Industrial Marketing Management 107 (2022) 161–175

Contents lists available at ScienceDirect

Industrial Marketing Management

journal homepage: www.elsevier.com/locate/indmarman

How privacy practices affect customer commitment in the sharing economy: A study of Airbnb through an institutional perspective

Shijiao (Joseph) Chen [a], Kuttimani Tamilmani [b,*], Khai Trieu Tran [c], Donia Waseem [b], Vishanth Weerakkody [b]

[a] Macquarie University, 4 Eastern Road, NSW 2109, Australia
[b] University of Bradford, Richmond Rd, Bradford BD7 1DP, United Kingdom
[c] University of Economics - The University of Danang, 71 Ngu Hanh Son Street, Danang 550000, Viet Nam

ARTICLE INFO

Keywords:
Sharing economy
Institutions
Legitimacy judgement
Privacy
Business-to-business marketing

ABSTRACT

Privacy is an emerging issue for home-sharing platforms such as Airbnb. Home-sharing providers (business customers) are subject to both digital privacy risks (e.g., data breaches and unauthorized data access) and physical privacy risks (e.g., property damage and invasion of their personal space). Therefore, platforms need to strengthen their institutions of privacy management to protect the interests of providers and maintain their commitment. By applying the micro-level psychological aspect of institutional theory, our research investigates how providers decide their level of commitment to a platform by evaluating the institutions of the platform's privacy management. Our survey recruited 380 Airbnb providers from the Prolific panel. Structural equation modelling analysis shows that both physical and digital privacy practices strengthen providers' legitimacy judgement of the platform's privacy management and subsequently increase their commitment to the platform. Our theoretical contribution lies in revealing the effects of physical and digital privacy practices on B2B relationships from an institutional perspective. Our research is among the first to provide an integrative framework illustrating providers' psychological process of legitimacy judgement. It also has practical implications for sharing economy platforms to manage privacy.

1. Introduction

While the sharing economy creates many business opportunities, it also raises concerns about privacy. On home-sharing platforms such as Airbnb, privacy has both digital and physical forms because the interactions between providers (i.e., hosts), guests, and the platform take place in both digital and physical environments (Ranzini, Etter, & Vermeulen, 2020). After relinquishing personal information to platforms, providers (business customers in our research) may be subject to *digital* privacy risks such as data breaches and unauthorized data access (Chatterjee & Kar, 2018; Kar, 2020; Martin et al., 2020; Martin, Borah, & Palmatier, 2017). For example, there have been cases in which Airbnb providers' account data were leaked to other business parties (Forums, 2020). In addition to digital privacy risks, providers are vulnerable to *physical* privacy risks because their relationship with guests extends to the physical environment they share (Hamari, Sjöklint, & Ukkonen, 2016; Ranzini et al., 2020). Physical privacy risks include guests invading providers' personal space or damaging their property (D'Acunto, Volo, & Filieri, 2021; Ranzini et al., 2020). For instance, there have been news reports about Airbnb guests wrecking providers' properties and even committing crimes there (DailyMail, 2021; NZHerald, 2021).

Previous privacy studies have focused primarily on digital privacy (Janakiraman, Lim, & Rishika, 2018; Lwin, Wirtz, & Williams, 2007; Martin et al., 2017). However, exposure to both digital and physical privacy risks is unique to the home-sharing context, and their combined impact is understudied (D'Acunto et al., 2021; Ranzini et al., 2020). Privacy risks make providers (business customers) feel vulnerable and damage their relationship with home-sharing platforms. To avoid this outcome, platforms need to manage privacy risks carefully (Jain, Dash, Kumar, & Luthra, 2021; Liu, Pavlou, & Cheng, 2021; Mir, Kar, Dwivedi, Gupta, & Sharma, 2020), especially by improving their institutions of privacy management (Lu, Wang, & Zhang, 2021). Institutions are structures of regulations, conduct norms, and ethical beliefs that guide

* Corresponding author.
E-mail addresses: joseph.chen@mq.edu.au (S.(J. Chen), k.tamilmani@bradford.ac.uk (K. Tamilmani), trantrieukhai@due.edu.vn (K.T. Tran), d.waseem@bradford.ac.uk (D. Waseem), v.weerakkody@bradford.ac.uk (V. Weerakkody).

https://doi.org/10.1016/j.indmarman.2022.08.020
Received 30 September 2021; Received in revised form 16 August 2022; Accepted 24 August 2022
Available online 8 October 2022

business activities and protect the interests of stakeholders, including, in this case, home-sharing providers (Chen, Zhang, Gao, Yang, & Mather, 2022; Scott, 1995; Zhang, Deephouse, van Gorp, & Ebbers, 2020). Therefore, platforms' institutions of privacy management play a vital role in facilitating interactions and building relationships with providers. For example, Airbnb has formulated privacy policies; implemented guest verification as well as guest review and compensation procedures; and employs customer service staff with a background in the provision of emergency services (Bloomberg, 2021).

Institutional theory (e.g., Scott, 1995; Suchman, 1995) provides insights into the institutions of home-sharing platforms' privacy management. Recent studies have applied the micro-level psychological aspect of institutional theory, which evaluates how individual stakeholder audiences (e.g., investors, managers, and employees) respond to institutional entities in the context of organizational research and business-to-consumer (B2C) research (Bitektine, 2011; Bitektine & Haack, 2015; Suddaby, Bitektine, & Haack, 2017; Tost, 2011; Zhang et al., 2020). For example, Chen et al. (2022) investigate the psychological process through which consumers as individual stakeholder audiences decide to support or challenge companies based on their evaluation of the institutions of these companies' product safety management systems. By extending this emerging aspect of institutional theory to business-to-business (B2B) research, we argue that providers are stakeholder audiences of the institutions of a platform's privacy management, because these institutions include both physical and digital privacy practices as key institutional mechanisms to mitigate potential risks. We therefore address the following research question: *How do providers decide their level of commitment to a platform based on their perceptions and evaluations of its institutions of privacy management?*

By investigating this question, our research has the potential to advance the understanding on privacy in B2B research and adds to the micro-level psychological aspect of institutional theory. It also has implications for home-sharing platforms to improve privacy management and develop good relationships with business customers (e.g., providers). Specifically, it provides home-sharing platforms with a nuanced understanding of both digital and physical privacy practices from an institutional perspective.

The remainder of the paper proceeds as follows. First, we review the literature and develop a conceptual model to illustrate how home-sharing providers decide their commitment to the platform based on their perceptions and evaluations of the institutions of its privacy management. Second, we introduce the survey method and conduct structural equation modelling (SEM) to test the conceptual framework. Third, we discuss the theoretical implications of our findings and provide practical guidance on how to address physical and digital privacy risks in the home-sharing economy.

2. Literature review

Privacy has become a serious concern in the sharing economy. Uniquely in the home-sharing market, privacy risks take on both digital and physical forms (Ranzini et al., 2020). *Digital* privacy is defined as customers' concern over the dissemination and use of their information (Chatterjee & Kar, 2018; Jaap, Xiao, Thomas, Hans, & Bernd, 2019; Kar, 2020; Martin & Murphy, 2017). Digital privacy is relevant when online platforms use customer data to improve their services, provide personalization, and even profit from using data for advertising purposes or selling them to other parties (Martin & Murphy, 2017). In recent years, many customers have become wary of companies that collect and use their data (Kim, Barasz, & John, 2019) and are concerned about digital privacy risks such as data access and data breaches (Martin et al., 2017; Mpinganjira & Maduku, 2019; Nunan & Di Domenico, 2017).

In addition to digital privacy, providers must safeguard their *physical* privacy, as their interactions with guests occur in a physical environment. Risks affecting physical privacy include damage to providers' property and invasion of their personal space (D'Acunto et al., 2021; Ranzini et al., 2020). If these privacy risks are not addressed adequately, they could undermine providers' confidence in the platform and their willingness to continue to participate in the sharing economy (Lu et al., 2021).

To mitigate privacy risks, platforms must implement privacy practices as institutional mechanisms that create a reliable and secure transactional environment (Liu et al., 2021; Lu, Fan, & Zhou, 2016; Lu, Zeng, & Fan, 2016; Lwin et al., 2007). Many home-sharing platforms specify *privacy practices* on how to collect, use, and store customer data (i.e., *digital* privacy practices), and how to handle issues related to damage and harassment (i.e., *physical* privacy practices). Our literature review shows that previous research on privacy has addressed mostly digital privacy practices rather than physical privacy practices while examining the consequences of privacy practices in the B2C context rather than the B2B context (Lwin et al., 2007; Martin et al., 2017; Wang, Asaad, & Filieri, 2020). In addition, prior studies have not investigated how business customers (e.g., providers) evaluate the institutions of firms' privacy management and the effects of this evaluation on B2B relationships (see Table 1).

To fill these research gaps, we adopt a micro-level psychological aspect from institutional theory—legitimacy as judgement. This aspect focuses on the psychological dynamics of individual stakeholder audiences, especially how they evaluate the institutions that underlie organizations' management practices and decide to support or challenge them (Bitektine, 2011; Bitektine & Haack, 2015; Suddaby et al., 2017; Tost, 2011). In the home-sharing economy, providers are key stakeholder audiences of the institutions of privacy management, because they expect these institutions to protect their interests from potential privacy risks. The literature on legitimacy as judgement suggests that stakeholder audiences need to undergo a three-stage psychological process—comprised of perception, judgement, and decision—before taking formal actions toward the observed organization (Bitektine, 2011; Tost, 2011). Applying this notion to our context, providers need to perceive the platform's privacy management and judge how well it upholds institutions to manage privacy risks. Known as "legitimacy judgement", this evaluative judgement helps stakeholder audiences (the providers in our research context) assess whether the actions of the organization are consistent with their expectations in their social context (Chen et al., 2022; Finch, Deephouse, & Varella, 2015). Many prior studies have shown that positive legitimacy judgements made by stakeholder audiences can contribute to desirable relational outcomes (Chen, Gao, & Zhang, 2021; Chen, Wright, Gao, Liu, & Mather, 2021; Finch et al., 2015).

2.1. Privacy practices as key institutional mechanisms

To mitigate privacy risks and maintain providers' commitment, platforms need to implement privacy practices (Liu et al., 2021; Lwin et al., 2007). Platforms have specific *digital* privacy practices for collecting, storing, and using customer data and communicating their privacy policies (Kar, 2020; Khan, Ibrahim, & Hussain, 2021; Martin et al., 2017; Martin et al., 2020). Platforms like Airbnb also have *physical* privacy practices such as guest verification, guest review, and compensation to manage the physical risks to providers (Airbnb, 2021a, 2021b, 2021c, 2021d).

2.1.1. Digital privacy practices

Home-sharing platforms require providers to disclose their personal information and details of their services to target potential guests effectively (Tussyadiah, 2016). Personal information in digital format can be easily copied, transmitted, and used by other parties, posing serious digital privacy risks (Malhotra, Kim, & Agarwal, 2004). For instance, providers may find their digital privacy infringed upon by other parties who learn about their living conditions, personal interests and tastes, and even intimate information (Lutz & Newlands, 2018). Drawing on gossip theory in the digital privacy literature (Martin et al.,

Table 1
Empirical studies on privacy from an institutional perspective.

Article	Methods	Explored the B2B context	Explored digital privacy	Explored physical privacy	Explored institutional constructs (e.g., legitimacy)	Explored relational outcomes (e.g., commitment)
Our research	Quantitative (survey)	Yes. Airbnb and its hosts	Yes	Yes	Yes	Yes
Afriat, Dvir-Gvirsman, Tsuriel, and Ivan (2020)	Qualitative (interviews)	No. B2C (social media)	Yes	No	Yes (legitimacy)	No
Alge, Ballinger, Tangirala, and Oakley (2006)	Quantitative (survey)	No. Organizational behaviour	Yes	No	Yes (legitimacy)	No
Bellamy, Raab, Warren, and Heeney (2007)	Qualitative (interviews)	No. Public administration	Yes	No	No	No
Chin, Harris, and Brookshire (2022)	Quantitative (survey)	No. B2C (mobile payment systems)	Yes	No	No	No
Dinev et al. (2006)	Quantitative (survey)	No. B2C (e-commerce)	Yes	No	Yes (institutional trust)	No
Esmark Jones, Stevens, Noble, and Breazeale (2020)	Quantitative (experiment)	No. B2C (retail)	Yes	No	Yes (legitimacy)	Yes (satisfaction)
Gao (2007)	Qualitative (case study)	No. Information system	Yes	No	No	No
Hine (1998)	Qualitative (interviews)	No. B2C (shopping)	Yes	No	Yes (legitimacy)	No
Jackson (2014)	Qualitative (case study)	No. Public administration	Yes	No	Yes (legitimacy)	No
Jozani, Ayaburi, Ko, and Choo (2020)	Quantitative (survey)	No. B2C (social media-enabled application)	Yes	No	Yes (institutional privacy concerns)	Yes (engagement)
Kropp and Totzek (2020)	Quantitative (survey)	Yes. B2B firms	Yes	No	Yes (perceived institutional pressure)	No
Kwak, Lee, and Lee (2022)	Qualitative (content analysis)	No. B2C (a general online context)	Yes	No	No	No
Lansing, Benlian, and Sunyaev (2018)	Qualitative (interviews)	No. B2C (information systems)	Yes	No	Yes (legitimacy)	No
Xu, Dinev, Smith, and Hart (2011)	Quantitative (survey)	No. B2C (websites)	Yes	No	No	No
Wang, Sun, Dai, Zhang, and Hu (2019)	Quantitative (survey)	No. B2C (social media)	Yes	No	No	No

Note: The literature search was conducted on Web of Science based on the combination of the following keywords: “institutional theory”, “privacy”, and “legitimacy”. For quality control purposes, we searched empirical articles in leading journals (ranked 3 and above by the Chartered Association of Business Schools) in the areas of hospitality, tourism, marketing, public administration, and information management.

2017), we focus on *privacy assurance* and *privacy control* because they are the most critical digital privacy practices to reduce privacy risks in the online environment. *Privacy assurance* refers to the provision of transparent policies to ensure that providers' digital privacy is protected (Lutz, Hoffmann, Bucher, & Fieseler, 2018; Xu et al., 2011), while *privacy control* means allowing providers to manage their personal data (Mpinganjira & Maduku, 2019; Tucker, 2014).

2.1.2. Physical privacy practices

Providers invite guests to stay in their “private spaces” and give them access to their furniture and appliance, leading to re-negotiation of their physical private boundaries (D'Acunto et al., 2021; Ranzini et al., 2020). Guests may invade the provider's personal space or cause damage to their property, resulting in physical privacy risks and harm (Lutz et al., 2018). Built on the theory of the extended self (e.g., Belk, 1988), physical privacy refers to how “an individual's identity and sense of self extend to persons, places, and things that they recognize as ‘their own’” (Ranzini et al., 2020, p. 2). Based on this notion, we searched the literature on physical privacy practices and identified three important practices that are suitable in our research context: *guest verification* (checking guests' background and certification and performing screening; e.g., Shao & Yin, 2019), *a two-way review system* (hosts and guests review each other; e.g., Liang, Schuckert, Law, & Chen, 2020), and *compensation* (guarantees and insurance to protect hosts and their belongings; e.g., Johnston & Michel, 2008).

Recent studies view these privacy practices as platforms' key institutional mechanisms to mitigate risks (e.g.,Lu et al., 2021; Newlands & Lutz, 2020). These mechanisms act as social structures to guide platforms' actions and ensure they are consistent with their social context (e.g., Scott, 1995; Suchman, 1995). According to the micro-level psychological aspect of institutional theory, institutional mechanisms help platforms create a trust-based interactive environment in the sharing economy and thus increase customers' continuous use intentions (Lu et al., 2021; Newlands & Lutz, 2020). We thus propose that institutional mechanisms, including physical and digital privacy practices, contribute to the legitimacy of the platform's overall privacy management and help the platform maintain good relationships with its providers.

2.2. Legitimacy judgements of the platform's privacy management and effects on B2B relationships

Providers pay close attention to the institutional mechanisms of the platforms' privacy management because these mechanisms reduce privacy risks and protect their interests (Lu et al., 2021; Xu et al., 2011). According to the micro-level psychological aspect of institutional theory, we consider providers as stakeholder audiences of the institutional mechanisms of platforms' privacy management. Prior research shows that stakeholder audiences undergo a psychological process—which includes experiencing perceptions and making judgements and decisions—prior to formally responding to the observed organizations (Bitektine, 2011; Tost, 2011). For example, consumers of a company need to perceive its practices and management systems, make legitimacy judgements, and then formulate behavioural responses toward that company (Chen et al., 2022; Guo, Tao, Li, & Wang, 2017).

Institutional studies have identified two forms of legitimacy judgement: pragmatic legitimacy and socio-political legitimacy (Zhang et al., 2020). Pragmatic legitimacy is developed when stakeholders' self-interest is satisfied (Guo et al., 2017; Suchman, 1995). In our research context, *pragmatic legitimacy* refers to providers' evaluation that in which extent the platform's privacy management benefits them and meets their utilitarian expectations. Socio-political legitimacy comprises both moral and regulatory components (Zhang et al., 2020). Aldrich and Fiol (1994, p. 648) refer to socio-political legitimization as "the process by which key stakeholders, the general public, key opinion leaders, or government officials accept a venture as appropriate and right, given existing norms and laws". Therefore, we define *socio-political legitimacy* as providers' evaluation of whether the platform's privacy management is consistent with legal requirements and social standards.

From a micro-level psychological point of view, stakeholder audiences' legitimacy judgement of an organization influences their decisions of forming a relationship with it (Chen et al., 2022). For a platform with a high degree of legitimacy, its practices and management are seen as being socially appropriate and consistent with the rule of law, norms, standards, values, and beliefs (Chen et al., 2022; Suchman, 1995). Proper practices and management reduce privacy risks, protect providers' interests, and gain their trust and confidence. As a result, customers generally tend to develop trust and positive relationships with the platform (Chen et al., 2022; Guo et al., 2017).

The relationship marketing literature demonstrates that customer commitment is central to relational exchanges between a consumer and a business, as it represents the strength of the relationship (Morgan & Hunt, 1994). In this research, to examine the effects of legitimacy judgement on B2B relationships precisely, we evaluate commitment by examining two different and sometimes incompatible forms—affective commitment and calculative commitment. *Affective commitment* refers to the intention to continue a relationship with the other party due to positive feelings and attachment (Zaefarian, Thiesbrummel, Henneberg, & Naudé, 2017). *Calculative commitment*, on the other hand, refers to the desire to maintain a relationship with the other party based on a rational and economic calculation because terminating the relationship could cause undesirable losses (Gilliland & Bello, 2002).

3. Conceptual model and hypothesis development

Our research develops a conceptual framework to illustrate the micro-level psychological processes through which providers decide their level of commitment to a platform based on their perceptions and evaluations of the institutions of the platforms' privacy management (see Fig. 1). In institutional theory, the literature on legitimacy as judgement suggests that perceptions, judgements, and decisions are the three psychological stages through which stakeholder audiences respond to organizations in an institutional context (Bitektine, 2011; Chen et al., 2022; Tost, 2011). Therefore, our research adopts this three-stage process to investigate the psychological dynamics of providers. We propose that, at the perception stage, providers perceive the platform's digital and physical privacy practices. After that, they make legitimacy judgements about the platform's privacy management based on its privacy practices (judgement stage) and apply the judgement outcomes to decide their level of commitment to the platform (decision stage).

3.1. Perceptions of privacy practices and legitimacy judgement

Our research proposes that both digital and physical privacy practices act as key institutional mechanisms and contribute to the legitimacy of a platform's privacy management, which helps the platform maintain commitment from providers. In the following sections, we discuss digital privacy practices and physical privacy practices, and propose that providers' perceptions of the effectiveness of these privacy practices influence their legitimacy judgement of the platform's privacy management.

3.1.1. Perceptions of digital privacy practices and legitimacy judgement

Privacy assurance. In the sharing economy, a platform's privacy assurance helps providers understand the collection and usage of their data, perceive the privacy practices as being transparent and fair, and feel that their digital privacy is protected (Martin et al., 2017; Xu et al.,

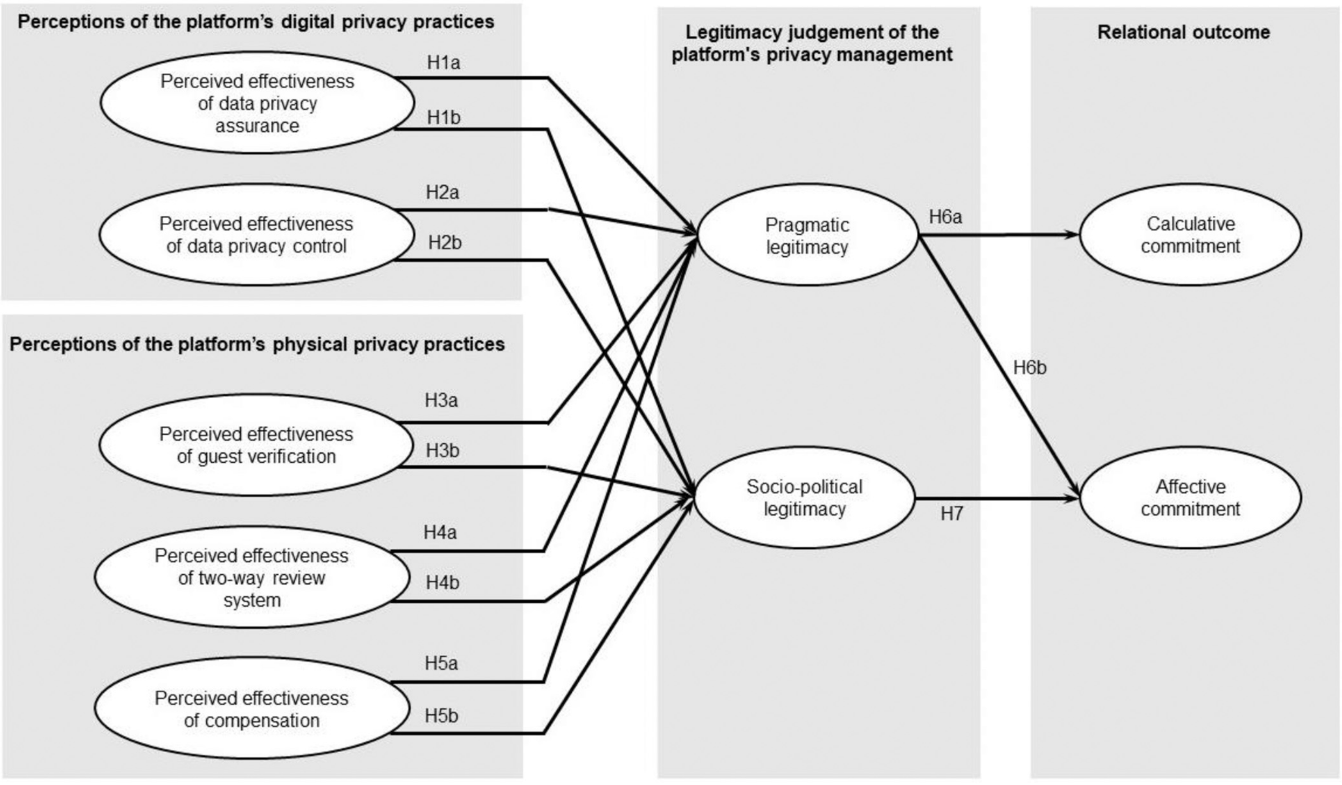

Perceptions of the platform's digital privacy practices
Perceived effectiveness of data privacy assurance
Perceived effectiveness of data privacy control
Perceptions of the platform's physical privacy practices
Perceived effectiveness of guest verification
Perceived effectiveness of two-way review system
Perceived effectiveness of compensation
H1a
H1b
H2a
H2b
H3a
H3b
H4a
H4b
H5a
H5b
Legitimacy judgement of the platform's privacy management
Pragmatic legitimacy
Socio-political legitimacy
H6a
H6b
H7
Relational outcome
Calculative commitment
Affective commitment

Fig. 1. Conceptual model.

2011). As providers' utilitarian expectations are met, privacy assurance contributes to pragmatic legitimacy. In addition, privacy assurance indicates that platforms' digital privacy practices are self-regulated, overseen by other parties, and comply with norms and standards (Walker, 2016), thus contributing to socio-political legitimacy. We posit the following hypothesis:

H1. Perceived effectiveness of privacy assurance is positively related to pragmatic legitimacy (H1a) and socio-political legitimacy (H1b).

Privacy control. Platforms have privacy control settings that determine the extent to which customers can control their data as a way of protecting their digital privacy (Martin et al., 2017). The perceived effectiveness of privacy control is the perception of the extent to which a platform allows users to manage their personal data (Mpinganjira & Maduku, 2019; Tucker, 2014). Control enables individuals to manage their environment in order to protect their self-interest and achieve desirable outcomes (Bandara, Fernando, & Akter, 2020), thus contributing to pragmatic legitimacy. Effective privacy control policies and settings also demonstrate that the platform adheres to industry standards and abides by legal requirements on data security (Gabisch & Milne, 2014; Martin et al., 2017), which helps the platform gain socio-political legitimacy. We therefore propose the following hypothesis:

H2. Perceived effectiveness of privacy control is positively related to pragmatic legitimacy (H2a) and socio-political legitimacy (H2b).

3.1.2. Perceptions of physical privacy practices and legitimacy judgement

Guest verification. In the home-sharing economy, platforms are expected to ensure that all providers and guests are qualified, eligible individuals who will not pose physical privacy risks to others. To achieve this outcome, platforms can implement rigorous verification procedures, including background checks, screening, and certification (Shao & Yin, 2019; Ter Huurne, Ronteltap, Corten, & Buskens, 2017). For example, Airbnb has introduced a guest verification mechanism by which providers can require guests to undergo a verification process as part of the reservation requirements (Airbnb, 2021a). We define the perceived effectiveness of guest verification as the extent to which providers believe that effective and rigorous verification procedures are implemented by the platform to guarantee qualified and eligible guests. This verification practice protects providers' interests by preventing potential threats and losses (Lu et al., 2021), contributing to pragmatic legitimacy. This practice also meets social and legal expectations to ensure safety in the sharing economy (Park & Tussyadiah, 2020) and thus tends to improve socio-political legitimacy. Therefore, we propose the following hypothesis:

H3. Perceived effectiveness of guest verification is positively related to pragmatic legitimacy **(H3a)** and socio-political legitimacy **(H3b).**

Two-way review system. A two-way review system is a type of referral or rating system that allows members of the community to provide or collect information about other users (Jøsang, Ismail, & Boyd, 2007; Liang et al., 2020). On Airbnb, for example, both providers and guests can write reviews and rate each other after completing the checkout process (Airbnb, 2021b). The review system offers providers relevant information to understand the background of their guests, so they can reject bookings made by unqualified guests to avoid physical privacy risks such as property damage or harassment (Liang et al., 2020). Given that this system can protect providers' interests, it contributes to pragmatic legitimacy. In addition, this system meets the social and legal expectations for more transparency and trust in the sharing economy (Köbis, Soraperra, & Shalvi, 2021), and thus enhances socio-political legitimacy. Therefore, we hypothesize as follows:

H4. Perceived effectiveness of the two-way review system is positively related to pragmatic legitimacy **(H4a)** and socio-political legitimacy **(H4b).**

Compensation. Compensation is a common practice in service recovery. After a service failure or incident, customers expect to receive compensation for their loss through a recovery effort (Johnston & Michel, 2008). In our research context, compensation refers to Airbnb policies, such as Host Guarantee and Host Protection Insurance, through which hosts are covered up to $1 million for unexpected accidents related to physical privacy risks and harms, such as property and belongings being damaged, and people being hurt or injured (Airbnb, 2021c, 2021d). This compensation practice ensures that providers' interests are protected and thus enhances their positive judgement of pragmatic legitimacy. In addition, compensation is consistent with social expectations and norms because it ensures fairness, rightness, or deservingness in business interactions (Kwon & Jang, 2012). Thus, compensation can facilitate positive judgement of socio-political legitimacy. We therefore propose the following hypothesis:

H5. Perceived effectiveness of compensation is positively related to pragmatic legitimacy **(H5a)** and socio-political legitimacy **(H5b).**

3.2. Legitimacy judgement of privacy management and B2B relationships

We propose that pragmatic legitimacy and socio-political legitimacy have distinct effects on affective commitment and calculative commitment. Pragmatic legitimacy indicates that the platform's actions can serve the interests of key stakeholder audiences, that is, providers (Chen et al., 2022; Suchman, 1995), so it is expected to strengthen providers' calculative commitment, which is built upon rational and economic calculations. In addition, securing the interests of providers demonstrates the platform's benevolence and goodwill (Chen et al., 2021; Guo et al., 2017), which develop providers' positive emotions and feelings toward it and further strengthen their affective commitment. We thus hypothesize as follows:

H6. Providers' pragmatic legitimacy of a platform's privacy management is positively related to their calculative commitment (**H6a**) and affective commitment (**H6b**).

A platform's socio-political legitimacy reflects its internal and stable characteristics, such as being responsible and benevolent (Castelló & Lozano, 2011; Zhang et al., 2020), that generate positive feelings among providers and allow them to form an emotional bond with the platform. Therefore, socio-political legitimacy contributes to affective commitment. However, socio-political legitimacy does not convey any explicit and salient information about the utilitarian benefits or financial implications of privacy management. Therefore, it is less likely to strengthen provides' calculative commitment. Overall, we propose the following hypothesis:

H7. Providers' socio-political legitimacy is positively related to their affective commitment.

4. Method

4.1. Research design, data collection, and sample

We employed a survey to test our research model and hypotheses. Given that Airbnb is currently the most widely used platform in the home-sharing economy (Statista, 2021), it was chosen as our research context. Our survey includes measures of all constructs in the model and records respondents' characteristics such as demographics and hosting experiences. Before launching the survey, we pre-tested it with both academics and Airbnb hosts ($n = 10$) to improve its understandability, content validity, and face validity. Some minor modifications such as wording were made during this process.

We recruited respondents from Prolific, an online panel platform used by social and behavioural researchers to source respondent samples (Palan & Schitter, 2018; Peer, Brandimarte, Samat, & Acquisti, 2017). We applied the following eligibility criteria to select respondents: (1)

having experience hosting on Airbnb, and (2) English speakers from Western countries (Europe and the Anglosphere). As Airbnb informs users of some basic privacy practices when they register as providers, we expect those who have hosted on Airbnb to have some basic ideas about these Airbnb practices. We focused on Western countries because personal privacy is highly valued in Western culture (Chen, Waseem, et al., 2021).

In total, we received 398 completed responses with minimal missing values (<5%) for all questions in the survey. Data cleaning included checking for IP address duplication ($n = 9$), failure of attention check ($n = 7$), and excessive LongString values ($n = 2$); it reduced the sample size to 380 (mean age = 28.72 years, 62.9% male, 72.1% had completed higher education). To assess the non-response bias, we compared the variables related to hosts' characteristics (e.g., gender, age, education, residency, and hosting experience on Airbnb) between early respondents ($n = 203$) and late respondents ($n = 177$) (Armstrong & Overton, 1977; Lambert & Harrington, 1990). The respondent waves were classified based on the median of the dates when their responses were recorded. No significant differences were found between the two groups (see Appendix A1), which indicates the absence of response bias. Overall, the sample characteristics suggest that the respondents have experiences in the home-sharing business, showing the suitability of the sample for this study. For more details on sample characteristics, please see Table 2.

Table 2
Respondent profile.

Demographic characteristics		n	%
Gender	Male	239	62.89%
	Female	137	36.05%
	Other	4	1.05%
Age	Mean = 28.72, SD = 8.71, Range = 18–71		
	25 and under	167	43.95%
	26–35	141	37.11%
	36–45	54	14.21%
	46 and above	18	4.74%
Education	High school or lower	86	22.63%
	Vocational school	20	5.26%
	Four-year college	159	41.84%
	Graduate school	115	30.26%
Residence	North America (US and Canada)	106	27.89%
	Europe and the UK	257	67.63%
	Oceania (Australia and New Zealand)	17	4.47%
Hosting experience			
Platform use	Airbnb only	357	93.95%
	Airbnb and others (e.g., booking.com)	22	5.79%
Frequency of living in the same property with guests	Mean = 2.84, SD = 1.84, Range = 1 (never) to 7 (always)		
	Less frequent (1–3)	256	67.37%
	More frequent (4–7)	124	32.63%
Duration of hosting : d *(months)*	Mean = 17.35, SD = 13.88, Range = 0–108		
	$d \leq 6$	97	25.53%
	$6 < d \leq 12$	82	21.58%
	$12 < d \leq 18$	61	16.05%
	$18 < d \leq 24$	69	18.16%
	$24 < d \leq 30$	18	4.74%
	$30 < d \leq 36$	27	7.11%
	$d > 36$	25	6.58%
Frequency of hosting : f *(times)*	Mean = 22.14, SD = 42.42, Range = 1–500		
	$f \leq 5$	142	37.37%
	$5 < f \leq 10$	73	19.21%
	$10 < f \leq 15$	40	10.53%
	$15 < f \leq 20$	29	7.63%
	$20 < f \leq 25$	16	4.21%
	$25 < f \leq 30$	16	4.21%
	$f > 30$	60	15.79%
Total		380	100.00%

4.2. *Measures*

All constructs in our research model were measured by adapting established multi-item scales from the literature. Respondents were asked to rate the scale items on a seven-point Likert scale, ranging from 1 = "strongly disagree" to 7 = "strongly agree".

Regarding digital privacy practices, we measured *perceived effectiveness of privacy assurance* and *perceived effectiveness of privacy control* by adopting three items from Lutz et al. (2018) and four items from Martin et al. (2017), respectively. To measure *perceived effectiveness of guest verification*, three items that capture respondents' perceptions of Airbnb's screening mechanisms were adopted from Lu et al. (2021). We adapted four items from Choi, Wu, Yu, and Land (2018) and Chen, Biamukda, and Tran (2020) to measure *perceived effectiveness of the two-way review system. Perceived effectiveness of compensation* was measured with three items from Shuqair, Pinto, and Mattila (2019).

After respondents became aware of digital and physical privacy practices, we measured their legitimacy judgement of the overall privacy management. Six items measuring *pragmatic legitimacy* and *sociopolitical legitimacy* of Airbnb's privacy management were adapted from Zhang et al. (2020). Finally, providers' *calculative commitment* and *affective commitment* to Airbnb were measured by using the scales of Gilliland and Bello (2002) and Lee, Sirgy, Brown, and Bird (2004), respectively. All of our measurement items are presented in Table 3.

We also employed control variables (e.g., hosting experience) that might have confounding effects on hosts' evaluation and behaviour toward Airbnb. Hosting experience was measured by hosting duration ("How long have you been a host on Airbnb?") and hosting frequency ("How many times have you been a host on Airbnb?"). Because data on hosting duration and frequency were highly abnormal (i.e., having high skewness and very high kurtosis), they were recoded into seven categories with equal intervals (6-month and 5-time intervals, respectively). As a result, the transformed variables of hosting duration and frequency were similar to a 7-point Likert scale and had lower skewness and kurtosis (absolute values <1).

5. Analysis and results

We employed a two-stage procedure in our data analysis (Hair Jr, Howard, & Nitzl, 2020; Hair, Risher, Sarstedt, & Ringle, 2019)—a confirmatory composite analysis to test the measurement model followed by structural equation modelling (SEM) to test the structural model. Testing of the models was based on the Partial Least Square (PLS) SEM technique using SmartPLS 3.0. This technique is widely accepted because of its flexibility in terms of sample and data requirements and model specifications (Hair et al., 2019). PLS-SEM is also suitable for theory development (Reinartz, Haenlein, & Henseler, 2009) and to evaluate models with complex relationships (Chin, 1998). Parameters were estimated by the bootstraping method with 5000 bootstrap samples. The observed variables did not deviate much from normality (|skewness| < 1 and |kurtosis| < 1), implying high-quality inputs for the SEM analysis.

5.1. *Measurement model*

We conducted a confirmatory composite analysis to assess the constructs' reliability and validity (Hair Jr et al., 2020). All latent variables were specified as reflective constructs. As can be seen in Tables 3 and 4, Cronbach's α, ρ, and construct reliability values are higher than 0.7, so the construct measures have adequate internal consistency and reliability. Convergent validity of the constructs is established because the standardized loadings of the items are >0.7 and statistically significant ($p < 0.001$), and the average variance extracted (AVE) values are >0.5. Using the Fornell–Larcker criterion (Fornell & Larcker, 1981), the square roots of AVE estimates for any two factors are also greater than the correlation between them, which provides evidence of discriminant

Table 3
Scale items and constructs' reliability and convergent validity.

Constructs and items		Loading	Maximum cross-loading
Perceived effectiveness of privacy assurance (α = 0.811; ρ = 0.819; CR = 0.887; AVE = 0.724)			
PASR1	Airbnb's privacy policy (i.e., privacy terms and conditions) is easy to find.	0.827***	0.417
PASR2	Airbnb's privacy policy is easy to understand.	0.884***	0.507
PASR3	Airbnb explains why it needs specific personal data (e.g., location, contact details, photos).	0.842***	0.547
Perceived effectiveness of privacy control (α = 0.868; ρ = 0.877; CR = 0.911; AVE = 0.720)			
PCON1	When I use Airbnb, I have control over what happens to my personal information on Airbnb.	0.735***	0.436
PCON2	It is up to me how much Airbnb uses my personal information.	0.880***	0.424
PCON3	I have a say in how my personal information is used by Airbnb.	0.898***	0.529
PCON4	I have a say in whether Airbnb shares my personal information with others.	0.872***	0.491
Perceived effectiveness of guest verification (α = 0.788; ρ = 0.820; CR = 0.875; AVE = 0.702)			
EOGV1	Airbnb's screening mechanisms provide excellent guests.	0.886***	0.456
EOGV2	Airbnb's guest screening mechanisms are rigorous.	0.741***	0.353
EOGV3	Airbnb's guest screening mechanisms are effective.	0.878***	0.469
Perceived effectiveness of the review system (α = 0.879; ρ = 0.892; CR = 0.917; AVE = 0.734)			
ETRS1	On the Airbnb platform, previous reviews of a guest are helpful for me to familiarize myself with him/her.	0.862***	0.487
ETRS2	Previous reviews of a guest are helpful for my overall evaluation of him/her.	0.882***	0.376
ETRS3	Previous reviews of a guest are helpful for my judgement of him/her.	0.878***	0.419
ETRS4	Previous reviews of a guest tell a lot about him/her.	0.803***	0.382
Perceived effectiveness of compensation (α = 0.918; ρ = 0.918; CR = 0.948; AVE = 0.859)			
COMP1	Airbnb has good compensation policy for any losses incurred to me.	0.917***	0.478
COMP2	Airbnb provides good compensation policy to cover my losses.	0.942***	0.480
COMP3	Airbnb has good compensation policy for the losses I encountered.	0.940***	0.483
Pragmatic legitimacy (α = 0.889; ρ = 0.890; CR = 0.931; AVE = 0.819)			
PRLG1	Airbnb's privacy management is beneficial to me.	0.873***	0.625
PRLG2	Airbnb's privacy management meets my needs.	0.922***	0.640
PRLG3	Airbnb's privacy management is good for me.	0.919***	0.689
Socio-political legitimacy (α = 0.903; ρ = 0.904; CR = 0.939; AVE = 0.837)			
SPLG1	Airbnb's privacy management conforms to values held by our society.	0.911***	0.678
SPLG2	Airbnb's privacy management meets norms and standards expected in our society.	0.918***	0.659
SPLG3	Airbnb's privacy management conforms to regulatory standards in our society.	0.916***	0.638
Calculative commitment (α = 0.832; ρ = 0.852; CR = 0.898; AVE = 0.746)			
CACT1	I continue to work with Airbnb as changing to another home-sharing platform would be too disruptive for my business.	0.870***	0.288
CACT2	I wouldn't shift my business away from Airbnb as my losses could be significant.	0.863***	0.208
CACT3	I need to keep working with Airbnb since leaving would create a hardship for my business.	0.857***	0.177
Affective commitment (α = 0.889; ρ = 0.891; CR = 0.931; AVE = 0.819)			
AFCT1	I will continue as an Airbnb host as I genuinely enjoy my relationship with them.	0.898***	0.573
AFCT2	I will continue my relationship with Airbnb, as I personally like them.	0.927***	0.617
AFCT3	I will continue my relationship with Airbnb as we are on friendly terms.	0.890***	0.575

Notes: *** p < 0.001; CR = Composite reliability; AVE = Average variance extracted.

validity. Moreover, discriminant validity of the constructs is confirmed by the fact that the cross–loadings exceed the loadings and by the Heterotrait–Monotrait ratio of correlations (HTMT) (Henseler, Ringle, & Sarstedt, 2015), which is consistently below the threshold value of 0.85.

In addition, as our data were cross-sectional and collected from single informants at one point in time, we followed recommendations from the literature to evaluate common method bias (CMB) (Malhotra, Schaller, & Patil, 2017; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Steenkamp & Maydeu-Olivares, 2021). Harman's single-factor test (Podsakoff & Organ, 1986) using the principal component analysis in SPSS shows that the most variance explained by one factor is 36.4% (below the threshold of 50%). The variance inflation factor (VIF) values from the full collinearity test (Kock & Lynn, 2012) are <3.3 (maximum VIF = 2.817), indicating no pathological collinearity (Kock, 2015). Apart from the correlation between pragmatic and socio-political legitimacy (r = 0.72), there are no high correlations between other constructs; all correlations are below 0.6, much smaller than the threshold of 0.9 (Pavlou, Liang, & Xue, 2007).

As suggested by Liang, Saraf, Hu, and Xue (2007), we also used the common method factor approach to compare how the items load on its theoretical constructs and on a latent method construct. Consequently, the variance of each item is mostly explained by its theoretical construct (average variance = 77.3%), but not by the common method factor (average variance = 0.4%). Additionally, all 29 item loadings on the corresponding theoretical constructs are statistically significant ($p <$ 0.001), yet several (23) loadings on the method factor are insignificant ($p >$ 0.05; see Appendix A2). Taken together, these results indicate that CMB is not a serious concern in this study.

Apart from the post-hoc analyses to check CMB, we employed ex-ante remedies to minimize it. In particular, we conducted pre-testings to minimize ambiguity of the survey and address social desirability bias in wordings, and we emphasized anonymity, confidentiality, and voluntariness of the respondents' participation. We also included attention checks and considered the order of the questions to avoid item-priming effects (Podsakoff et al., 2003).

5.2. Structural model

PLS-SEM with bootstraping was used to test the direct and mediating effects in the model. The model fit indices were shown to be relatively good in this study (e.g., standardized root mean square residual [SRMR] = 0.068 < 0.08; normed fit index [NFI] = 0.832 > 0.8) (Henseler, Hubona, & Ray, 2016). The structural model was evaluated based on

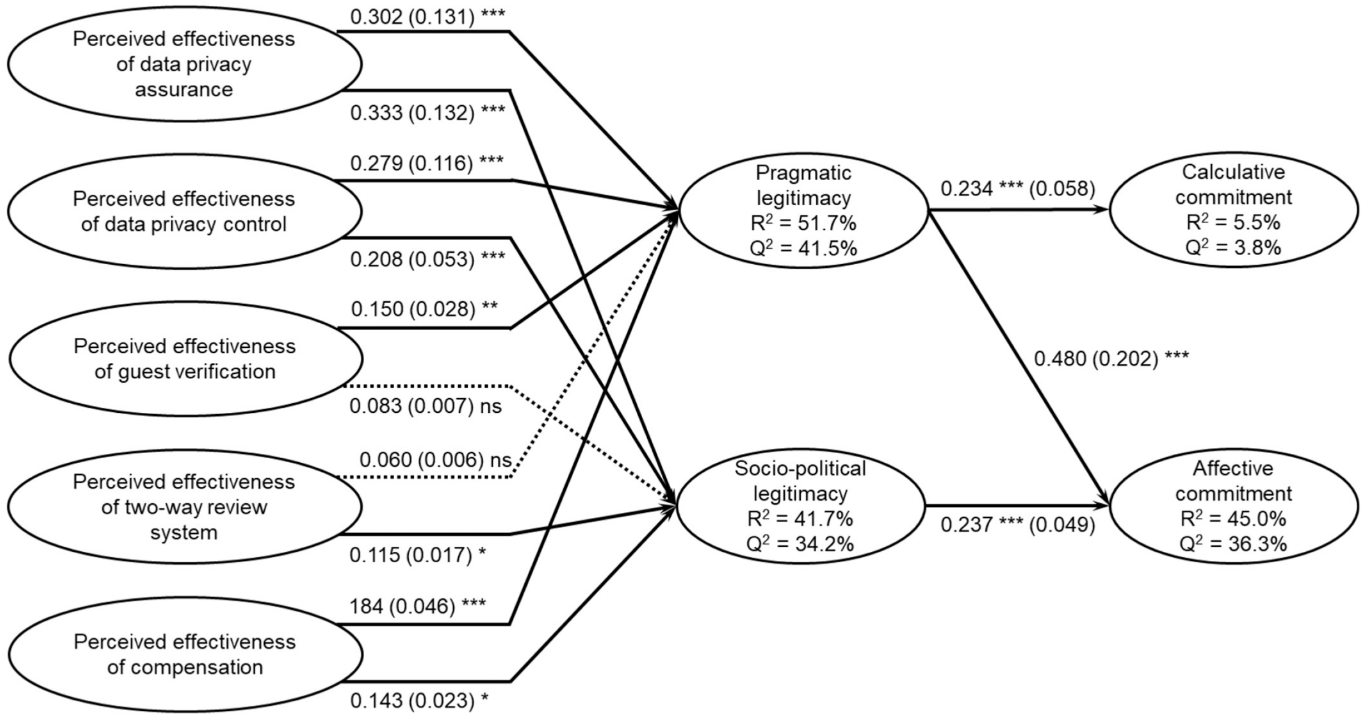
Table 4
Constructs' discriminant validity.

	1	2	3	4	5	6	7	8	9
1. PRVASR	**0.851**	0.545	0.369	0.275	0.428	0.677	0.641	0.240	0.534
2. PRVCON	0.460	**0.849**	0.354	0.187	0.411	0.632	0.529	0.235	0.441
3. GUEVER	0.447	0.421	**0.838**	0.574	0.568	0.564	0.470	0.287	0.547
4. REVSYS	0.325	0.212	0.491	**0.857**	0.328	0.362	0.363	0.212	0.365
5. COMPEN	0.494	0.458	0.485	0.298	**0.927**	0.574	0.489	0.211	0.484
6. PRALEG	0.581	0.558	0.479	0.324	0.518	**0.905**	0.803	0.267	0.731
7. SPOLEG	0.552	0.471	0.406	0.329	0.446	0.720	**0.915**	0.236	0.649
8. CALCMT	0.196	0.203	0.232	0.187	0.188	0.234	0.207	**0.863**	0.277
9. AFFCMT	0.460	0.386	0.468	0.325	0.438	0.650	0.582	0.247	**0.905**

Notes: Bold values on the diagonal represent square root of AVEs. Values below the diagonal are correlations. Values above the diagonal are HTMT ratios.
PRVASR = Perceived effectiveness of privacy assurance.
PRVCON = Perceived effectiveness of privacy control.
GUEVER = Perceived effectiveness of guest verification.
REVSYS = Perceived effectiveness of the review system.
COMPEN = Perceived effectiveness of compensation.
PRALEG = Pragmatic legitimacy.
SPOLEG = Socio-political legitimacy.
CALCMT = Calculative commitment.
AFFCMT = Affective commitment.

predictive accuracy/explanatory power (R^2), predictive relevance (Q^2), and violation of the non-multicollinearity assumption (VIF) (Hair et al., 2019). As can be seen in Fig. 2 and Appendix A3, VIF values of the exogenous variables in the model are below the threshold of 3, suggesting that the model is not subject to collinearity problems. All endogenous variables, except for *calculative commitment*, have moderate predictive accuracy (R^2 of *pragmatic legitimacy* = 51.7%, R^2 of *socio-political legitimacy* = 41.7%, R^2 of *affective commitment* = 45.0%, and R^2 of *calculative commitment* = 5.5%) and medium predictive relevance (Q^2 of *pragmatic legitimacy* = 41.5%, Q^2 of *socio-political legitimacy* = 34.2%, Q^2 of *affective commitment* = 36.3%, and Q^2 of *calculative commitment* = 3.8%). To further examine the holdout-based sample prediction of the model, the PLSpredict procedure on the item level (Shmueli et al., 2019) was used. Table 5 shows that the Q^2_{predict} values of all items are >0. All root mean square error (RMSE) values of the 12 items in the PLS-SEM are lower than those in the linear regression model (LM), indicating that the model has high predictive power.

The hypotheses were tested based on the estimated path coefficients (β), their significance (p), and their effect size (f^2). The results show that digital privacy practices had stronger effects on both forms of legitimacy than physical privacy practices. Of the examined privacy practices, the coefficients and effect sizes of the paths from *privacy assurance* to *pragmatic legitimacy* (β = 0.302, p < 0.001, f^2 = 0.131) and *socio-political legitimacy* (β = 0.333, p < 0.001, f^2 = 0.132) are the highest, followed by



Notes: *** p < 0.001; ** p < 0.01; * p < 0.5; † p < 0.1; ns p ≥ 0.1. Effect size (f^2) values are in brackets.

Fig. 2. Results of structural model testing.

Table 5
PLS predict assessment.

Item	PLS		LM		RMSE PLS – RMSE LM
	RMSE	Q^2_{predict}	RMSE	Q^2_{predict}	
PLG3	0.879	0.422	0.897	0.398	−0.018
PLG1	0.918	0.383	0.933	0.363	−0.015
PLG2	0.899	0.414	0.919	0.388	−0.020
SPLG1	0.927	0.352	0.950	0.319	−0.023
SPLG3	0.907	0.319	0.931	0.284	−0.024
SPLG2	0.920	0.312	0.946	0.273	−0.026
CCT1	1.376	0.047	1.389	0.028	−0.013
CCT2	1.375	0.049	1.393	0.023	−0.018
CCT3	1.465	0.034	1.501	−0.014	−0.036
ACT3	1.099	0.245	1.123	0.212	−0.024
ACT2	1.129	0.278	1.155	0.244	−0.026
ACT1	1.073	0.264	1.081	0.252	−0.008

Notes: PLG = Pragmatic legitimacy, SPLG = Socio-political legitimacy, CCT = Calculative commitment, ACT = Affective commitment.

the paths from *privacy control* (to *pragmatic legitimacy*: $\beta = 0.279$, $p < 0.001$, $f^2 = 0.116$, and to *socio-political legitimacy*: $\beta = 0.208$, $p < 0.001$, $f^2 = 0.053$). These results offer strong support for **H1a, H1b, H2a**, and **H2b**.

Results relating to physical privacy practices show that perceived effectiveness of Airbnb's *guest verification* has a positive and significant effect on the judgement of *pragmatic legitimacy* ($\beta = 0.150$, $p = 0.003$, $f^2 = 0.028$), but its effect on judgement of *socio-political legitimacy* is insignificant ($\beta = 0.083$, $p = 0.127$, $f^2 = 0.007$). Thus, **H3a** rather than **H3b** is supported. Respondents' perception of the *review system* exerts a significant impact on *socio-political legitimacy* ($\beta = 0.115$, $p = 0.022$, $f^2 = 0.017$), but not on *pragmatic legitimacy* ($\beta = 0.060$, $p = 0.172$, $f^2 = 0.006$). Therefore, **H4b** rather than **H4a** is supported. The relationships between *compensation* and both *pragmatic* and *socio-political legitimacy* are positive and significant ($\beta = 0.184$, $p < 0.001$, $f^2 = 0.046$; and $\beta = 0.143$, $p = 0.012$, $f^2 = 0.023$, respectively). Hence, the results support both **H5a** and **H5b**.

The results show that *pragmatic legitimacy* is positively and significantly related to *calculative commitment* ($\beta = 0.234$, $p < 0.001$, $f^2 = 0.058$) and *affective commitment* ($\beta = 0.480$, $p < 0.001$, $f^2 = 0.202$), supporting **H6a** and **H6b**. The relationship between *socio-political legitimacy* and *affective commitment* is also positive and significant ($\beta = 0.237$, $p < 0.001$, $f^2 = 0.049$), thus providing support for **H7**.

We also examined the mediating effects of pragmatic and socio-political legitimacy on the relationship between Airbnb's privacy practices and providers' commitment. A series of specific indirect effect tests (see Table 6) showed that *review system* does not indirectly influence either form of commitment, through neither *pragmatic* nor *socio-political legitimacy* ($p > 0.05$). In contrast, other privacy practices positively influence calculative and affective commitment through both forms of legitimacy (coefficients >0, $p < 0.05$). The only exception is that *guest verification* does not significantly influence *affective commitment* through *socio-political legitimacy*.

For the robustness check, we tested another PLS-SEM model by adding control variables (i.e., sex, age, hosting duration, and hosting frequency of Airbnb hosts) which potentially influence Airbnb hosts' legitimacy judgement and commitment. The results show that the magnitude and significance of the relationships in the original model remain unchanged. The maximum change in the path coefficients is 0.013 (for the path GUEVER → PRALEG). This result indicates the stability and robustness of the findings (see Appendix A4 for more details).

Table 6
Testing specific indirect effects.

Specific indirect effect	β	SD	t	p	LCI95% BC	UCI95% BC
PRVASR → PRALEG → CALCMT	0.071	0.019	3.723	0.000	0.038	0.111
PRVCON → PRALEG → CALCMT	0.065	0.018	3.529	0.000	0.034	0.105
GUEVER → PRALEG → CALCMT	0.035	0.015	2.413	0.016	0.011	0.067
REVSYS → PRALEG → CALCMT	0.014	0.011	1.234	0.217	−0.006	0.039
COMPEN → PRALEG → CALCMT	0.043	0.017	2.557	0.011	0.017	0.083
PRVASR → PRALEG → AFFCMT	0.145	0.031	4.684	0.000	0.092	0.214
PRVASR → SPOLEG → AFFCMT	0.079	0.025	3.204	0.001	0.035	0.132
PRVCON→ PRALEG → AFFCMT	0.134	0.026	5.073	0.000	0.087	0.193
PRVCON → SPOLEG → AFFCMT	0.049	0.019	2.555	0.011	0.018	0.095
GUEVER → PRALEG → AFFCMT	0.072	0.027	2.663	0.008	0.024	0.132
GUEVER → SPOLEG → AFFCMT	0.020	0.015	1.315	0.188	−0.004	0.054
REVSYS → PRALEG → AFFCMT	0.029	0.022	1.339	0.181	−0.013	0.072
REVSYS → SPOLEG → AFFCMT	0.027	0.015	1.831	0.067	0.003	0.061
COMPEN → PRALEG → AFFCMT	0.088	0.029	3.036	0.002	0.038	0.152
COMPEN → SPOLEG → AFFCMT	0.034	0.016	2.098	0.036	0.009	0.074

Notes: SD = Standard deviation, LCI95%BC = Lower limit of bias-corrected 95% confidence interval, UCI95%BC = Upper limit of bias-corrected 95% confidence interval.
PRVASR = Perceived effectiveness of privacy assurance.
PRVCON = Perceived effectiveness of privacy control.
GUEVER = Perceived effectiveness of guest verification.
REVSYS = Perceived effectiveness of the review system.
COMPEN = Perceived effectiveness of compensation.
PRALEG = Pragmatic legitimacy.
SPOLEG = Socio-political legitimacy.
CALCMT = Calculative commitment.
AFFCMT = Affective commitment.

6. Discussion

6.1. Discussion of results

This research investigates how home-sharing providers decide their level of commitment to a platform based on their perceptions of its privacy practices and legitimacy judgement of its overall privacy management. The results of our model are consistent with the literature on legitimacy as judgement based on institutional theory, which demonstrates that stakeholders need to undergo three key interrelated psychological stages: perception, legitimacy judgement, and decision (Bitektine, 2011; Chen et al., 2022; Tost, 2011). The results of our model show that the identified physical and digital privacy practices explain 51.7% and 41.7% of the variance in pragmatic legitimacy and socio-political legitimacy of the platform's privacy management, respectively. Specifically, digital privacy practices engender stronger effects on both forms of legitimacy than physical privacy practices. Of all the examined privacy practices, the results offer strong support for the effects of *privacy assurance*, followed by *privacy control*. These results are consistent with the privacy literature that demonstrates the positive role of firm practices on the digital (e.g., Martin et al., 2017) and physical environment (e.g., Ranzini et al., 2020).

Among physical privacy practices, compensation is shown to be the strongest predictor of both pragmatic and socio-political legitimacy of the platforms' privacy management. Aligned with previous studies (e.g., Johnston & Michel, 2008), this result shows that compensation protects providers' self-interest and is highly accepted and expected by them. Although the two-way review system had a significant effect on *socio-political legitimacy*, its effect on *pragmatic legitimacy* is not supported. Similar to prior research (e.g., Dolnicar, 2017), our result suggests that such a review system is socially accepted by providers as it facilitates transparency in service interactions and mitigates potential physical risks. The result also highlights that Airbnb's two-way review system has shortcomings in protecting providers' interests to gain pragmatic legitimacy. Finally, guest verification has a significant impact on *pragmatic legitimacy* but not on *socio-political legitimacy*. Unlike provider verification (Lu et al., 2021), guest verification has not yet reached social consensus as something necessary and appropriate in a platform's privacy management.

Aligned with recent institutional research (e.g., Zhang et al., 2020), we evaluate specific forms of legitimacy judgement and demonstrate their distinctive effects. The results show that providers' legitimacy judgements, including both pragmatic and socio-political legitimacy, explain a significant proportion of variance of their affective commitment to the platform. This highlights that if the platform's privacy management meets utilitarian expectations, legal requirements, and social standards, it will create positive emotions and feelings among providers and gain their affective commitment. Although the pragmatic legitimacy of privacy management has a significant relationship with calculative commitment, the explained variance of calculative commitment is relatively small. This suggests that privacy management contributes to the economic component in the B2B relationship, but it is not a dominant factor.

6.2. Theoretical contributions

Our research explored both physical and digital privacy practices for the first time and examined their effects on B2B relationships from an institutional perspective. Our research makes the following theoretical contributions. First, it adds to the literature on B2B marketing by showing the effects of privacy practices on B2B relationships. Although privacy practices have been widely studied in B2C research (Lwin et al., 2007; Martin et al., 2017), their effects on B2B relationships remain unclear (Wang et al., 2020). Our paper suggests that platforms' privacy practices can strengthen business customers' (providers') commitment from an institutional perspective.

Second, our findings offer novel implications for understanding providers' psychological process of legitimacy judgement, contributing to B2B marketing research by incorporating the micro-level psychological aspects of institutions (Bitektine, 2011; Bitektine & Haack, 2015; Suddaby et al., 2017; Tost, 2011). The literature on legitimacy judgement is rooted in the perspective of stakeholders outside of B2B research, such as employees (Bitektine, 2011). Recent research suggests that legitimacy judgement varies across different groups of stakeholder audiences because they hold different interests (Helms, Patterson, & Hudson, 2019; Slimane, Chaney, Humphreys, & Leca, 2019). Our research contributes to this literature by conceptualizing and illuminating the process of legitimacy judgement of providers (business customers) as stakeholder audiences. It demonstrates that providers are key stakeholder audiences of the institutions of privacy management and thus are propelled to evaluate such institutions. The findings expand the institutional analysis of key stakeholder audiences from intra-organizational networks (e.g., employees and managers) (Bitektine, 2011) to B2B networks. To our knowledge, this is among the first empirical studies to provide an integrative framework illustrating business customers' (providers') psychological process of legitimacy judgement. In addition, our research is one of the first to examine specific forms of legitimacy judgement in the psychological process and demonstrate their distinctive effects.

Third, our research contributes to the privacy literature by examining both physical and digital privacy practices in a platform's privacy management. Previous marketing studies on data privacy have focused on digital privacy (Janakiraman et al., 2018; Lwin et al., 2007; Martin et al., 2017) and examined various digital privacy practices (Kim et al., 2019; Martin et al., 2017). Recent research suggests that home-sharing providers are concerned about both digital and physical privacy (Ranzini et al., 2020). However, it is still unclear what privacy practices can effectively address physical privacy. Our study, as one of the first to investigate the effects of both physical and digital privacy practices, suggests that given the unique business interactions in the home-sharing economy, both physical and digital privacy practices must be incorporated in platform management.

6.3. Practical implications

This research has significant practical implications. It highlights the key role of legitimacy of privacy management at the platform level in strengthening providers' commitment. With this understanding, platforms can design better strategies to communicate their aligned interests with providers in the sharing economy and develop long-term collaborative relationships (Constantiou, Marton, & Tuunainen, 2017). The findings of this research also provide specific recommendations for both platforms and policymakers to address privacy risks and thus enhance the legitimacy of the sharing economy.

Sharing economy platforms should undertake effective physical privacy practices to improve providers' commitment. First, platforms like Airbnb need to develop verification policies that adhere to the existing norms and laws to avoid problematic guests. The laws and rules regarding home-sharing services are different across regions. Therefore, platforms' policies must adapt to the rule of law enforced by local governments (Nieuwland & Van Melik, 2020). Second, to ensure that the two-way review system is perceived effectively, platforms need to develop review policies that help providers screen problematic guests and safeguard their self-interest (e.g., better reputation, increased earnings, improved visibility of their property listing, and positive guest referrals). In addition, platforms should be transparent about their compensation practice and policy. They should do so by allowing independent auditors to publish detailed reports on the platform's compensation practices. This helps mitigate providers' perceived uncertainty and reduce their anxiety.

To enhance providers' commitment, sharing economy platforms also need to undertake practices to address digital privacy risks. They need to formulate privacy assurance policies that are comprehensible. Many platforms' privacy assurance policies are lengthy and vague, making it difficult for providers to comprehend them. For example, Airbnb's privacy assurance policy uses language like "adequate performance" and "legitimate interest". Although this way of communicating privacy assurance provides flexibility for Airbnb to defend its data practices in a lawsuit, it creates uncertainty about what is being done with providers' data (Litman-Navarro, 2021). Finally, platforms should give providers access to and control over their own data. For example, Airbnb collects personal data including geolocation, property listings, booking history, sign-in history, and device information. In their account settings, users can control what kind of information they would like to share with Airbnb and decide how Airbnb uses their cookies.

6.4. Limitations and future research directions

The present research has limitations that offer opportunities for future study. First, this research used a survey to collect cross-sectional data and measured providers' psychological constructs without tracking the changes in B2B relationships over time. Future research could conduct longitudinal studies by using financial and market-based metrics from archival data or apply field experiments to trace the changes in privacy perceptions and B2B relationships. Second, this research examined the institutions of privacy management at the platform level. Future research could extend our conceptual model to the macro level and evaluate the roles of platform-independent institutional factors such as government regulations and rules (Lu et al., 2021). Third, contextual factors such as organizational and national culture play an important role in customer responses in the sharing economy (Gupta, Esmaeilzadeh, Uz, & Tennant, 2019). Future research can include these contextual factors to test the effects of privacy management in sharing economy platforms.

7. Conclusion

Overall, this research demonstrates that physical and digital privacy practices can improve providers' legitimacy judgement of the platform's privacy management and subsequently increase their commitment to the platform. The findings contribute to understanding privacy management in the sharing economy from an institutional perspective. Future research can extend the current findings by conducting longitudinal research and considering macro factors and cultural impacts.

Funding

The authors gratefully acknowledge the Seed Corn Funding from University of Bradford and the Research Productivity Support Scheme from Macquarie University.

Ethical approval

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent

Informed consent was obtained from all individual participants included in the research.

Declarations of interest

None.

Appendix A. Appendix

A.1. Assessment of non-response bias

Characteristics		Early wave (n = 203)		Late wave (n = 177)		Total (n = 380)		Test of difference		
		n	%	n	%	n	%	χ^2	**df**	**p**
Gender	Male	130	64.0	109	61.6	239	62.9	1.14	2	0.57
	Female	70	34.5	67	37.9	137	36.1			
	Other	3	1.5	1	0.6	4	1.1			
Education	High school or below	51	25.1	35	19.8	86	22.6	5.80	3	0.12
	Vocational	9	4.4	11	6.2	20	5.3			
	Undergraduate	91	44.8	68	38.4	159	41.8			
	Postgraduate	52	25.6	63	35.6	115	30.3			
Residency	North America	50	24.6	56	31.6	106	27.9	2.88	2	0.24
	Europe and the UK	142	70.0	115	65.0	257	67.6			
	Oceania	11	5.4	6	3.4	17	4.5			
Platform use	Airbnb only	188	93.1	169	95.5	357	94.2	1.00	1	0.32
	Airbnb and others	14	6.9	8	4.5	22	5.8			
		Mean	**SD**	**Mean**	**SD**	**Mean**	**SD**	**t**	**df**	**p**
Age (in years)		28.4	8.3	29.0	9.1	28.7	8.7	−0.69	378	0.49
Hosting duration (in months)		18.3	13.9	16.3	13.8	17.3	13.9	1.39	377	0.17
Hosting frequency (times)		23.3	41.1	20.8	44.0	22.1	42.4	0.56	374	0.57
Frequency of living in the same property with guests (7–point Likert scale)		2.8	1.8	2.8	1.9	2.8	1.8	0.00	378	1.00

A.2. Assessment of common method bias by common method factor approach

Item	Loading on theoretical construct			Loading on method factor		
	R_1	p value	R_1^2	R_2	p value	R_2^2
PASR1	0.917	0.000	84.1%	−0.100	0.015	1.0%
PASR2	0.912	0.000	83.1%	−0.035	0.342	0.1%
PASR3	0.726	0.000	52.7%	0.135	0.009	1.8%
CODC1	0.669	0.000	44.7%	0.087	0.134	0.8%
CODC2	0.957	0.000	91.5%	−0.100	0.004	1.0%
CODC3	0.864	0.000	74.6%	0.046	0.159	0.2%
CODC4	0.886	0.000	78.5%	−0.021	0.553	0.0%
EOGV1	0.830	0.000	68.8%	0.064	0.064	0.4%
EOGV2	0.858	0.000	73.6%	−0.126	0.021	1.6%
EOGV3	0.837	0.000	70.0%	0.044	0.232	0.2%
ETRS1	0.787	0.000	61.9%	0.099	0.005	1.0%
ETRS2	0.922	0.000	85.1%	−0.059	0.068	0.3%
ETRS3	0.899	0.000	80.8%	−0.031	0.282	0.1%

(*continued on next page*)

(*continued*)

Item	Loading on theoretical construct			Loading on method factor		
	R_1	*p* value	R_1^2	R_2	p value	R_2^2
ETRS4	0.818	0.000	66.9%	−0.005	0.898	0.0%
COMP1	0.886	0.000	78.5%	0.039	0.215	0.2%
COMP2	0.961	0.000	92.3%	−0.023	0.289	0.1%
COMP3	0.933	0.000	87.0%	−0.015	0.568	0.0%
PLG1	0.867	0.000	75.1%	0.008	0.877	0.0%
PLG2	0.967	0.000	93.4%	−0.051	0.153	0.3%
PLG3	0.880	0.000	77.5%	0.044	0.379	0.2%
SPLG1	0.850	0.000	72.2%	0.073	0.048	0.5%
SPLG2	0.940	0.000	88.3%	−0.027	0.414	0.1%
SPLG3	0.956	0.000	91.4%	−0.046	0.179	0.2%
CCT1	0.813	0.000	66.1%	0.054	0.155	0.3%
CCT2	0.882	0.000	77.7%	0.005	0.874	0.0%
CCT3	0.899	0.000	80.9%	−0.056	0.056	0.3%
ACT1	0.876	0.000	76.7%	0.029	0.364	0.1%
ACT2	0.937	0.000	87.8%	−0.015	0.581	0.0%
ACT3	0.902	0.000	81.3%	−0.014	0.672	0.0%
Average	**0.877**		**77.3%**	**0.000**		**0.4%**

Notes: PASR = Perceived effectiveness of privacy assurance.
CODC = Perceived effectiveness of privacy control.
EOGV = Perceived effectiveness of guest verification.
ETRS = Perceived effectiveness of the review system.
COMP = Perceived effectiveness of compensation.
PLG = Pragmatic legitimacy.
SPLG = Socio-political legitimacy.
CCT = Calculative commitment.
ACT = Affective commitment.

A.3. Parameter estimates for the structural model

Hypothesis	Structural path			β	SD	t	p	LCI95% BC	UCI95% BC	f^2	VIF	R^2	Q^2
H1a	PRVASR	→	PRALEG	0.302	0.048	6.320	0.000	0.207	0.394	0.131	1.437	0.517	0.415
H2a	PRVCON	→	PRALEG	0.279	0.045	6.129	0.000	0.189	0.366	0.116	1.393		
H3a	GUEVER	→	PRALEG	0.150	0.050	2.975	0.003	0.050	0.248	0.028	1.649		
H4a	REVSYS	→	PRALEG	0.060	0.044	1.365	0.172	−0.031	0.142	0.006	1.341		
H5a	COMPEN	→	PRALEG	0.184	0.053	3.488	0.000	0.084	0.288	0.046	1.508		
H1b	PRVASR	→	SPOLEG	0.333	0.051	6.556	0.000	0.227	0.428	0.132	1.437	0.417	0.342
H2b	PRVCON	→	SPOLEG	0.208	0.055	3.794	0.000	0.100	0.316	0.053	1.393		
H3b	GUEVER	→	SPOLEG	0.083	0.055	1.528	0.127	−0.027	0.187	0.007	1.649		
H4b	REVSYS	→	SPOLEG	0.115	0.050	2.284	0.022	0.006	0.205	0.017	1.341		
H5b	COMPEN	→	SPOLEG	0.143	0.057	2.516	0.012	0.031	0.255	0.023	1.508		
H6a	PRALEG	→	CALCMT	0.234	0.053	4.441	0.000	0.130	0.334	0.058	1.000	0.055	0.038
H6b	PRALEG	→	AFFCMT	0.480	0.065	7.422	0.000	0.350	0.606	0.202	2.077	0.450	0.363
H7	SPOLEG	→	AFFCMT	0.237	0.064	3.716	0.000	0.101	0.356	0.049	2.077		

Notes: SD = Standard deviation, LCI95%BC = Lower limit of bias–corrected 95% confidence interval, UCI95%BC = Upper limit of bias-corrected 95% confidence interval.
PRVASR = Perceived effectiveness of privacy assurance.
PRVCON = Perceived effectiveness of privacy control.
GUEVER = Perceived effectiveness of guest verification.
REVSYS = Perceived effectiveness of the review system.
COMPEN = Perceived effectiveness of compensation.
PRALEG = Pragmatic legitimacy.
SPOLEG = Socio-political legitimacy.
CALCMT = Calculative commitment.
AFFCMT = Affective commitment.

A.4. Parameter estimates for the model with and without control variables

Structural path			Alternative model with control variables		Original model without control variables		Δβ
			β	p	β	p	
PRVASR	→	PRALEG	0.297	0.000	0.302	0.000	0.005
PRVCON	→	PRALEG	0.271	0.000	0.279	0.000	0.008
GUEVER	→	PRALEG	0.163	0.001	0.150	0.003	0.013
REVSYS	→	PRALEG	0.054	0.222	0.060	0.172	0.006
COMPEN	→	PRALEG	0.184	0.000	0.184	0.000	0.000
PRVASR	→	SPOLEG	0.328	0.000	0.333	0.000	0.005
PRVCON	→	SPOLEG	0.209	0.000	0.208	0.000	0.001
GUEVER	→	SPOLEG	0.082	0.150	0.083	0.127	0.001

(*continued on next page*)

(*continued*)

Structural path			Alternative model with control variables		Original model without control variables		Δβ
			β	p	β	p	
REVSYS	→	SPOLEG	0.120	0.017	0.115	0.022	0.005
COMPEN	→	SPOLEG	0.140	0.014	0.143	0.012	0.003
PRALEG	→	CALCMT	0.233	0.000	0.234	0.000	0.001
PRALEG	→	AFFCMT	0.491	0.000	0.480	0.000	0.011
SPOLEG	→	AFFCMT	0.234	0.000	0.237	0.000	0.003
Age	→	PRALEG	−0.057	0.106			
Age	→	SPOLEG	−0.023	0.542			
Age	→	CALCMT	0.073	0.147			
Age	→	AFFCMT	−0.003	0.935			
Sex	→	PRALEG	0.040	0.296			
Sex	→	SPOLEG	0.008	0.854			
Sex	→	CALCMT	0.045	0.400			
Sex	→	AFFCMT	−0.035	0.341			
Hosting duration	→	PRALEG	0.004	0.917			
Hosting duration	→	SPOLEG	0.057	0.232			
Hosting duration	→	CALCMT	−0.044	0.453			
Hosting duration	→	AFFCMT	0.081	0.032			
Hosting frequency	→	PRALEG	−0.011	0.788			
Hosting frequency	→	SPOLEG	−0.055	0.183			
Hosting frequency	→	CALCMT	0.023	0.708			
Hosting frequency	→	AFFCMT	0.082	0.059			

Notes: PRVASR = Perceived effectiveness of privacy assurance.
PRVCON = Perceived effectiveness of privacy control.
GUEVER = Perceived effectiveness of guest verification.
REVSYS = Perceived effectiveness of the review system.
COMPEN = Perceived effectiveness of compensation.
PRALEG = Pragmatic legitimacy.
SPOLEG = Socio-political legitimacy.
CALCMT = Calculative commitment.
AFFCMT = Affective commitment.

References

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2020). “This is capitalism. It is not illegal”: Users’ attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society, 37*(2), 115–127.

Airbnb. (2021a). Booking requirements for guests. Retrieved September 4, 2021 from https://www.airbnb.co.uk/help/article/272/can-i-require-guests-to-be-verified-before-booking.

Airbnb. (2021b). Reviews for stays. Retrieved September 4, 2021 from https://www.airbnb.co.uk/help/article/13/reviews-for-stays.

Airbnb. (2021c). What is host protection insurance?. Retrieved September 4, 2021 from https://www.airbnb.co.uk/help/article/937/what-is-host-protection-insurance.

Airbnb. (2021d). What is the airbnb host guarantee?. Retrieved September 4, 2021 from https://www.airbnb.co.uk/help/article/279/what-is-the-airbnb-host-guarantee.

Aldrich, H. E., & Fiol, C. M. (1994). Fools rush in? The institutional context of industry creation. *Academy of Management Review, 19*(4), 645–670.

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology, 91*(1), 221.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research, 14*(3), 396–402.

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services, 52*, Article 101947.

Belk, R. W. (1988). Possessions and the extended self. *Journal of Consumer Research, 15*(2), 139–168.

Bellamy, C., Raab, C., Warren, A., & Heeney, C. (2007). Institutional shaping of interagency working: Managing tensions between collaborative working and client confidentiality. *Journal of Public Administration Research and Theory, 17*(3), 405–434.

Bitektine, A. (2011). Toward a theory of social judgments of organizations: The case of legitimacy, reputation, and status. *Academy of Management Review, 36*(1), 151–179.

Bitektine, A., & Haack, P. (2015). The “macro” and the “micro” of legitimacy: Toward a multilevel theory of the legitimacy process. *Academy of Management Review, 40*(1), 49–75.

Bloomberg. (2021). Airbnb is spending millions of dollars to make nightmares go away. Retrieved September 4, 2021 from https://www.bloomberg.com/news/features/2021-06-15/airbnb-spends-millions-making-nightmares-at-live-anywhere-rentals-go-away.

Castelló, I., & Lozano, J. M. (2011). Searching for new forms of legitimacy through corporate responsibility rhetoric. *Journal of Business Ethics, 100*(1), 11–29.

Chatterjee, S., & Kar, A. K. (2018). Regulation and governance of the internet of things in India. *Digital Policy, Regulation and Governance, 20*(5), 399–412.

Chen, J. V., Biamukda, S., & Tran, S. T. T. (2020). Service providers’ intention to continue sharing: The moderating role of two-way review system. *Industrial Management & Data Systems, 120*(8), 1543–1564.

Chen, S., Gao, H., & Zhang, J. A. (2021). Consumers’ responses to corporate normalised misconduct during an industry-wide crisis: An investigation in the Chinese dairy industry. *Australasian Marketing Journal*. https://doi.org/10.1177/18393349211065193

Chen, S., Wright, M., Gao, H., Liu, H., & Mather, D. (2021). The effects of brand origin and country-of-manufacture on consumers’ institutional perceptions and purchase decision-making. *International Marketing Review, 38*(2), 343–366.

Chen, S., Zhang, J. A., Gao, H., Yang, Z., & Mather, D. (2022). Trust erosion during industry-wide crises: The central role of consumer legitimacy judgement. *Journal of Business Ethics, 175*, 95–116.

Chen, S. J., Waseem, D., Xia, Z. R., Tran, K. T., Li, Y., & Yao, J. (2021). To disclose or to falsify: The effects of cognitive trust and affective trust on customer cooperation in contact tracing. *International Journal of Hospitality Management, 94*, Article 102867.

Chin, A. G., Harris, M. A., & Brookshire, R. (2022). An empirical investigation of intent to adopt mobile payment systems using a trust-based extended valence framework. *Information Systems Frontiers, 24*(1), 329–347.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Choi, B., Wu, Y., Yu, J., & Land, L. P. W. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of the Association for Information Systems, 19*(3), 124–151.

Constantiou, I., Marton, A., & Tuunainen, V. K. (2017). Four models of sharing economy platforms. *MIS Quarterly Executive, 16*(4), 231–251.

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.

DailyMail. (2021). Shocking video shows house guests trash an Airbnb rental during an all-out brawl in Dallas. Retrieved September 4, 2021 from https://www.dailymail.co.uk/news/article-9689781/Shocking-video-shows-house-guests-trash-Airbnb-rental-brawl-Dallas.html.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—A study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389–402.

Dolnicar, S. (2017). *Peer-to-peer accommodation networks*. Oxford, UK: Goodfellow Publishers.

Esmark Jones, C. L., Stevens, J. L., Noble, S. M., & Breazeale, M. J. (2020). Panic attack: How illegitimate invasions of privacy cause consumer anxiety and dissatisfaction. *Journal of Public Policy & Marketing, 39*(3), 334–352.

Finch, D., Deephouse, D., & Varella, P. (2015). Examining an individual's legitimacy judgment using the value–attitude system: The role of environmental and economic values and source credibility. *Journal of Business Ethics, 127*(2), 265–281.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Forums, C. W. (2020). Airbnb admits to "technical issue" that resulted in exposure of users' private messages. Retrieved September 4, 2021 from https://www.grcworldforums.com/systems-security/airbnb-admits-to-technical-issue-that-resulted-in-exposure-of-users-private-messages/142.article.

Gabisch, J. A., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing, 31*(1), 13–26.

Gao, P. (2007). Counter-networks in standardization: A perspective of developing countries. *Information Systems Journal, 17*(4), 391–420.

Gilliland, D. I., & Bello, D. C. (2002). Two sides to attitudinal commitment: The effect of calculative and loyalty commitment on enforcement mechanisms in distribution channels. *Journal of the Academy of Marketing Science, 30*(1), 24–43.

Guo, R., Tao, L., Li, C. B., & Wang, T. (2017). A path analysis of greenwashing in a trust crisis among Chinese energy companies: The role of brand legitimacy and brand loyalty. *Journal of Business Ethics, 140*(3), 523–536.

Gupta, M., Esmaeilzadeh, P., Uz, I., & Tennant, V. M. (2019). The effects of national cultural values on individuals' intention to participate in peer-to-peer sharing economy. *Journal of Business Research, 97*, 20–29.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24.

Hair, J. F., Jr., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research, 109*, 101–110.

Hamari, J., Sjöklint, M., & Ukkonen, A. (2016). The sharing economy: Why people participate in collaborative consumption. *Journal of the Association for Information Science and Technology, 67*(9), 2047–2059.

Helms, W. S., Patterson, K. D., & Hudson, B. A. (2019). Let's not "taint" stigma research with legitimacy, please. *Journal of Management Inquiry, 28*(1), 5–10.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems, 116*(1), 2–20.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135.

Hine, C. (1998). Privacy in the marketplace. *The Information Society, 14*(4), 253–262.

Jaap, W., Xiao, M., Thomas, R., Hans, R., & Bernd, S. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*, 915–925.

Jackson, C. (2014). Structural and behavioural independence: Mapping the meaning of agency independence at the field level. *International Review of Administrative Sciences, 80*(2), 257–275.

Jain, D., Dash, M. K., Kumar, A., & Luthra, S. (2021). How is blockchain used in marketing: A review and research agenda. *International Journal of Information Management Data Insights, 1*(2), Article 100044.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105.

Johnston, R., & Michel, S. (2008). Three outcomes of service recovery: Customer recovery, process recovery and employee recovery. *International Journal of Operations & Production Management, 28*(1), 79–99.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618–644.

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

Kar, A. K. (2020). What affects usage satisfaction in mobile payments? Modelling user generated content to develop the "digital service usage satisfaction model". *Information Systems Frontiers, 23*, 1341–1361.

Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights, 1*(2), Article 100015.

Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research, 45*(5), 906–932.

Köbis, C., Soraperra, N., & Shalvi, S. (2021). The consequences of participating in the sharing economy: A transparency-based sharing framework. *Journal of Management, 47*(1), 317–343.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546–580.

Kropp, E., & Totzek, D. (2020). How institutional pressures and systems characteristics shape customer acceptance of smart product-service systems. *Industrial Marketing Management, 91*, 468–482.

Kwak, C., Lee, J., & Lee, H. (2022). Could you ever forget me? Why people want to be forgotten online. *Journal of Business Ethics, 179*, 25–42.

Kwon, S., & Jang, S. S. (2012). Effects of compensation for service recovery: From the equity theory perspective. *International Journal of Hospitality Management, 31*(4), 1235–1243.

Lambert, D. M., & Harrington, T. C. (1990). Measuring nonresponse bias in customer service mail surveys. *Journal of Business Logistics, 11*(2), 5–25.

Lansing, J., Benlian, A., & Sunyaev, A. (2018). "Unblackboxing" decision makers' interpretations of IS certifications in the context of cloud service certifications. *Journal of the Association for Information Systems, 19*(11), 1064–1096.

Lee, D.-J., Sirgy, M. J., Brown, J. R., & Bird, M. M. (2004). Importers' benevolence toward their foreign export suppliers. *Journal of the Academy of Marketing Science, 32*(1), 32–48.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59–87.

Liang, S., Schuckert, M., Law, R., & Chen, C.-C. (2020). The importance of marketer-generated content to peer-to-peer property rental platforms: Evidence from Airbnb. *International Journal of Hospitality Management, 84*, Article 102329.

Litman-Navarro, K. (2021). *We read 150 privacy policies. They were an incomprehensible disaster*. The New York Times. Retrieved September 4, 2021 from https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Liu, B., Pavlou, P. A., & Cheng, X. (2021). Achieving a balance between privacy protection and data collection: A field experimental examination of a theory-driven information technology solution. *Information Systems Research*. https://doi.org/10.1287/isre.2021.1045

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical research. *Computers in Human Behavior, 56*, 225–237.

Lu, B., Wang, Z., & Zhang, S. (2021). Platform-based mechanisms, institutional trust, and continuous use intention: The moderating role of perceived effectiveness of sharing economy institutional mechanisms. *Information & Management, 58*(7), Article 103504.

Lu, B., Zeng, Q., & Fan, W. (2016). Examining macro-sources of institution-based trust in social commerce marketplaces: An empirical study. *Electronic Commerce Research and Applications, 20*, 116–131.

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.

Lutz, C., & Newlands, G. (2018). Consumer segmentation within the sharing economy: The case of Airbnb. *Journal of Business Research, 88*, 187–196.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572–585.

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.

Malhotra, N. K., Schaller, T. K., & Patil, A. (2017). Common method variance in advertising research: When to be concerned and how to control for it. *Journal of Advertising, 46*(1), 193–212.

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

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., & Weaven, S. K. (2020). Data privacy in retail. *Journal of Retailing, 96*(4), 474–489.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly, 37*(2), Article 101442.

Morgan, R. M., & Hunt, S. D. (1994). The commitment–trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20–38.

Mpinganjira, M., & Maduku, D. K. (2019). Ethics of mobile behavioral advertising: Antecedents and outcomes of perceived ethical value of advertised brands. *Journal of Business Research, 95*, 464–478.

Newlands, G., & Lutz, C. (2020). Fairness, legitimacy and the regulation of home-sharing platforms. *International Journal of Contemporary Hospitality Management, 32*(10), 3177–3197.

Nieuwland, S., & Van Melik, R. (2020). Regulating Airbnb: How cities deal with perceived negative externalities of short-term rentals. *Current Issues in Tourism, 23*(7), 811–825.

Nunan, D., & Di Domenico, M. (2017). Big data: A normal accident waiting to happen? *Journal of Business Ethics, 145*(3), 481–491.

NZHerald. (2021). Christchurch Airbnb party fatal stabbing: Property owners 'devastated'. Retrieved September 4, 2021 from https://www.nzherald.co.nz/nz/christchurch-airbnb-party-fatal-stabbing-property-owners-devastated/SWAJKDOCLFXE4ZO5K2YKBU5ZRM/.

Palan, S., & Schitter, C. (2018). Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance, 17*, 22–27.

Park, S., & Tussyadiah, I. P. (2020). How guests develop trust in hosts: An investigation of trust formation in P2P accommodation. *Journal of Travel Research, 59*(8), 1402–1412.

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.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology, 70*, 153–163.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531–544.

Ranzini, G., Etter, M., & Vermeulen, I. (2020). My home on the platform: Exploring the physical privacy concerns of home-sharing providers. *International Journal of Hospitality Management, 86*, Article 102433.

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332–344.

Scott, W. R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Shao, Z., & Yin, H. (2019). Building customers' trust in the ridesharing platform with institutional mechanisms: An empirical study in China. *Internet Research: Electronic Networking Applications and Policy, 29*(5), 1040–1063.

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *European Journal of Marketing, 53*(11), 2322–2347.

Shuqair, S., Pinto, D. C., & Mattila, A. S. (2019). Benefits of authenticity: Post-failure loyalty in the sharing economy. *Annals of Tourism Research, 78*, Article 102741.

Slimane, K. B., Chaney, D., Humphreys, A., & Leca, B. (2019). Bringing institutional theory to marketing: Taking stock and future research directions. *Journal of Business Research, 105*, 389–394.

Statista. (2021). Airbnb – statistics & facts. Retrieved September 4, 2021 from https://www.statista.com/topics/2273/airbnb/.

Steenkamp, J. B. E., & Maydeu-Olivares, A. (2021). An updated paradigm for evaluating measurement invariance incorporating common method variance and its assessment. *Journal of the Academy of Marketing Science, 49*(1), 5–29.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571–610.

Suddaby, R., Bitektine, A., & Haack, P. (2017). Legitimacy. *Academy of Management Annals, 11*(1), 451–478.

Ter Huurne, M., Ronteltap, A., Corten, R., & Buskens, V. (2017). Antecedents of trust in the sharing economy: A systematic review. *Journal of Consumer Behaviour, 16*(6), 485–498.

Tost, L. P. (2011). An integrative model of legitimacy judgments. *Academy of Management Review, 36*(4), 686–710.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562.

Tussyadiah, I. P. (2016). Factors of satisfaction and intention to use peer-to-peer accommodation. *International Journal of Hospitality Management, 55*, 70–80.

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing, 35*(1), 144–158.

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H.-H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 1679–1703.

Wang, Y., Asaad, Y., & Filieri, R. (2020). What makes hosts trust Airbnb? Antecedents of hosts' trust toward Airbnb and its impact on continuance intention. *Journal of Travel Research, 59*(4), 686–703.

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

Zaefarian, G., Thiesbrummel, C., Henneberg, S. C., & Naudé, P. (2017). Different recipes for success in business relationships. *Industrial Marketing Management, 63*, 69–81.

Zhang, J., Deephouse, D. L., van Gorp, D., & Ebbers, H. (2020). Individuals' perceptions of the legitimacy of emerging market multinationals: Ethical foundations and construct validation. *Journal of Business Ethics, 176*, 801–825.