Privacy Policy and Hosts' Concerns on Accommodation Sharing Platforms

Jiang Hu
University of Texas at Arlington
Jiang.hu@mavs.uta.edu

Jennifer Jie Zhang
University of Texas at Arlington
jiezhang@uta.edu

Huigang Liang
University of Memphis
hliang1@memphis.edu

Abstract

Recent years have witnessed increasing embracement of accommodation sharing services via online community platforms. Meanwhile, users' privacy concerns over social interactions and online transactions on these platforms are escalating. This study investigates whether and how privacy policy can properly mitigate hosts' privacy concerns, enhance perceived benefits, and subsequently encourage their information disclosure on the accommodation sharing platforms (ASPs). Through a scenario-based survey and a controlled experiment, we find that the hosts are more concerned about the other users' misappropriating the private information that the hosts disclose on the platform than the platforms' privacy invasion behaviors. However, this major concern is not significantly mitigated by the current privacy policy. Moreover, privacy policy engenders two types of perceived benefits, among which the perceived social benefit has a stronger effect than economic benefit on the hosts' intentions to disclose information on ASPs.

Keywords: Accommodation sharing platforms (ASPs), Privacy policy, Information disclosure, Privacy concerns.

1. Introduction

In recent years, more people have embraced accommodation sharing services via online community marketplaces such as Airbnb.com and Vacation Rental by Owner (VRBO.com). A survey conducted by Pew Research Center reports that about 11% of American adults stayed overnight in a private residence using a home-sharing site in 2015. In 2017, over 33.9 million adults in the United States used Airbnb for their travel (Lock 2020). These online services, named accommodation sharing platforms (ASPs), are two-sided collaborative consumption platforms that connect accommodation providers and consumers in the travel and tourism markets and enable them to initiate and carry out transactions with each other electronically (Krasnova et al. 2015; Teubner & Flath 2019; Wang et al. 2020).

ASP, as a combination of social media and e-commerce platform, attracts the general public's attention, which brings both benefits and risks to the hosts. On the one hand, hosts can gain extra income by renting out their surplus properties and cumulate social capital via building a trusting relationship with visitors. On the other hand, since trading with strangers on ASPs involves social interactions characterized by information asymmetry, both the hosts and the guests can have privacy concerns during the transactions. Although ASPs are becoming increasingly popular in the tourism and rental markets and have significantly impacted the economy, consumers' concerns about their privacy are increasingly growing. For example, Airbnb reported a data security incident that occurred within its service, exposing the data of Airbnb hosts to other platform users. The exposed data includes hosts' personally identifiable information (PII), account passwords, phone numbers, property addresses, and property access codes (DecisionMarketing 2020).

The issue of privacy concern and information disclosure has received a great deal of attention in the IS field (e.g., Hong & Thong 2013; Malhotra et al. 2004; Pavlou et al. 2007; Smith et al. 2011). While consumers are faced with similar concerns in ASPs as in the general e-commerce context, hosts who disclose private information on ASPs may suffer additional risks. For example, Airbnb hosts typically post pictures of the authentic interior of their properties, associated facilities, and surrounding attractions, and text description about their personal background, occupation, hobby, and even other family members' information. All of the above personal information opens possibilities of intrusions into hosts' daily lives and even physical damage or loss of amenities. Thus, the findings of the literature about privacy concerns and information disclosure on traditional e-commerce platforms may not be directly applied to the ASP setting.

A privacy policy informs users of a firm's data protection practice in order to enhance their willingness to provide personal information. Some studies (Bansal et al. 2015; Hui et al. 2007; Wang & Herrando 2019; Wu et al. 2012) have explored users' perceptions of the

HⁱCSS

privacy policy and the factors that may predict a user's intention to disclose personal information or to purchase online. However, researchers have paid little attention to the information privacy and self-disclosure behaviors in the context of accommodation sharing, especially from the service providers' (i.e., hosts) perspective (Teubner & Flath 2019). Thus, there is a need for explicit theorization and systematic investigation of the drivers and impediments that jointly influence a service provider's decision-making process. Therefore, this research aims to gain insights into this topic by answering the following research questions:

1. What are the mechanisms of the impacts of the privacy policy on hosts' disclosure of personal information?

2. How to enhance the hosts' disclosure of personal information by improving privacy policy design?

By answering these questions, we bridge three theoretical gaps. First, the existing conceptualizations of privacy concern only consider the concern from a consumer (buyer)'s point of view and are unable to capture the uniqueness from the service provider (seller)'s angle. As a result, these conceptualizations are insufficient to explain a service provider's disclosure behavior. Second, extant privacy literature primarily emphasizes the role of individual-level privacy perception and relationships. The role of contextual factors, such as platform-level social and policy factors, in shaping disclosure behavior has not been theorized and explored in depth (Smith et al. 2011). There is a need to examine how the individual-level factors (e.g., privacy concern and benefit expectancy) and platform-level factors (e.g., privacy policy) interplay to affect personal information disclosure collectively. Third, prior literature (Bansal et al. 2015; Guo et al. 2021; Wu et al. 2012) suggests that different dimensions of privacy policy content (i.e., notice, choice, access, security, and enforcement) influence individuals' privacy concern, trust belief, and information disclosure behavior in different ways. It is thus essential to examine how different privacy policy clauses impact hosts' perceptions and behaviors differently on APSs.

Our study complements the existing privacy literature on a unique user group, i.e., hosts on ASPs, by demonstrating that hosts' participation in ASPs depends on extrinsic benefits, privacy concerns, and platform features. Therefore, we provide supporting empirical evidence to earlier theoretical developments that emphasize the role of privacy calculus on an individual's self-disclosure behavior. Additionally, this study takes the first step to bridge the gap in the existing literature that has so far ignored the different dimensions of privacy concern. Our research advances this body of knowledge by showing that on ASPs, hosts can have both concerns about privacy invasions by the platform and privacy concerns from other platform users' opportunistic behaviors.

2. Literature review

2.1 Information disclosure in Accommodation Sharing Context

Past work has examined a range of issues related to individuals' willingness to disclose their personal information online in various contexts. For example, in the healthcare context, researchers find that patients' intention to disclose health-related information depends on their trust to the platform, privacy concern about the misuse of their personal health information, and the level of information sensitivity (Bansal et al. 2010). In online health communities, users disclose their health information to obtain informational and emotional support and establish a reciprocal relationship with others (Kordzadeh and Warren 2017; Zhang et al. 2018). In the e-commerce context, consumer's willingness to share private information to exchange for personalized advertising or service is determined by their purchasing experience, concerns over the process firms utilize to collect and use consumer data, consumer characteristics, and culture/climate (Awad and Krishnan 2006; Dinev and Hart 2006; Kolotylo-Kulkarni et al. 2021; Malhotra et al. 2004; Smith et al. 2011).

Prior studies have demonstrated the impacts of various drivers and barriers to information disclosure in e-commerce contexts. However, we argue that hosts' privacy concern and information self-disclosure on ASPs are significantly different from consumers' privacy concern and information self-disclosure on traditional e-commerce platforms. First, e-commerce consumers and ASPs' hosts play entirely different roles in their respective business transactions, with the former being the buyer and the latter being the seller.

Second, the information disclosed by e-commerce consumers and ASPs hosts is different. E-commerce platforms typically collect consumers' financial information (e.g., credit card, PayPal, and billing address) for payment, location information (e.g., address and zip code) for delivery services, or personalized recommendations (e.g., promotion and advertising) (Xu et al. 2011). However, information published by the hosts on ASPs is more personal and sensitive, including the hosts' contact information, belongings, properties, and intimate insights into their personal spheres (Lutz et al. 2018; Teubner and Flath 2019). Since the amount of private information released by hosts is huge and colossal, they may be more concerned about how their data will be used and protected.

Third, the audiences or recipients of the information differ in the e-commerce and ASP contexts. In the e-commerce context, consumers' credit card information and location information are kept by the business owners (e.g., the E-commerce platform firms). By contrast, in the ASP context, hosts' private information (e.g., inside view of their home, geographic information, associated facilities, and surrounding attractions) is displayed to a vast number of individuals whose integrity and trustworthiness are doubtful. Due to the nature of accommodation sharing, the assets are still possessed by the hosts after transactions. Disclosure of such private information may bring serious security problems for both hosts' personal and property safety. For example, An Atlanta Airbnb host reported to the police that guests damaged his rental home in Southwest Atlanta on New Year's Eve with a broken window, damaged appliances, and holes in the walls (Alston 2022).

Fourth, a fundamental difference between traditional e-commerce platforms and ASPs is that the former focuses on selling products/services with almost zero offline interaction, while ASPs offer accommodation services that are entirely offline. Therefore, traditional e-commerce sellers, who communicate with consumers online, involve only monetary risks, while ASPs hosts will ultimately have offline interaction with consumers, which brings more uncertainty not only for their privacy but also for their personal safety and property safety (Lutz et al. 2018). For instance, a host in San Francisco blogged about returning from a work trip to find her home ransacked. Her guests had trashed her clothes, burned her belongings, and smashed a hole through a locked closet door to steal her passport, credit card, laptop, and hard drives, as well as her grandmother's jewelry (Carville 2021).

More importantly, the motivation to release information differs between seller and buyer. From service providers' (sellers') perspective, they strategically disclose information to signal the quality of their listings in return for economic benefit and to establish a trusting relationship with consumers for social benefit through various platform design features such as visual trust by a personal photo of host and property images and textual trust by customer reviews (Bridges and Vásquez 2018; Cheng and Jin 2019; Ert et al. 2016). For instance, through an empirical analysis of Airbnb's data and a controlled experiment, researchers found that guests infer a host's trustworthiness from their visual information cue (photos) and non-visual information cue (reputation) (Ert et al. 2016). Specifically, when the host is perceived to be more trustworthy, the price of the listing and the probability of its being chosen will be higher. By contrast,

consumers share their personal information to fulfill the transaction or in exchange for monetary benefits or services (Xu et al. 2011).

The differences mentioned above indicate several limitations of extant research and have implications for theoretical examinations on privacy concerns and information disclosure in the context of accommodation sharing.

2.2 Privacy Policy Literature

Privacy policy, also named privacy statement, is a comprehensive description that companies provide to inform users of a website's information practices (Xu et al. 2011). Such policies explain to customers how websites will collect, store, and use consumers' personal data and consequently inform them about the websites' security tools and protection systems (Xu et al. 2011). The proliferation of new technologies with advanced capabilities for social features potentially incurs huge consumer concern about whether service providers properly collect and use their information. Privacy policy can inform users of service providers' practices, improve transparency, reduce information asymmetry, and help alleviate users' privacy concerns (Zhao et al. 2012).

Previous research has identified the critical role of privacy policies in building user trust. For example, Wang and Herrando (2019) found that consumers are willing to trust social-commerce sites if these sites can guarantee privacy and data protection by implementing privacy features (e.g., a privacy policy statement) and data and payment protection mechanisms. In healthcare context, patients become more likely to exchange health information when cognitive trust and emotional trust are formed (Esmaeilzadeh 2020). Other scholars have considered the effects of the privacy policy on consumers' privacy concerns. For instance, drawing upon communication privacy management theory, Xu et al. (2007) showed that individuals' perceptions of institutional privacy assurances (i.e., privacy policies and industry privacy self-regulation) are posited to negatively influence privacy concerns by strengthening user's risk control and reducing perceived risk. Additionally, some studies have investigated the impact of different dimensions of the privacy policy on users' privacy perception. For example, Guo et al. (2021) revealed that three privacy policy dimensions (i.e., transparency, control, and protection) influence the perceived effectiveness of privacy policy by enhancing perceived corporate benevolence. By contrast, privacy control positively affects the perceived effectiveness of privacy policy by reducing perceived vulnerability. Existing studies have also examined the consequences of an effective privacy policy, including users'

information disclosure, purchase intention, and willingness to be profiled. Hui et al. (2007) suggested that the presence of a privacy statement induced more people to share their personal information with the website. However, in a laboratory experiment with 206 participants, Berendt et al. (2005) argued that privacy policy has no impact on disclosure choice because consumers often do not monitor and control their actions sufficiently in online interaction. Due to the contradictory findings on the presence and strength of privacy policies in the literature, more research should be conducted to examine the specific roles of different privacy policy content in the online environment.

3. Hypotheses and model

3.1 The Impact of Privacy Policy on Hosts' Privacy Concerns

On ASPs, hosts' exposure to the risk not only derives from the platform's inability and unwillingness to protect their personal information but also derives from other platform users' opportunistic behavior. We contend that hosts' concern on ASP consist of two distinct aspects, namely, privacy concern about platform and privacy concern about user. We define privacy concern about platform as a host's concern about a platform owner's inability and unwillingness to protect his personal information from improper use, disclosure to third parties, and secondary use without the host's consent (Pavlou et al. 2007). Privacy concern about user is defined as a host's concern that other platform users may act opportunistically (Pavlou et al. 2007). Platform users' opportunism includes collecting, processing, disseminating, and invading a host's private information for unauthorized use or scam activities (Xu et al. 2011). Prior research shows that the privacy policy's completeness can alleviate users' privacy concerns over their self-disclosure online (Andrade et al. 2002; Wu et al. 2012). The privacy policies posted on the ASPs describe a varied collection of information practices to protect hosts' privacy, which can help mitigate the negative effect of privacy fears of participants on their intentions and behaviors. When hosts perceive that they are enabled by the platform to control when and how their private information is used by others, the psychological threat of privacy intrusion on information disclosure would be weakened (Olivero & Lunt 2004). Therefore, we propose the following hypotheses:

H1a: Privacy policy reduces hosts' privacy concerns about platform.

H1b: Privacy policy reduces hosts' privacy concerns about user.

3.2 The Impact of Privacy Policy on Perceived Benefits

When providing accommodation sharing services, hosts obtain economic rewards by allocating their idle resources and social benefits by establishing a friendship with travelers (Belk 2014). Privacy policy can enhance hosts' benefit prospects in the following two ways.

First, privacy literature suggested that firms' ability to influence consumers' beliefs on trust and a firm's reputation depends on whether firms can send explicit signals (e.g., privacy policy) with high clarity and credibility to consumers regarding their intention to protect privacy (Tang et al. 2008). When individuals are informed of how their private information will be handled and protected by the organization, information asymmetry will be reduced, and their trust perception towards the company will be enhanced (Esmaeilzadeh 2020; Wu et al. 2012). Thus, they will feel more comfortable and safer when doing business and making social interactions with other peers on the platform. Second, prior studies showed that resource providers will benefit more if they perceive that the platform can reach a larger number of potential customers (Teubner & Flath 2019). Trusting ASP's competence in protecting users' private information, hosts can easily deduce that other people will have similar perceptions and be willing to use the ASP, thus offering them a more extensive potential customer base. Hence, we argue that hosts will perceive more economic and social benefits if the platform can safeguard their private data by providing a comprehensive privacy policy statement. Therefore, we propose the following hypotheses:

H1c: Privacy policy increases hosts' economic benefit.

H1d: Privacy policy increases hosts' social benefit.

3.3 Host's Concerns in Accommodation Sharing Context

The transaction between host and guest on ASPs follows a two-stages process. In the first stage, host publish listing information online to advertise their properties. In this stage, as we discuss before, hosts may have privacy concern about the platform and privacy concern about the platform users. In the second stage, the transaction moves to the offline condition, in which guest live in host's property and have interaction with host. In this stage, host's concerns change from online privacy concerns to offline concern, including their personal safety concern and property safety concern. Personal safety concern is defined as a host's concern about the incidents where they may be abused, threatened or assaulted by a guest including an explicit

or implicit challenge to hosts' safety, well-being and health. For example, an Airbnb host in Dallas reported to the police one of her previous guests kept harassing her through messages and showing up around her apartment since he knew where she lives (Strapagiel 2018). Property safety concern is defined as a host's concern that any condition, practice, or violation that causes a substantial probability of property damage, loss, or misuse. For instance, an Airbnb host, who works as a photographer, reported to the police that his camera equipment and electronics were stolen by a guest, as were at least 50 percent of his clothes, his social insurance card and a photo ID, although all his valuables had been stored in locked areas (Breen, 2017).

For the hosts who have high privacy concerns on the ASP, they worry that the platform can't protect their personal information and property information effectively and may share their data with others without their authorization, which leads to negative consequences of their personal safety and property safety. Similarly, when hosts have high platform visitor concern, their trust on guests will be low, their perception of the probability that a guest may take opportunistic behavior will be enhanced, therefore, they will have more concern on their personal safety and property safety. Hence, we propose:

H2a: privacy concern about platform positively affects personal safety concern.

H2b: privacy concern about platform positively affects property safety concern.

H2c: privacy concern about user positively affects personal safety concern.

H2d: privacy concern about user positively affects property safety concern.

3.4 Privacy Calculus and Host's Information Disclosure

Privacy calculus theory is commonly employed to explain individuals' disclosure behavior (Dinev & Hart 2006; Kolotylo-Kulkarni et al. 2021; Kordzadeh & Warren 2017; Min & Kim 2015; Xu et al. 2009). Privacy calculus theory states that individuals' information disclosure intentions depend on their perceived benefit and perceived risk. People will consider sharing information if the perceived benefits of disclosure are higher or at least no less than their perceived risks.

The privacy calculus theory is widely applied to investigate the intentions to disclose information and behavior in different contexts (e.g., e-commerce, online social networks, and online healthcare). However, limited research focuses on information disclosure on ASPs. In fact, ASPs users also perform a cost-benefit analysis to decide on whether to disclose private information. Therefore, the privacy calculus model is also suitable for the analysis of information disclosure in the accommodation sharing context.

Unlike traditional e-commerce, in which transaction is commonly initiated and finished online, hosts on ASPs will have face-to-face interaction with consumers and even live together for a short term. Since the information of consumers' background and trustworthiness is inaccessible for hosts, they may concern their personal safety (e.g., harassment, stalking or discrimination.) and property safety (e.g., misuse or stolen). Hosts' offline security concerns can increase their perceived negative uncertainty, which make them less willing to publish private information online. Since individuals are always motivated to minimize negative outcomes, we expected that the behavioral intention to provide information will be low when hosts' perceptions of safety concerns are high. Therefore, we propose:

H3a: Personal safety concern negatively impacts information disclosure intention.

H3b: Property safety concern negatively impacts information disclosure intention.

In the accommodation sharing context, hosts participate in ASPs to gain economic rewards by renting out their surplus resources. In fact, about 51 percent of Airbnb hosts say that the income from hosting accommodation helps them afford their homes (Airbnb 2019). Prior literature has provided rich empirical evidence that economic benefits substantially drive individuals' information disclosure (Hui et al. 2007; Xu et al. 2009; Xu et al. 2011). In line with this research, we posit that hosts' intention to disclose information will be stronger if they perceive a high economic benefit.

Besides the economic benefit, in ASPs, hosts can also gain social benefit by getting in touch with other people, making new friends, or maintaining existing friendships (Belk 2014). When renting out a room, Airbnb hosts are open to social interaction with guests ranging from small talk to sharing a meal. The social interaction generates valuable social capital for both the hosts and guests. Besides, social interaction can also generate positive emotional support (Kang and Na 2018). Communication, smiling, eye contact with new people, or simply being in the presence of unfamiliar guests will create happy emotions for the pro-social type of individuals. We therefore state that hosts are more likely to disclose personal information when they perceive a high social benefit.

H3c: Economic benefit positively influences information disclosure intention.

H3d: Social benefit positively influences information disclosure intention.

4. Methods

4.1 Study 1: The Impact of Privacy Policy on Host's Information Disclosure Intention

4.1.1 Scale Development

We derived the measurement instruments that have been validated in prior literature and adapted them to fit the context of this research. All items are measured on a seven-point Likert scale anchored on "1 = strongly disagree" and "7 = strongly agree". We adapt four items generated by Liu et al. (2005) to measure a host's perception of the platform privacy policy. Questions pertaining to the host's privacy concern about platform and privacy concern about user are adapted from Dinev and Hart (2006). The measurement items for personal safety concern and property safety concern are adapted from Li et al. (2010) and Li et al. (2010) with four items, respectively. Economic benefit is measured with three items developed by Teubner and Flath (2019). Social benefit is measured with three items developed by Bucher et al. (2016). The dependent variable hosts' information disclosure intention is measured with three items adapted from Gefen and Straub (2003). We consider several control variables including demographic characteristics such as participants' age, gender, education, ethnicity, and annual household income. We also ask participants whether they have used any ASP before. If yes, we further ask them to specify the role to be host or guest.

4.1.2 Data Analyses and Results

A web-based questionnaire survey was developed using QuestionPro. We tested the hypotheses by conducting a cross-sectional survey on Amazon Mechanical Turk. There are 725 participants who access the survey. After removing 60 responses with incomplete data, we obtain 665 valid responses, among which 47.52% are female, about 43.61% are in the range of 25 to 34 years old, and another 26.92% are 35 to 44 years old.

The structural model was examined using SmartPLS. Our results show that 1.3% of the variance in host's privacy concern about platform, 0.1% of the variance in host's privacy concern about user, 23.4% of the variance in host's perceived economic benefit and 18.9% of the variance in host's perceived social benefit were explained by privacy policy. The variance in personal safety concern and property safety concern explained by exercise adherence and social engagement were 65.1% and 34.7%, respectively. Our results show that 40.5% of the variance in ASPs hosts' intention to

disclose information were explained by antecedent variables considered in this model.

As hypothesized, we found that the privacy policy has a significant negative influence on host's privacy concern about platform (β=-0.112, p<0.01), thus H1a is supported. However, we found no significant impact of privacy policy on host's privacy concern about user (β=-0.112, p=0.561), indicating that the existing privacy policy can only mitigate host's privacy concern about platform, but cannot reduce host's privacy concern about user, thus H1b is not supported.

Consistent with the proposed research model, privacy policy exerted significant positive influence on economic benefit (β=0.484, p<0.001). In addition, privacy policy also was found to have a significant positive effect on hosts perceived social benefit (β=0.435, p<0.001), thus H2s and H2b are supported.

As we hypothesized, a host's privacy concern about platform has significant positive impacts on personal safety concern (β=0.189, p<0.001) and property safety concern (β=0.186, p<0.01), therefore H3a and H3b are supported. Similarly, we found that the impacts of a host's privacy concern about user on personal safety concern (β=0.655, p<0.001) and property safety concern (β=0.433, p<0.001) are significant. Hence, H3c and H3d are supported.

In terms of the dependent variable in the research model, we found that economic benefit (β=0.162, p<0.001) and social benefit (β=0.482, p<0.001) both have positive influences on a host's information disclosure intention, hence, H4c and H4d are supported. However, personal safety concern did not have a significant impact on disclosure intention (β=-0.152, p<0.001). Therefore, H4a is not supported. Property safety concern was found to have a significant negative impact on the hosts' information disclosure intention (β=-0.152, p<0.001), thus H4b is supported.

Besides age, we found no significant impact of control variables on a host's intention to disclose private information on ASPs. Age was found to have a negative influence on host's information disclosure intention (β=-0.079, p<0.05), suggesting that young people are more willing to share private information on ASPs than old people.

4.2 Study 2: The Differential Impacts of Privacy Policy

Study 1 demonstrates that the existing ASP privacy policy can significantly address a host's concern about platform's privacy invasion but cannot mitigate a host's privacy concern about other users' opportunistic behavior. To check the generalizability of this issue, we further collected fifty privacy policies from most

popular ASPs according to Global Alexa Ranking, including Airbnb, VRBO, Couchsurfing among others. After scrutinizing each privacy policies, we find that the ASPs' privacy policies contain similar provisions, which only concentrate on the platform's data management practice but overlook the importance of safeguarding the hosts' privacy from being misused by other platform users.

To shed light on the direction of improving the privacy policy, and to understand how different privacy policy content influence the hosts' privacy concerns, we design a scenario-based 2 (high/low platform-focused clauses) x 2 (high/low platform user focused clauses) between-subjects factorial experiment to study how different protection levels of privacy policies applicable to the platform and those applicable to the platform users influence hosts' privacy concerns, perceived benefits, and information disclosure intention. Given the void of real data and empirical evidence, our controlled experiment is a feasible and appropriate approach to investigate the problem. We define platform-focused clauses as the provisions that regulate platform-related behavior in the privacy policy, while user-focused clauses refer to the provisions that regulate platform user-related behavior in the privacy policy. Specifically, the study consists of four groups of participants whose privacy is protected by the high platform-focused clauses and high user-focused clauses (HH), high platform-focused clauses and low user-focused clauses (HL), low platform-focused clauses and high user-focused clauses (LH), and low platform-focused clauses and low user-focused clauses (LL) in the privacy policy.

4.2.1 Participants

A total of 433 participants from Amazon's Mechanical Turk (MTurk) completed the experiment and were each paid $0.50. Participants were recruited by employing the built-in qualification features on MTurk. To generate high quality data from MTurk, we followed Peer et al.' (2014) criteria to hire participants who resided in the United States and had completed at least 500 Human Intelligence Tasks (HITs) with an approval rate greater than 95%. The study was advertised as taking 5-10 minutes (the average participant completed the study in about 7 minutes).

4.2.2 Experimental Treatment Conditions

This study aims to understand how users' perception of privacy policy influences their intention to disclose information on the ASP. Participants are given the role to be ASP host. First, to help participants understand what information would be shared on the platform, they were given an example of the ASP listing and were told that their posts on the ASP include sensitive private personal information such as their names, face picture, occupation, hobby, and other background information and property information such as rough property address, pictures of the inside view of their apartment, and the surroundings of the property.
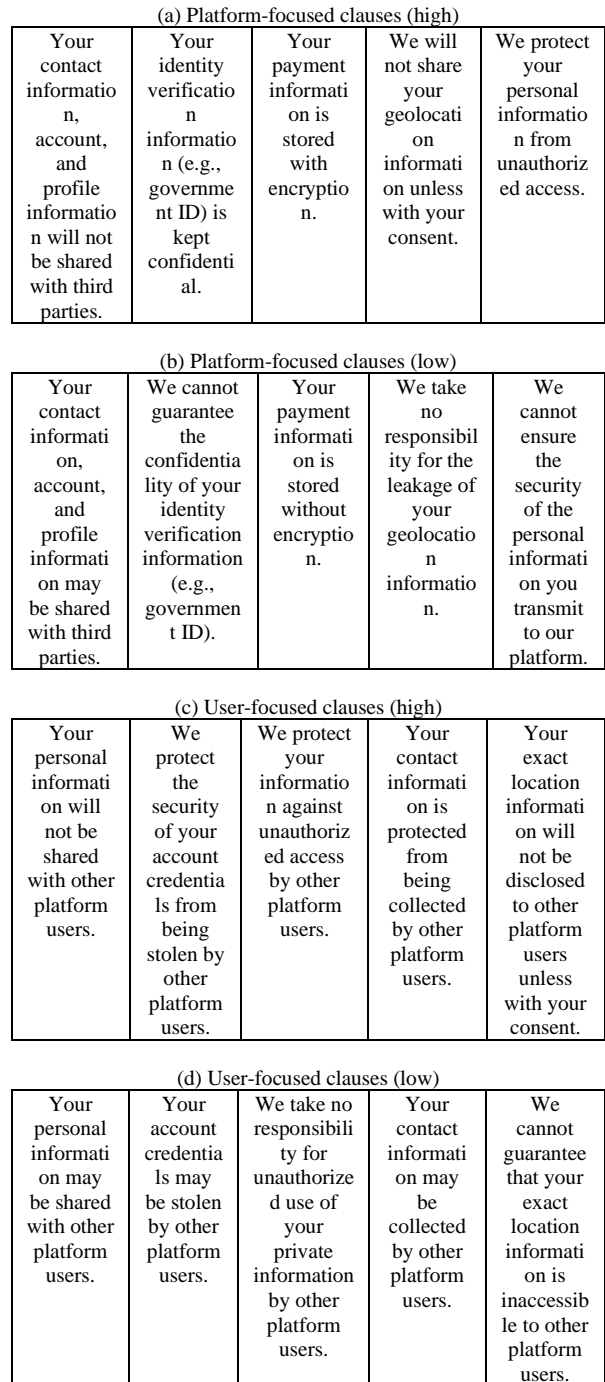
(a) Platform-focused clauses (high)

Your contact information, account, and profile information will not be shared with third parties.	Your identity verification information (e.g., government ID) is kept confidential.	Your payment information is stored with encryption.	We will not share your geolocation information unless with your consent.	We protect your personal information from unauthorized access.

(b) Platform-focused clauses (low)

Your contact information, account, and profile information may be shared with third parties.	We cannot guarantee the confidentiality of your identity verification information (e.g., government ID).	Your payment information is stored without encryption.	We take no responsibility for the leakage of your geolocation information.	We cannot ensure the security of the personal information you transmit to our platform.

(c) User-focused clauses (high)

Your personal information will not be shared with other platform users.	We protect the security of your account credentials from being stolen by other platform users.	We protect your information against unauthorized access by other platform users.	Your contact information is protected from being collected by other platform users.	Your exact location information will not be disclosed to other platform users unless with your consent.

(d) User-focused clauses (low)

Your personal information may be shared with other platform users.	Your account credentials may be stolen by other platform users.	We take no responsibility for unauthorized use of your private information by other platform users.	Your contact information may be collected by other platform users.	We cannot guarantee that your exact location information is inaccessible to other platform users.

Figure 2. Levels of Privacy Protection

Table 1. ANOVA Results						
Dependent variables	Platform-focused clauses		F	User-focused clauses		F
	High	Low		High	Low	
Privacy concern about platform	4.65 (1.37)	5.42 (1.19)	41.27***	5.14 (1.26)	4.95 (1.40)	2.91
Privacy concern about user	4.95 (1.35)	5.17 (1.24)	3.16	4.79 (1.28)	5.34 (1.26)	18.94***
Number of observations	210	223		220	213	
Note: * significant at p<0.05 level; ** significant at p<0.01 level; *** significant at p<0.001 level.						

Second, to better observe the influence of privacy policy on participants' privacy concerns and disclosure intention, we control their privacy concerns to be high by giving them some newspaper reports containing examples of how guests misappropriate hosts' private information posted on ASPs in the past. All participants were given the same information at the beginning of the experiment. After they read the instruction and newspaper reports, they were given a description of the privacy policy, including platform-focused clauses and user-focused clauses which were described using a figure that showed, on five parameters, the degree to which participants' privacy would be protected (see Figure 2).

In each condition, once the participants read the information on the privacy policy, as a manipulation check, they were asked to report their satisfaction with the two types of clauses separately. Finally, participants were asked to complete a questionnaire that measures their perceptions of privacy concern about platform and privacy concern about user.

4.2.3 Results

We first conducted the manipulation checks. The independent sample t-test shows a significant effect for perceived satisfaction of platform-focused clauses (two-tailed t=7.39, p<0.001). Another independent sample t-test shows a significant effect for perceived satisfaction of user-focused clauses (two-tailed t=7.61, p<0.001). In sum, both platform-focused clauses and user-focused clauses manipulations are successful.

The experiment results are summarized in Table 1. Specifically, the main effect of platform-focused clauses on privacy concern about platform was significant (F= 41.27, p<0.001). The main effect of user-focused clauses on privacy concern about platform was not significant (F=2.91, p=0.09). To explore the impacts of platform-focused clauses and user-focused clauses on privacy concern about user, a two-way ANOVA was performed with privacy concern about user as the dependent measure. The main effect of user-focused clauses on privacy concern about user was significant (F=18.94, p<0.001). The main effect of platform-

focused clauses on privacy concern about user was not significant (F=3.16, p=0.08).

5. Discussion and conclusion

This study makes several important contributions to privacy and information disclosure literature. First, our proposed model explains hosts' decision-making by viewing privacy policy as a key role in the context of ASPs. Specifically, we focus on privacy policy as the antecedent of hosts' motivational factors, and we further examine how different concerns and benefits affect hosts' decision-making processes. Second, we differentiate general online privacy concerns into privacy concern about platform and privacy concern about user. Our results in study 1 show that the existing privacy policy cannot effectively mitigate hosts' concerns about other platform users' opportunistic behavior. Third, we conducted an experiment to test the influence of different privacy clauses on hosts' privacy concern and disclosure intentions. Consistent with our expectations, the results show that platform-focused clauses can significantly reduce hosts' privacy concern about platform. Meanwhile, user-focused clauses can significantly reduce hosts' privacy concerns about platform user.

The findings of this study provide several guidelines on privacy policy design and implementation in practice. First, policymakers should recognize that users' perception of privacy concerns will be greatly reduced when the privacy policy is comprehensive. Thus, policymakers can consider the two types of privacy policy clauses as the criteria when evaluating the effectiveness of a privacy policy. Additionally, the results show that different privacy clauses do not necessarily exert the effects on privacy concerns in the same way. It is worth noting that both types of privacy clauses can influence individuals' intention to disclose personal and property information. Second, ASP hosts' intentions to disclose their private information are based on the trade-off between their privacy concerns and the benefits of information disclosure. Therefore, hosts must adequately handle the risk of potential negative outcomes of releasing information. Third, a novel aspect

of accommodation sharing service is to provide opportunities for meeting new people and creating rewarding interpersonal communications. From platform owners' perspective, they actively emphasize and advertise such social value by offering travelers a sense of belonging and local experience. Therefore, it is essential for policymakers to complement the existing privacy policy by including comprehensive provisions to guard against platform users' opportunistic behavior in order to promote hosts' social activities.

6. References

Airbnb. (2019). Airbnb Estimated Direct Economic Impact Exceeds $100 Billion in One Year. (https://news.airbnb.com/airbnb-estimated-direct-economic-impact-exceeds-100-billion-in-one-year/)

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. Association for Consumer Research, 29, 350-353.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. European Journal of Information Systems, 24(6), 624-644.

Belk, R. (2014). You are what you can access: Sharing and collaborative consumption online. Journal of Business Research, 67(8), 1595-1600.

Böcker, L., & Meelen, T. (2017). Sharing for people, planet or profit? Analyzing motivations for intended sharing economy participation. Environmental Innovation and Societal Transitions, 23, 28-39.

Bridges, J., & Vásquez, C. (2018). If nearly all Airbnb reviews are positive, does that make them meaningless? Current Issues in Tourism, 21(18), 2065-2083.

Bucher, E., Fieseler, C., & Lutz, C. (2016). What's mine is yours (for a nominal fee)–Exploring the spectrum of utilitarian to altruistic motives for Internet-mediated sharing. Computers in Human Behavior, 62, 316-326.

Cheng, M., & Jin, X. (2019). What do Airbnb users care about? An analysis of online review comments. International Journal of Hospitality Management, 76, 58-70.

DecisionMaking. (2020). "Airbnb sleepwalks into breach of hosts' personal data," (https://www.decisionmarketing.co.uk/news/airbnb-sleepwalks-into-breach-of-hosts-personal-data)

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), 61-80.

Esmaeilzadeh, P. (2020). The effect of the privacy policy of Health Information Exchange (HIE) on patients' information disclosure intention. Computers & Security, 95, 101819.

Gefen, D., & Straub, D. (2003). Managing user trust in B2C e-services. e-Service, 2(2), 7-24.

Guesty. (2015). The Social Benefits of Renting out a Room on Airbnb. Guesty. (https://www.guesty.com/blog/social-benefits-of-renting-out-room-airbnb/)

Guo, Y., Wang, X., & Wang, C. (2021). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. Journal of Enterprise Information Management, 35(3), 774-795.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Quarterly, 37(1), 275-298.

Hu, J., He, W., & Davis, F. (2020). When Hosts Disclose Their Private Information on Accommodation Sharing Platforms: An Information Commercialization Perspective. in Proceedings of the 53rd Hawaii International Conference on System Sciences.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment," MIS Quarterly, 31(1), 19-33.

Kang, S., & Na, Y. K. (2018). The effect of the relationship characteristics and social capital of the sharing economy business on the social network, relationship competitive advantage, and continuance commitment. Sustainability, 10(7), 1-22.

Keh, H. T., & Xie, Y. (2009). Corporate reputation and customer behavioral intentions: The roles of trust, identification and commitment. Industrial marketing management, 38(7), 732-742.

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. Journal of Business Research, 126, 221-238.

Kordzadeh, N., & Warren, J. (2017). Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. Journal of the Association for Information Systems, 18(1), 45-81.

Krasnova, H., Abramova, O., Fuhrer, A., Shavanova, T., & Buxmann, P. (2015). Understanding the Sharing Economy: The Role of Response to Negative Reviews in the Peer-To-Peer Accommodation Sharing Network? in Proceeding of 23rd European Conference on Information Systems.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. Journal of Computer Information Systems, 51(1), 62-71.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Information & Management, 42(2), 289-304.

Lock, S. (2020). Short-term rental home sharing users in the US 2019-2023. (https://www.statista.com/statistics/1191533/home-sharing-economy-users-us/#statisticContainer)

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. Information, Communication & Society, 21(10), 1472-1492.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336-355.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social

network sites? The calculus between benefit and cost. Journal of the Association for Information Science and Technology, 66(4), 839-857.

Möhlmann, M. (2015). Collaborative consumption: determinants of satisfaction and the likelihood of using a sharing economy option again. Journal of Consumer Behavior, 14(3), 193-207.

Müller, M., Neumann, J., & Kundisch, D. (2022). Peer-To-Peer Rentals, Regulatory Policies, And Hosts' Cost Pass-Throughs. Journal of Management Information Systems, 39(3), 834-864.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, 25(2), 243-262.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS Quarterly (31:1), 105-136.

Smith, A. (2016). Shared, Collaborative and on Demand: The New Digital Economy. Pew Research Center. (https://www.pewresearch.org/internet/2016/05/19/shared-home-sharing-services/#:~:text=In%20total%2C%20roughly%20one%2Din,as%20Airbnb%2C%20VRBO%20or%20HomeAway)

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), 989-1015.

Tang, Z., Hu, Y.J., & Smith, M.D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory