
```

```
t.test(data$Q123, data$Q124, alternative= 'greater', paired = TRUE)
# test whether people who prefer to delete will actually transfer to action
# no, more people said they prefer but less people said they would pay

# Analysis between scenarios
# Smart devices (scenario 4)  + Marketing (scenario 5)
data$Q116 <- as.numeric(as.character(data$Q116))
data$Q118 <- as.numeric(as.character(data$Q118))
model <- lm(Q123 ~ Q116 + Q118, data = data)
print(summary(model))
# transparency + opt out preferences predict proactive delete personal data behavior
```