That’s private!

Understanding travelers’ privacy concerns and online data disclosure[1]

Athina Ioannou
School of Hospitality and Tourism Management
University of Surrey, United Kingdom
Email: a.ioannou@surrey.ac.uk

Iis Tussyadiah
School of Hospitality and Tourism Management
University of Surrey, United Kingdom
Email: i.tussyadiah@surrey.ac.uk

Graham Miller
School of Hospitality and Tourism Management
University of Surrey, United Kingdom
Email: g.miller@surrey.ac.uk

Accepted for publication in
Journal of Travel Research
16th July 2020

Acknowledgement

This work was part of the PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers (PriVELT) Project, funded by the UK’s Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/R033196/1.

[1] Citation: Ioannou, A., Tussyadiah, I., Miller, G. (2020). That’s Private! Understanding travelers’ privacy concerns and online data disclosure. Journal of Travel Research.

Abstract

Against the backdrop of advancements in technology and its deployment by companies and governments to collect sensitive personal information, information privacy has become an issue of great interest for academics, practitioners, and the general public. The travel and tourism industry has been pioneering the collection and use of biometric data for identity verification. Yet, privacy research focusing on the travel context is scarce. This study developed a valid measurement of Travelers' Online Privacy Concerns (TOPC) through a series of empirical studies: pilot (*N*=277) and cross-validation (*N*=287). TOPC was then assessed for its predictive validity in its relationships with trust, risk, and intention to disclose four types of personal data: biometric, identifiers, biographic, and behavioral data (*N*=685). Results highlight the role of trust in mitigating the relationship between travelers' privacy concerns and data disclosure. This study provides valuable contribution to research and practice on data privacy in travel.

Keywords: privacy concerns, data disclosure, personal data, data sharing, traveler, online travel environment

Introduction

The year 2018 saw a total of 1.4 billion in international tourist arrivals, a 5% increase from the year prior, making it the ninth consecutive year of sustained expansion of travel and tourism worldwide (World Tourism Organization, 2019). While the World Tourism Organization (UNWTO) attributed this growth mainly to a strong global economy, digital technologies are also credited as driving the transformation in travelers' experience (World Tourism Organization, 2019). As more and more people engage in travel and tourism, the drive to ease travel facilitation through advanced technologies intensifies. As a result, an increasing number of travel service providers and tourism destinations rely on advanced technologies to offer hyper-personalized services, measure tourism experiences in real time, and improve their business performance (World Tourism Organization, 2019). For example, a cruise line company offers passengers a coin-sized wearable device called the Ocean Medallion. With around 8,000 sensors installed on the ship, the medallion can be used to track passengers' real-time location and movements. Using the combination of these and other data gathered from passengers' personal profile they completed online before the trip, such as food preferences and allergies, hobbies, and lifestyle, crew members are able to offer highly personalized services (Hinson 2019). Approaches to personalization and travel facilitation are implemented at a much larger scale by government agencies and private companies around the globe to tackle the complexity of managing an increasing number of travelers. Booking engines and travel companies adopt personalized travel planning with artificial intelligence (AI), relying on customer profiles to send personalized recommendations and predictions of prices, delays, etc. Various travel consortia introduced travelers' digital identity, largely taking advantage of biometric verification, for secure and seamless border crossing (Sorrells, 2019). Ultimately, these solutions offer frictionless end-to-end experience for travelers while at the same time contribute to geopolitical security worldwide (WEF, 2018). For such technological implementation to be effective, companies and government agencies depend on the availability of travelers' (personal) data and thus travelers' willingness to disclose information. This presents a challenge because while the collection and use of personal data can lead to more attractive tourism offers and more efficient travel, it can also create security risks, privacy concerns and so ultimately hinder data disclosure.

The continuous rise and development of new technological solutions, having significantly influenced the way travelers gain access and use travel environments, make the concept of privacy more current than ever (Xiang et al. 2015). Public awareness of information privacy has been shaped by recent 'eye-opening' events, such as the Cambridge Analytica scandal involving the collection and use of personal data on Facebook without user consent, US government's adoption of biometric verification through facial recognition for all travelers crossing the US border (Alba 2019), the Google health data scandal (Project Nightingale) collecting detailed personal health information of millions of US people without notifying them (Copeland 2019), and many others. However, despite the growing importance of this issue, studies about privacy concerns in the travel context remain relatively scarce (Ozturk et al. 2017; Wozniak et al. 2018). Extant literature generally focuses on the measurement of privacy concerns in generic online environments (Malhotra, Kim, and Agarwal 2004; Stewart and Segars 2002; Buchanan et al. 2007; Taddicken 2010). In these studies, privacy is investigated in an institutional context, whereby privacy concerns are suggested to originate from individuals' relationships with companies and organizations with regards to the collection and use of personal information (Ozdemir et al. 2017). The complexities of data sharing and use in the travel context might create privacy threats stemming not only from the aforementioned, but also from the specificities of the context. Contextualizing privacy studies in travel is therefore important not only theoretically to gauge whether generic models of privacy concerns developed previously will apply in specific consumption context, but also practically to ameliorate business challenges around technological requirements for the collection and use of travelers' personal information.

Tussyadiah, Li, and Miller (2019) suggest that travelers may have less awareness of privacy threats and greater vulnerability to privacy violations due to existing and emerging issues contributing to the idiosyncrasy of information privacy. These include: (a) new technologies developed for collection and processing of travelers' data (e.g., AI-powered authentication) could induce additional layers of privacy concerns; (b) travelers being more inclined to share personal information due to inflated sense of urgency to obtain service or information; (c) limited opportunities for trust building to occur as the interactions between travelers and providers are short-lived; (d) travelers often feel the urge to share travel experiences online, which may contain sensitive information of selves and others; and (e) risks of compounded physical and digital information, where information exchanged during interactions with providers in physical environments (e.g., while on tour) could be captured and shared online (e.g., pictures posted with an online review). Therefore, it is considered necessary to refine existing measures of privacy concerns by incorporating different aspects of information privacy in the travel context and validating the measures with travelers (Tussyadiah, Li, and Miller 2019).

To address the gap in literature on data privacy in travel, the goals of this study are (1) to adapt existing measurements of privacy concerns to fit the travel context and (2) to test the predictive validity of the adapted measurements by assessing the effect of travelers' privacy concerns on intention to disclose various types of personal information to travel service providers online. Grounded on the trust–risk framework (Mcknight, Cummings, and Chervany

1998), this study contributes to the operationalization of privacy concerns measurements in online travel environments and provides empirical support to explicate the relationship between privacy concerns, risk, trust, and disclosure intention for four types of personal information (i.e., biometric, identifiers, biographic, and behavioral information) relevant to the context of travel. This study provides managerial implications for travel providers with regards to aspects of data privacy to pay particular attention to when attempting to encourage travelers to disclose various types of personal data, especially for those relying on various travelers' personal information to create personalized offer or promotion.

Theoretical Background

Privacy Concerns

The concept of privacy has been described differently from various disciplinary perspectives. From a legal perspective, privacy is defined as a right to control the circulation of information about oneself, as manifested in such regulation as the ‘right to be forgotten’ or right to erasure (General Data Protection Regulation [GDPR], 2020). Exploring privacy in more depth, researchers uncovered the phenomenon of privacy paradox: although people reported a high level of privacy concerns regarding sharing sensitive personal information, their actual sharing behavior is inconsistent with these concerns (Kokolakis 2017; Gerber, Gerber, and Volkamer 2018). Thus, privacy is then defined as a commodity, encapsulating the idea of economic value and cost-trade benefit (Smith, Dinev, and Xu 2011). Another stream of research developed the control-based definition describing privacy as a state of control regarding the transactions between an individual and others in order to enhance autonomy and reduce vulnerability (Smith, Dinev, and Xu 2011). The latter conceptualization has been used to define information privacy in information systems (IS) literature, describing it as the desire and ability to control the acquisition of one’s personal information and secondary uses of this information (Bélanger and Crossler 2011). In summary, extant literature does not provide one equivocal operational definition of privacy, reflecting the complexity and meaning of the concept.

Furthermore, several studies have attempted to develop methods to measure privacy; however “because of the near impossibility of measuring privacy itself” (Smith et al. 2011), (p. 997), past research has been using a proxy to measure privacy. One such proxy is privacy concerns. Several studies have attempted to operationalize the measure of privacy concerns. The most widely adopted scale is the Concern for Information Privacy (CFIP) instrument developed by Smith et al. (1996). CFIP includes four dimensions of privacy concerns: collection, error, secondary uses, and unauthorized access (Bélanger and Crossler 2011). Collection reflects the perception and concerns of individuals that excessive amount of personal information is being collected, accumulated, and stored by various entities in society (Smith, Milberg, and Burke 1996). Error describes the concerns of individuals that the protection measures taken against accidental or deliberate errors are inadequate (Smith, Milberg, and Burke 1996). Secondary uses refer to individuals' concerns that collected personal information is used either internally or externally by organizations for other than the stated purposes, without peoples' authorization (Smith, Milberg, and Burke 1996). Unauthorized access describes the concerns of individuals that personal information is readily available to even unauthorized people or organizations (Smith, Milberg, and Burke 1996).

Following the CFIP instrument, the Internet Users' Information Privacy Concerns (IUIPC) instrument was developed to measure privacy concerns of consumers transacting in e-commerce environments (Malhotra, Kim, and Agarwal 2004). IUIPC includes three dimensions: control, awareness, and collection. *Control* describes the sense of control that people have over their personal information manifested by the existence of voice, such as approval or modification, or exit, such as opt out. *Awareness* of privacy practices refers to the passive dimension of information privacy, which is the degree that a consumer is aware of organizational information privacy practices. *Collection* refers to the degree that a person feels concerned about the amount of personal information that other entities are holding comparative to the benefits received in exchange (Malhotra, Kim, and Agarwal 2004). A number of studies followed, attempting either to improve the items of existing scales or adapting them in different contexts, such as Internet use (Malhotra, Kim, and Agarwal 2004; Stewart and Segars 2002; Buchanan et al. 2007; Taddicken 2010).

The issue of data privacy also revolves around specific types of data being shared. According to the General Data Protection Regulation (GDPR, 2020), personal data is any information related to an identified or identifiable natural person. This refers to any information that can identify an individual, such as biographical, workplace, education, location, physical, physiological, genetic, mental, economic, cultural, or social data of a person (GDPR, 2020). In consumer contexts, it may include basic demographic information (e.g., name, home address), health data (e.g., medical records), financial information (e.g., credit card, credit score), or biometric information (e.g., facial image, fingerprint) (Kim and Kim 2018; Morosan 2019; Y. Li 2011). From a comprehensive review of empirical studies on privacy, Li (2011) found that people are more sensitive to some types of information requests than others. That is, consumers feel more protective of the types of information they perceive as more sensitive as they associate the disclosure of these information with different levels of risk (Malhotra, Kim, and Agarwal 2004; Morosan 2019). Nevertheless, the focus of most privacy research has been limited to disclosure of basic demographic or financial information.

Privacy and Travel

Existing privacy research has focused mainly on generic online environments with less consideration on new aspects and contexts of use (e.g., Smith et al. 1996). There is a dearth of literature focusing on privacy in the travel context, particularly those providing empirical support to measure travelers’ privacy concerns (Tussyadiah, Li, and Miller 2019). Among the few privacy studies in travel and tourism are investigations of privacy risks and breaches in location based social media (LBSM) (Vu, Law, and Li 2018), travelers perceptions of privacy in smart tourism destinations (Femenia-Serra, Perles-Ribes, and Ivars-Baidal 2018), and users' privacy concerns when using mobile booking (Ozturk et al. 2017). Fewer studies have focused on privacy concerns and their impact on behavioral outcomes (Bonsón Ponte, Carvajal-Trujillo, and Escobar-Rodríguez 2015a, Hew et al. 2017). Research investigating privacy concerns and information disclosure in the travel context remains extremely limited (Wozniak et al. 2018).

Travelers using online applications throughout the spectrum of their customer journey are faced with numerous requests for personal information. These requests come from a myriad of service providers, such as airline companies, hotels, travel agencies, mobile app developers, location-based services (LBS), online review platforms, social networking sites, and others. Some of these providers are local to the destination (e.g., destination apps), thus are not familiar to the travelers, and some are connected to each other (e.g., hotels partnering with online travel agencies and tour operators), thus might share a certain amount of customer data with each other. As a result, the complexities around the amalgamation of various online travel providers may contribute to privacy concerns beyond those captured in general online interactions.

Additionally, privacy concerns could arise from the use of a wide range of new disruptive technologies, especially those converging the physical and digital worlds in order to enhance the travel experience. The use of wearables devices, sensors, and Internet-of-Things (IoT) in smart cities and smart tourism destinations, collecting continuous flow of data in real time, might augment or create new aspects of privacy concerns for travelers as they might be unfamiliar with local regulations regarding (or unaware of giving consent to) the collection and use of personal data.

The use smartphones and LBS during travel can create additional value and enhance overall travel experience via relevant tourist information on the go, but can also raise plenty of privacy issues and threats for users. The collection, storage, and use of geographical location as well as the probability of privacy abuse constitutes a major concern for users of LBS (Anuar and Gretzel 2011). Aiming to provide unique travel experiences, more and more travel providers offer personalized services, such as travel packages (e.g., bundling flight and hotel) tailored to travelers' browsing and purchasing preferences (i.e., behavioral data) (Lee and Cranage 2011). Although travelers value the benefits of personalization from the fit of the provided products and the convenience of them being delivered proactively (Chellapa and Sin 2005), personalization provokes information privacy concerns as travelers become aware of the amount of personal behavioral information collected and used to create the personalized products (Karwatzki et al. 2017). Lee and Cranage (2011) argue that personalized travel products may be perceived as less invasive as they usually require much less sensitive information compared to those from financial agencies or medical services. However, emerging travel technologies such as biometric verification at airports require the collection, use, and storage of new types of information that are considered highly sensitive, such as face and retina images, fingerprints, and speech recognition (i.e. biometric data). At times, travelers may perceive that they did not have a choice to opt out from sharing their biometric data for processing at airports, or that they were not appropriately notified or asked to give consent in advance of collection and use of their biometric data (Street, 2019).

In sum, contextualizing online privacy concerns in travel requires careful consideration of *who* collects, uses, stores, and shares travelers' personal information (e.g., online travel companies), *why, how,* and *what* types of data are collected, used, stored, and shared (e.g., behavioral data, biometric data). It is crucial to refine the measurements of travelers' privacy concerns to incorporate awareness of collection and potential misuse of personal information with the aforementioned considerations in mind.

Hypotheses Development

This study draws its theoretical foundation from the Antecedents–Privacy Concerns–Outcomes (APCO) (Smith, Dinev, and Xu 2011) and trust–risk frameworks (Mcknight, Cummings, and Chervany 1998). Smith, Dinev, and Xu (2011) offer a macro model, Antecedents–Privacy Concerns–Outcomes, to explain the relationship between privacy concerns and other constructs, such as behavioral reactions (e.g., information disclosure), privacy risks, and benefits. The trust–risk framework has been adopted to explain various behaviors in uncertain environments; in cases where potential risks are present, trust plays a major role in determining an individual's behavior (Malhotra, Kim, and Agarwal 2004). Studies show that individuals with higher concerns over their privacy are more likely to show less trust in companies/providers, affecting their privacy decisions and willingness to disclose information (Ozturk et al. 2017). Following the study of Malhotra, Kim, and Agarwal (2004), the trust–risk framework was adopted in this study to evaluate the predictive validity of the context specific measurement scale of privacy concerns in a causal model, and more specifically to test the influence of travelers' privacy concerns on willingeness to disclose personal information.

Effects of Travelers' Online Privacy Concerns on Trust and Risk

Belief constructs, such as risk and trust, have been associated with privacy concerns and privacy-related behaviors in a wealth of literature. Perceived privacy risk can be defined as the “expectation of losses associated with the disclosure of personal information online” (Xu et al. 2008, 5), while trust can be described as one’s “willingness to be vulnerable to the actions of another” (Benamati, Ozdemir, and Smith 2017, 588). It has been shown that people with high privacy concerns exhibit lower trust in online providers and higher perceived risk (Malhotra, Kim, and Agarwal 2004). Confirming this finding, Ozturk et al. (2017) demonstrated that mobile users who are concerned about their information privacy show less trust in mobile hotel booking systems. Thus, it can be hypothesized that travelers with high privacy concerns will be likely to have lower trusting beliefs and higher risk beliefs:

H1. Travelers’ online privacy concerns are negatively associated with trusting beliefs.

H2. Travelers’ online privacy concerns are positively associated with risk beliefs.

Relationship between Trust and Risk

The use of new technologies is often associated with a higher perceived risk by consumers (Ozturk et al. 2017). However, previous studies have demonstrated that sufficient level of trust in a provider or a vendor can actually outweigh the perceived risk (Ozturk et al. 2017). It has been shown that the higher trust beliefs a consumer has over an online business provider, the less likely s/he is to foresee risk during an interaction or transaction that includes disclosure of personal information (Malhotra, Kim, and Agarwal 2004). Ozturk et al. (2017) found that trust improves consumers’ beliefs in hotel booking platforms and their infrastructure, thus decreases the risk associated with potential transactions. Likewise, Agag and El-Masry (2017) showed that consumer trust in online travel websites negatively influences the perceived risk of online shopping. Therefore, it can be hypothesized that:

H3. Trusting beliefs will have a negative association with risk beliefs.

Effects of Trust and Risk on Willingness to Share Information

In existing trust–risk research (Mcknight, Cummings, and Chervany 1998), trusting and risk beliefs are considered critical in significantly affecting behavioral intention. Trust has a positive impact on willingness to share information (Malhotra, Kim, and Agarwal 2004; Benamati, Ozdemir, and Smith 2017), while higher perceived risk can decrease willingness to share information with online providers (Keith et al. 2013; Malhotra, Kim, and Agarwal 2004). Keith et al. (2013) found that increased perceived privacy risk from a mobile application decreases users' intention to share personal information, including location and financial information. Also, Halevi et al. (2015) found that risk perceptions have a negative influence on users' intention to share biometric (fingerprint) data with an online vendor. Thus, it can be hypothesized that:

H4. Trusting beliefs will have a positive effect on intention to share personal information.

H5. Risk beliefs will have a negative effect on intention to share personal information.

Methodology

In order to investigate travelers' online privacy concerns and their willingness to disclose personal information with online travel providers, this study was conducted in two stages. Stage 1 included a pretest by pooling a set of initial items identified from a comprehensive literature review, refining the measurement instrument, and evaluating its validity and reliability in actual conditions in a pilot test. A cross-validation study was conducted to establish the generalizability of the developed instrument in a new sample. The aim of Stage 2 was to establish the predictive validity of the adapted instrument in a nomological network by investigating the effect of online privacy concerns of travelers on willingness to disclose information using the trust–risk framework. Details of measurement items, data collection, and data analysis will be provided in the following subsections.

Stage 1. Measuring Travelers' Online Privacy Concerns (TOPC)

The aim of Stage 1 of the study was to identify the measurement of privacy concerns befitting those of travelers interacting with providers in an online environment/setting. Various existing scales were reviewed to develop a reliable and valid scale of online privacy concerns in the context of travel. Following best practices of scale development (Mackenzie et al. 2011; Carpenter 2018), this stage was conducted through the following three consecutive steps: a pre-test, a pilot test, and a cross-validation study.

Pre-test

The objective of the pre-test was to refine a pool of potential items to measure online privacy concerns in the context of travel. The pre-test process followed the recommendations and guidance of existing literature on scale development (Worthington and Whittaker 2006; DeVellis 2016). First, a comprehensive literature review in relevant disciplines (i.e., Information Systems, Business, and Tourism Management) was conducted to identify existing measures of privacy concerns. This resulted in the identification of several instruments, including CFIP and IUIPC, as well as self-developed measures adapted for the purposes of specific research study (Stewart and Segars 2002; Malhotra, Kim, and Agarwal 2004; Xu et al. 2008; Wozniak et al. 2018; Huang et al. 2017; Preibusch 2013; Li 2014). The item selection process was conducted by identifying common themes, considering the established privacy concerns dimensions, such as collection, secondary use, and improper access of data (Smith, Milberg, and Burke 1996). Duplicate items or slightly differently worded items were removed, resulting in an initial pool of 51 items. Next, the selected items were adapted to the online travel context by modifying words that represent the context of use, such as replacing "online company" with "online travel company."

An online questionnaire was developed to include the 51 items and distributed to experts in travel and information technologies (i.e., academics affiliated with a public university in the UK working with expertise in the field of Tourism) in order to test how well each item represents online privacy concerns of travelers, thus testing the face validity and content validity of the items. Extant research has recommended having knowledgeable people (expert judges) review the initial pool of items for the development of a scale and it is widely adopted as a crucial step in the scale development process (Worthington and Whittaker 2006; Hardesty and Bearden 2004; DeVellis 2016). The experts were asked to rate each item with a three-point scale: 1 = "not representative," 2 = "somewhat representative," and 3 = "clearly representative." For an item to be retained for the following steps, all experts should have rated it with no less than 2 ("somewhat representative"). The pre-test study received a total of 18 answers from expert judges, refining the total number of items in the proposed scale from 51 to 22 items.

Pilot Test

A pilot study was carried out to test the instrument and further refine its items. An online survey was distributed to a panel of UK residents who have traveled and transacted with an online travel company within the past six months (i.e., a set of screening questions regarding previous travelling experience as well as frequency of booking tickets and accommodation services online during the last six months was included in the survey). A total of 330 participants completed the survey and after removing missing data and disqualified participants, the sample size was reduced to 277. The majority of participants were female (53.4%), mostly between the ages of 26-45 years old (44%), and achieved a high school qualification (49%) (see Table A1 in Appendix A).

Exploratory Factor Analysis (EFA) was performed to extract and identify latent variables from the manifest variable (Carpenter 2018). Maximum Likelihood (ML) with Promax rotation based on eigenvalues more than one was used as the factor extraction method. According to Carpenter (2018), ML results are more generalizable than other methods. Promax rotation was selected in order to allow for the likelihood of correlations among the factors (Belanger, Hiller, and Smith 2002).

After inspecting the communalities and pattern matrix (see Table 1), items with factor loadings less than 0.5 as well as items with high cross loadings (>0.3) were discarded in order to determine a simple factor structure. Bartlett's test of sphericity demonstrated significant correlation between the original variables ($\chi_2=4006.126$, $p<0.001$) while Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy is close to 1 (KMO=0.912); together they indicate that the data is suitable for factor analysis.

Table 1 about here

The results of EFA show a final solution of two factors consisting of 17 items, confirming the multidimensionality of the scale. Variance explained was 43.5% for the first factor and 20.7% for the second factor (see Table A2 in Appendix A). Emerging factors were interpreted as representing: (1) Self-privacy concerns (SPC) and (2) Normative privacy concerns (NPC) (see Table 2). The reliability of the new adapted scale was tested by checking the value of Cronbach's alpha. Alpha values above 0.8 are considered a good result, while those above 0.9 demonstrate excellent reliability (George and Mallery 2003). The results show that Cronbach's Alpha of 0.949 for the first factor and 0.886 for the second factor, confirming very good reliability of the new adapted scale.

Table 2 about here

The next step was to evaluate the latent structure of the instrument as well as the goodness of fit of the measurement by performing Confirmatory Factor Analysis (CFA) (Mackenzie, Podsakoff, and Podsakoff 2011). Different plausible representations of the phenomenon of Travelers' Online Privacy Concerns (TOPC) were tested to establish the dimensionality of the scale. Various models were estimated: a two-factor first order model, a three-factor model, as well as second-order models with two and three factors, respectively. Results of the CFA showed that a two-factor model (Chi-square Mean/Degree of Freedom (*CMIN/DF*)=2.688 [<3 and >2], Comparative Fit Index (*CFI*)=0.953, Root Mean Square Error of Approximation (*RMSEA*)=0.078 [<0.08]) (see Figure 1) fits the data better.

Figure 1 about here

Cross-validation

To establish whether the findings of the pilot test regarding the validity and reliability of the scale would be generalized in a new sample, an online survey was conducted to cross-validate the instrument using a new sample following Mackenzie et al. (2011). An online questionnaire was distributed to a consumer panel in the US. The survey included the final 17-item instrument resulted from the pilot and the same qualifying questions aiming to identify relevant participants (i.e., those who have traveled and transacted with an online travel company within the past six months). Data were collected from 300 participants. After removing missing data, the usable dataset was 287 responses. The majority of participants were male (57.1%), mostly between the ages of 26-45 years old (72%), and achieved a highest qualification of a bachelor's degree (64%) (see Table A1 in Appendix A). It is apparent that the recruited sample of the cross-validation study (the US) has different demographic characteristics from the sample of pilot test (the UK). Therefore, it can be concluded that the scale was tested in a different sample.

The CFA results showed that the data fits the model well; the fit indices fall between the suggested thresholds (*CMIN/DF*=2.749 [<3], *CFI*=0.948, *RMSEA*=0.078 [<0.08]). Thus, it can be suggested that the two-factor first order model (Model 1) constitutes a better conceptualization of Travelers' Online Privacy Concerns (TOPC), having been tested in two different samples, the UK and the US. Moreover, convergent and discriminant validity, as well as reliability of the scale were tested. Cronbach's Alpha value was 0.944 for the latent construct, 0.957 for the first factor, and 0.890 for the second factor, indicating excellent reliability of the newly adapted scale. Discriminant validity was assessed by conducting a chi-square difference test between two models, one in which the constructs are correlated and another without correlations. The chi-square difference test revealed a significant difference between the two models at $p<0.001$, with Model 1 (no correlations) $\chi_2=350.5$ and Model 2 (with correlations) $\chi_2=313.4$. Therefore, discriminant validity was established. Discriminant and convergent validity were assessed by estimating the Average Variance Extracted (AVE) and composite reliability (CR) scores, ensuring that both exceed the required thresholds: AVE>0.5 and CR>0.7 (Hair et al. 2010). Results showed for the first factor AVE=0.67 and CR=0.96 and for the second factor AVE=0.58 and CR=0.89, thus establishing both discriminant and convergent validity of the psychometric properties of the examined latent construct.

Discussion

Results of the pilot test supported the validity and reliability of the proposed 17-item measurement scale identified in the pre-test, empirically demonstrating that the latent construct of privacy concerns consists of two factors: self-privacy concerns and normative privacy concerns. These represent both personal feelings towards data sharing and potential secondary use of personal information as well as normative perceptions about appropriate data sharing business practices. The results were cross-validated using a different sample, establishing the validity of the new adapted instrument and supporting that the scale constitutes a reliable multidimensional measurement scale of privacy concerns in the online travel context.

Extant privacy literature has mostly adopted an organizational perspective of privacy concerns' dimensions, focusing more on the business practices of collecting and (mis)using data and less on individual's beliefs towards data collection, sharing and use of their own personal information (Ozdemir, Jeff Smith, and Benamati 2017). This study takes on a dual perspective, focusing on both the organizational and individual dimensions of privacy concerns, highlighting the need to distinguish between individual (self) privacy concerns and normative privacy concerns, which has not been addressed by existing literature. Self-privacy concerns represent personal concerns of individuals towards the sharing and re-use of their personal information by business providers; while normative beliefs reflect normative judgements about how the world and society should be (how society should preserve others' privacy) and more specifically about how business' data sharing practices should be (Mudrack 2007).

The resulting instrument is a multidimensional (two-factor) measurement consisting of (1) normative concerns about general business practices in terms of collection and use of personal information and (2) concerns towards the collection and (re-)use of own personal information. The first dimension is akin to Malhotra et al. (2004)'s 'awareness' factor, reflecting users' awareness of business practices on collection and management of personal data. The second dimension from this study includes concerns regarding 'collection,' 'control,' 'errors,' and 'improper access' of personal information as suggested in Smith et al. (1996)'s and Malhotra et al. (2004)'s scale. Moreover, the newly adapted scale embeds new travel-specific aspects into the conceptualization of privacy concerns, considering new types of data and additional media channels, such as location data for location-based social networks, deployed throughout the customer journey. Therefore, it can be suggested that the scale reinforces the important dimensions of general online privacy concerns while more accurately assesses specific privacy concerns of travelers.

Stage 2. Estimating the Effect of Travelers' Online Privacy Concerns on Disclosure

The second stage of the study aimed to investigate the effect of Travelers' Online Privacy Concerns on information disclosure, thus testing the predictive validity of the developed two-factor first order 17-item instrument of TOPC in a nomological network using the trust–risk framework (see Figure 2 for the model and Appendix B for measurement items). Particularly, it aims to understand the influence of TOPC on individual's willingness to disclose information (Malhotra, Kim, and Agarwal 2004). Similar to the pilot test, an online survey was distributed to UK residents who have traveled and transacted with an online travel company within the past six months. A total of 836 responses were collected from the panel survey. After excluding responses with missing data and disqualified participants, the usable sample size was 685. Among the respondents, 47.2% were male, with the majority of them being between 26 and 45 years old (45%) and having finished high school (38.8%) (see Table A1 in Appendix A).

Figure 2 about here

Exploratory Factor Analysis (EFA) with Maximum Likelihood (ML) and Promax rotation was performed to uncover the underlying structure of willingness to share different types of personal information. Items with factor loadings less than 0.5 and those with high cross loadings (>0.3) were discarded in order to determine a simple factor structure. Bartlett's test of sphericity demonstrated significant correlation between the original variables (χ_2=9965.325, p<0.001) while Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy is close to 1 (KMO=0.9), thus indicating that the data are suitable for factor analysis. Four factors with 19 out of 23 items were retained, explaining 61% of the total variance. The four factors were labelled after the characteristics of the data types: biometric information, biographical information, behavioral data and identifiers (see Table 3). Variance explained was 34.4% for biographic information, 21.8% for biometric information, 6.6% for behavioral data, and 4.4% for identifiers (see Table A2 in Appendix A).

Table 3 about here

Biometric information refers to sensitive personal information about a person's physical characteristics that can be used to determine his/her identity. Items loading on this factor are fingerprint, voice sample, face scan, and iris/retina image. Identifiers refer to sensitive personal information of a person including financial information such as credit card number, bank account number, as well as identification information such as passport and driver's license number. Biographic information refers to a person's basic personal information describing the demographics of a person such as name and date of birth, email and home address, and phone number. Behavioral data refer to the information about the behavioral patterns of individuals including hobbies and personal interests, personal preferences such as room selection in a hotel and dietary requirements, real time position, smartphone search history (cookies), activity data sensor (body movements, number of steps, floors), specific expenses in places they have travelled, and services they have purchased. The reliability for each factor was calculated; Cronbach's Alpha values were: biometric information (0.917), identifiers (0.869), biographic information (0.849), and behavioral data (0.838); indicating reliability.

In order to assess the model, covariance-based structural equation modeling (CB-SEM) was performed by first conducting a CFA to evaluate the reliability and validity of the constructs and then testing the proposed hypotheses by evaluating the structural model and the path coefficients. CB-SEM was determined to be the most appropriate choice for establishing the validity and reliability of the model in a nomological network (Hair et al. 2019). In the first stage, the measurement model is estimated to gauge how well the proposed model fits the collected data. This includes the evaluation of the convergent and discriminant validity, as well as reliability of the latent constructs. To assess reliability, all outer loadings of items on their respective latent constructs were checked to ensure they exceed 0.5. One item with very low outer loadings (<0.5) was removed to allow for better indicator reliability; the rest were retained. Moreover, Cronbach's Alpha values were larger than 0.8, indicating excellent reliability. Discriminant and convergent validity were assessed by estimating the AVE and CR scores, ensuring that both exceed the required thresholds, AVE>0.5 and CR>0.7 (Hair et al. 2010). Results showed that both discriminant and convergent validity were established, confirming the psychometric properties of the examined latent constructs. Table 4 presents the CR, Cronbach Alpha, AVE, as well as mean and standard deviation values for all constructs in the measurement model. Tables 5 shows the results of the discriminant validity assessment using the Fornell–Larcker criterion.

Tables 4 – 5 about here

In order to assess the fit of the model, several goodness-of-fit indices were checked. Results showed that the data fit the final model well; the fit indices fall between the suggested thresholds (*CMIN/DF*=3.077 [3-5], *CFI*=0.927, *RMSEA*=0.055 [<0.08]) (Hair et al. 2010). Furthermore, two popular tests were conducted in order to check for Common Method Variance (CMV) on the observed relationships among the measured variables (Mackenzie, Podsakoff, and Podsakoff 2011; Podsakoff et al. 2003). First, Harman's single factor test was performed; results indicated that only 36% of variance in all variables can be explained by a single factor. This demonstrates that CMV is not a concern in our study. A further test was conducted to ensure that no correlations exceed 0.90, which could indicate a possible bias in the collected data (Pavlou, Liang, and Xue 2007). Results show that none of the calculated correlations exceed the suggested threshold, thus

CMV is not a concern in this study. Consequently, the rest of the analysis can continue without the addition of a common latent factor.

The second stage of the analysis included the evaluation of the proposed hypotheses. In order to assess the structural model, the path coefficients between the investigated variables were estimated. The goodness-of-fit indices indicate that the data fits the model well (*CMIN/DF*=3.460 [3-5], *CFI*=0.903, *RMSEA*=0.06 [<0.08]) (Hair et al. 2010). The results of the hypotheses testing showed that all except three of the proposed hypotheses were supported (see Table 6); normative privacy concerns are negatively associated with trust (*b*=-0.100, *p*<0.05) and risk (*b*=-0.252, *p*<0.001), while self-privacy concerns showed a negative impact on trust (*b*=-0.409, *p*<0.001). Moreover, trust showed a positive association with willingness to share all types of information, biographical data (*b*=0.215, *p*<0.001), behavioral data (*b*=0.317, *p*<0.001), biometric information (*b*=0.317, *p*<0.001), and identifiers (*b*=0.257, *p*<0.001). Risk had a negative effect on willingness to share biographical information (*b*=-0.395, *p*<0.001) and identifiers (*b*=0.371, *p*<0.001). In addition to the independent variables, gender, age, and education were incorporated as control variables to gauge whether demographic variables have an influence on willingness to share personal information. Results are shown in Table 7, demonstrating significant effects of gender on all willingness to share variables, age on all but biographic data, and education on biometric data. Table 8 shows the R_2 values for the dependent variables in the model, which also encapsulate the effects of the control variables.

Tables 6 – 8 about here

Discussion

A multidimensional instrument for the measurement of privacy concerns of travelers interacting with providers in online contexts, TOPC, comprising self-privacy concerns and normative concerns, was developed in Stage 1. Stage 2 proceeded to test the effect of TOPC on the intention to share personal information with online providers. Consistent with previous studies (Ozturk et al. 2017), the results of this study demonstrated that travelers' privacy concerns have a significant negative impact on trusting beliefs and a positive impact on risk beliefs (H1 and H2). Findings suggest that travelers with elevated privacy concerns are more likely to have lower levels of trust in online travel providers and higher levels of perceived risk associated with data disclosure.

Moreover, the results revealed that trust has a significant and negative relationship with risk thus demonstrating the important role of trust in acting as a mitigator when a traveler is asked to disclose personal information (H3). However, the study results revealed that normative privacy concerns, the concerns of how business providers deal with travelers' personal data, show a negative association with risk beliefs, showing the opposite direction to what was expected (H2b). One possible reason for this unexpected result is that strong normative beliefs regarding privacy protection (i.e., what travelers believe the service providers ought to do when handling travelers' personal data), independent of concerns for the privacy of self, will lower the perception of risk during interactions and transactions with online travel providers.

Furthermore, the results indicated that trusting beliefs positively influence willingness to share four types of personal information: biometric, identifiers, biographic, and behavioral data. These confirm that higher levels of trust in online travel providers increase travelers' willingness to share various types of information with the providers, as suggested in the findings from Benamati, Ozdemir, and Smith (2017).

The results showed the negative impact of risk beliefs on travelers' willingness to share biographic information and identifiers with online travel providers. This indicates that when travelers perceive interacting with an online travel provider as risky, they are less likely to share biographical and identifying information (e.g., financial and passport data). However, there is no impact of risk beliefs on travelers' willingness to share behavioral data (H5d). It can be suggested that travelers are very protective of basic personal information, such as name, email address, financial, and passport information, when they perceive the sharing of information is risky. According to GDPR (2020), biographic information and identifiers alone can be considered identifiable information, while behavioral data alone (when decoupled with identifiers) cannot. It can be suggested that travelers might perceive the sharing of behavioral data to be of less significant weight in disclosure decision involving risky interactions with travel providers. Also, the hypothesized negative relationship between risk and willingness to share biometric information was not supported. Considering biometric information had the lowest level of disclosure intention (*Mean*=1.680, *St. Dev*=1.060), an explanation for this result lies in the overall novelty of biometric data sharing practice, which may cause consumers to reject the sharing of biometric data as a form of heuristic decision making (e.g., relying more on emotions rather than reasoning). Although biometric authentication is currently gaining momentum (e.g., using Face ID to unlock the latest generation iPhone), its implementation in travel is still in its early stages. Another possible reason is that travelers associate the disclosure of biometric information more with the physical environments (e.g., at airports), rather than the online platforms (e.g., on airline's mobile apps). Travelers might not fully comprehend the risk associated with sharing this type of information online. To better explain the link between perceived risk and willingness to share biometric information, participants in lowest perceived risk group (*N*=342) were compared with those in highest perceived risk group (*N*=343) (i.e., highest/lowest quartiles based on the median value). However, the mean difference of willingness to share biometric data between these groups is not statistically significant (low group: *Mean*=1.652, *St. Dev*=1.041; high group: *Mean*=1.724, *St. Dev*=1.086). Consequently, further research is necessary to investigate in more depth the impact of various antecedents on the intention to disclose biometric information in online travel environments.

In order to assess whether travelers' willingness to share personal information varies across demographic characteristics, gender, age, and education were incorporated as control variables. Results show that gender has a significant effect on willingness to share all four types of information, demonstrating that male travelers tend to have higher intention to share personal information with online travel companies. Further, age has been shown to significantly influence willingness to share personal data, except for biographic information. The older the travelers, the less likely they are to disclose identifiers, biometric, and behavioral data. Finally, education levels have a significant effect on willingness to share biometric information, with highly educated travelers less willing to disclose. This might be due to highly educated travelers being better informed about the nature of biometric data sharing and/or the risk associated with it. Further research incorporating these variables in a moderating or mediating role within the relationships in the model is encouraged to further explicate the roles of personal characteristics in disclosure behavior among travelers.

Conclusion and Implications

Information privacy has been one of the most central topics of interest among researchers in various disciplines as well as amongst users and industry practitioners (Smith et al. 2011). The implications of travel companies collecting and sharing vast amounts of data with numerous business partners have manifested in increasing users' privacy concerns, with consumers demonstrating less trust in providers and very often opting out of data sharing for personalized services (Kim et al. 2018). Although privacy has been widely investigated and various instruments have been developed to measure privacy concerns, most privacy studies have focused on privacy in generic online environments, failing to recognize contexts of use that encompass new aspects of privacy. This study addresses the gap by investigating privacy concerns in online travel environments. By doing so, this study makes important theoretical contributions in two areas: identifying and measuring privacy concerns in the travel context and providing empirical support to explicate the relationships between travelers' online privacy concerns, trust, risk, and willingness to share personal information with travel service providers online.

First, this study contributes to existing literature by enhancing current understanding of online privacy concerns of travelers. This is among the very few studies to investigate privacy of travel consumers in the context of online environments by developing a context specific measurement scale called 'Travelers' Online Privacy Concerns' (TOPC). This research provides empirical evidence to present TOPC as a valid and appropriate instrument quantifying the key dimensions of travelers' privacy concerns: self-privacy concerns and normative privacy concerns. Therefore, both researchers and practitioners can deploy the scale in future studies to capture privacy concerns of consumers within online travel environments. With respect to the broader privacy literature, the study findings suggest that a context specific instrument of privacy is able to explain, relate, and reflect better privacy concerns of consumers that are using a wide range of technologies for travel.

Secondly, as privacy is highly context dependent (Acquisti, Brandimarte, and Loewenstein 2015), this study contextualizes privacy in travel by investigating the effects of privacy concerns on trust, risk, and willingness to share four distinct types of personal information relevant to travel and tourism: biometric information, identifiers, biographic information, and behavioral data. While biographic information and identifiers have been widely investigated in previous privacy studies, the inclusion of biometric information and behavioral data in this study constitutes an important contribution. Biometric information and behavioral data reflect important aspects of information sharing that are significant to travel but have not been thoroughly investigated in previous research.

As hypothesized, travelers' privacy concerns have significant effects on trust and risk, except for the relationship between normative privacy concerns and perceived risk (H2b), which showed significant effect with the opposite direction. As previously explained, the normative privacy concerns constitute people's beliefs in what companies *should* or *ought to* do to protect the privacy and personal data of travelers. Hence, this may represent people's beliefs in the 'existence of the norm' within the travel industry, thus helps decrease the perception of risk of sharing personal data with online travel providers. A further investigation to explicate this relationship is suggested for future research.

Further, our findings suggest that the online travel context encompasses distinct complexities when it comes to data privacy. These are derived from the amount as well as the range of types of data being requested simultaneously (e.g., activity and fingerprint, facial image and demographics) while past research has mostly focused on specific data type requests rather than a bundle. Regarding the disclosure of basic information such as biographic and identifiers, travelers seem to report similar privacy behaviors with previously studied generic populations. For example, similar behaviors were observed amongst undergraduate students in the US when disclosing basic membership sign up information (i.e., name, gender, e-mail address, phone) to a commercial website (H. Li, Sarathy, and Xu 2010) as well as household respondents sharing financial information with an online discount store (Malhotra, Kim, and Agarwal 2004). In these studies, respondents were less willing to share such information when they believed releasing the information to a provider constitutes high risk.

This study did not find a significant effect of perceived risk on disclosure intention of behavioral information, while perceived risk was found to positively affect disclosure intention of biometric information. In terms of behavioral data, Xu et al. (2009) found that mobile phone users are less willing to disclose their location information to LBS service providers when feeling that their personal information is not effectively protected. While their study focused only on location data, behavioral data in this study encompasses other types of data (i.e., expenses during travel, activity sensor data, smartphone search history, real time position, personal preferences, hobbies), which may prompt different reactions. In their study with academics in the US, Halevi et al. (2015) argue that users who perceive high risk during an online interaction are less willing to share their fingerprint data with commercial websites. Investigating consumers' intention to disclose their facial image to facial recognition systems (FRS) in hotels, Morosan (2019) found that disclosure intention is impeded by privacy concerns, although these concerns have a low impact as they are overridden by the value of disclosure. The positive relationship between perceived risk and disclosure intention of biometric information found in this study may be due to the context (i.e., travel vs. general commerce [Halevi et al., 2015]; online vs. on-site/hotels [Morosan, 2019]) or an indication of different attitudes toward, and thus the perception of risk of, each of the aggregated types of information (i.e., fingerprint, voice sample, face scan, iris/retina pattern), as previous studies only focused on one type (i.e., fingerprint [Halevi et al., 2015] and facial image [Morosan, 2019]). Finally, these unexpected results may be due to the measurements of perceived risk (generic: personal data) and willingness to share (specific: biometric or behavioral) used in this study, in that attitudes toward personal data in general do not translate the same way to specific personal information.

In practice, this study offers an enhanced understanding of travelers' privacy decision making process in order to inform better decisions and operations of travel companies. The availability of travelers' (personal) information enables travel companies to know their customers better, allowing them to operate more efficiently by providing services in the most effective way. For example, using behavioral data such travelers' personal preferences, a travel company can offer unique customer experiences that better serve travelers' needs. This, in turn, will improve customer satisfaction, improve loyalty, and increase revenues. Therefore, the findings of this study can enhance comprehension of user privacy concerns in order to increase consumer confidence in sharing their personal information. They will also understand privacy preferences of certain customer segments, such as older adults and younger generations, more educated individuals, and female consumers. By understanding the characteristics of their customers, companies will be able to offer more tailored, personalized privacy solutions, with engaging and relevant content while also a variety of privacy preferences options. These practical implications are relevant not only to travel and tourism firms but also in a wider range of industries, such as marketing, finance, and general e-commerce (e.g., retail) that are targeting travelers in online environments.

This study links privacy concerns with personal information disclosure through trust and risk, which should further inform online travel companies and organizations with impending issues due to increased privacy concerns. As aforementioned, the collection and use of travelers' personal data have intensified with the introduction of advanced technologies such as AI, sensors, and recognition technologies, and recent events highlighting privacy breaches by firms and government initiatives regarding the collection of personal data have captured the public's attention. Consequently, there has been an increase in users' privacy concerns over the collection and handling of personal information as well as their consciousness of privacy (Micallef and Misra 2018). The results in this study reinforce the notion that increased concerns over privacy can significantly impact information disclosure, thus travel providers relying on consumers' willingness to share their data will be facing immense difficulties. Specifically, trust has been proven in this study to positively influence disclosure intention of all types of travelers' personal data. Hence, to mitigate this issue, travel providers should focus on trust-building and risk-mitigating strategies and activities, including the communication of privacy policies in a clear and transparent way on their website, while also adopting privacy protection mechanisms (e.g. privacy enhancing technologies [PETS]) and relevant regulatory frameworks in collaboration with other businesses and governmental entities to ultimately reduce privacy concerns.

As with all empirical studies, this study has limitations. The first stage of this study involved multiple steps with respondents from two different countries (UK and US) in an attempt to establish the validity and reliability of the TOPC instrument. Then, a UK-based sample was used for the examination of TOPC's impact on trust, risk, and disclosure behavioral intention.

Users perceptions of privacy concerns, trust, and risk might differ between countries and cultures. Thus, future studies should consider more diverse cross-cultural samples, such as a wider range of countries and people from diverse populations in order to replicate this study and generalize the results. Moreover, this study recruited participants from a wide range of ages and educational backgrounds, aiming to achieve a representation of generic travelers using online platforms. Future research should consider recruiting more specific groups with different travel preferences, such as youth or senior travelers, as well as specific travel segments who might have distinct privacy concerns with additional aspects that were not considered in this study. Also, this study used self-reported measures in order to capture travelers' online privacy concerns; individuals might sometimes misreport behaviors due to cognitive constraints or desire for self-justification. As a result, inferences to causality should be made with caution and further research is essential to validate the results using potentially different measures for privacy concerns (i.e., observations and experiments). This study measured privacy concerns, trust, and risk in terms of general personal data while willingness to disclose information was measured for specific information. Future studies should attempt to test the model in specific information contexts, i.e., measuring perceived risk of specific types of personal information and its effect on specific disclosure behavior. Finally, this study used age, gender and education as control variables in the SEM model to capture their impact on information disclosure. Future research should examine the impact of additional variables such as experience with online travel providers or frequency of use of online travel websites on information disclosure.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015) ‘Privacy and human behavior in the age of information’, Science, pp. 509–514.

Agag, Gomaa M., and Ahmed A. El-Masry. 2017. “Why Do Consumers Trust Online Travel Websites? Drivers and Outcomes of Consumer Trust toward Online Travel Websites.” *Journal of Travel Research* 56 (3): 347–69. doi:10.1177/0047287516643185.

Alba, D. 2019. “The US Government Will Use Facial Recognition In Top Airports.” Buzzfeed News. https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.

Anuar, Faiz I., and Ulrike Gretzel. 2011. “Privacy Concerns in the Context of Location-Based Services for Tourism.” In *ENTER 2011, Innsbruck (Austria), January 26-28*.

Ardito, Lorenzo, Roberto Cerchione, Pasquale Del Vecchio, and Elisabetta Raguseo. 2019. “Big Data in Smart Tourism: Challenges, Issues and Opportunities.” *Current Issues in Tourism* 22 (15). Taylor & Francis: 1805–9. doi:10.1080/13683500.2019.1612860.

Bélanger, France, and Robert E Crossler. 2011. “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.” *MIS Quarterly* 35 (4): 1017–41. doi:10.1159/000360196.

Belanger, France, Janine S Hiller, and Wanda J Smith. 2002. “Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes.” *Journal of Strategic Information Systems* 11: 245–70. doi:10.1016/S0963-8687(02)00018-5.

Benamati, John H., Zafer D. Ozdemir, and H. Jeff Smith. 2017. “An Empirical Test of an Antecedents - Privacy Concerns - Outcomes Model.” *Journal of Information Science* 43 (5): 583–600. doi:10.1177/0165551516653590.

Bennett, C. 1995. “Bennett, C. J. 1995. The Political Economy of Privacy: A Review of the Literature.” In *Hackensack, NJ: Center for Social and Legal Research*.

Bonsón Ponte, Enrique, Elena Carvajal-Trujillo, and Tomás Escobar-Rodríguez. 2015. “Influence of Trust and Perceived Value on the Intention to Purchase Travel Online: Integrating the Effects of Assurance on Trust Antecedents.” *Tourism Management*. doi:10.1016/j.tourman.2014.10.009.

Buchanan, T, C Paine, A Joinson, and Ulf Dietrich Reips. 2007. “Development of Measures of Online Privacy Concern and Protection for Use on the Internet.” *Journal Of The American Society For Information Science and Technology* 58 (2): 157–65. doi:10.1002/asi.

Carpenter, Serena. 2018. “Ten Steps in Scale Development and Reporting: A Guide for Researchers.” Communication Methods and Measures 12 (1). Routledge: 25–44. doi:10.1080/19312458.2017.1396583.

Chellapa, R., and R.G. Sin. 2005. “Personalisation vs. Privacy: An Empirical Examination of the Online Consumers’ Dilemma.” *Information Technology and Management* 6 (2–3): 181–202.

Copeland, R. 2019. “Google’s ‘Project Nightingale’ Gathers Personal Health Data on Millions of Americans - WSJ.” *WSJ*. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

DeVellis, R. 2016. *Scale Development Theory and Applications*. SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/scale-development/book246123.

Femenia-Serra, Francisco, José F. Perles-Ribes, and Josep A. Ivars-Baidal. 2018. “Smart Destinations and Tech-Savvy Millennial Tourists: Hype versus Reality.” *Tourism Review*. doi:10.1108/TR-02-2018-0018.

“General Data Protection Regulation (GDPR).” 2020. Accessed January 15. https://gdpr-info.eu/issues/personal-data/.

George, Darren., and Paul. Mallery. 2003. *SPSS for Windows Step by Step : A Simple Guide and Reference*. Allyn and Bacon.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. “Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior.” *Computers and Security*. doi:10.1016/j.cose.2018.04.002.

Hair, Joseph F., William Black, Barry Babin, Rolph Anderson, and Ronald Tatham. 2010. Multivariate Data Analysis. 6th ed. Pearson Prentice Hall

Hair, Joseph F., Jeffrey J. Risher, Marko Sarstedt, and Christian M. Ringle. 2019. “When to Use and How to Report the Results of PLS-SEM.” *European Business Review* 31 (1). Emerald Publishing Limited: 2–24. doi:10.1108/EBR-11-2018-0203.

Halevi, Tzipora, Trishank Karthik Kuppusamy, Meghan Caiazzo, and Nasir Memon. 2015. “Investigating Users’ Readiness to Trade-off Biometric Fingerprint Data.” In *2015 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2015*. doi:10.1109/ISBA.2015.7126366.

Hardesty, David M., and William O. Bearden. 2004. “The Use of Expert Judges in Scale Development. Implications for Improving Face Validity of Measures of Unobservable Constructs.” *Journal of Business Research* 57 (2): 98–107. doi:10.1016/S0148-2963(01)00295-8.

Hew, Jun Jie, Garry Wei Han Tan, Binshan Lin, and Keng Boon Ooi. 2017. “Generating Travel-Related Contents through Mobile Social Tourism: Does Privacy Paradox Persist?” *Telematics and Informatics* 34 (7). Elsevier Ltd: 914–35. doi:10.1016/j.tele.2017.04.001.

Hinson, T. 2019. “Ocean Medallion: Fun Gimmick or Invasion of Privacy? The New Device That Means Cruise Lines Can Track Their Passengers.” *Telegraph*. https://www.telegraph.co.uk/travel/cruises/articles/testing-princess-cruises-ocean-medallion/.

Huang, C. Derrick, Jahyun Goo, Kichan Nam, and Chul Woo Yoo. 2017. “Smart Tourism Technologies in Travel Planning: The Role of Exploration and Exploitation.” *Information and Management* 54 (6). Elsevier B.V.: 757–70. doi:10.1016/j.im.2016.11.010.

Karwatzki, Sabrina, Olga Dytynko, Manuel Trenz, and Daniel Veit. 2017. “Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization.” *Journal of Management Information Systems* 34 (2). Routledge: 369–400. doi:10.1080/07421222.2017.1334467.

Keith, Mark J., Samuel C. Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. “Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior.” *International Journal of Human Computer Studies* 71 (12). Elsevier: 1163–73. doi:10.1016/j.ijhcs.2013.08.016.

Kim, Min Sung, and Seongcheol Kim. 2018. “Factors Influencing Willingness to Provide Personal Information for Personalized Recommendations.” *Computers in Human Behavior* 88 (December 2017). Elsevier: 143–52. doi:10.1016/j.chb.2018.06.031.

Kokolakis, Spyros. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers and Security* 64. Elsevier Ltd: 122–34. doi:10.1016/j.cose.2015.07.002.

Lee, Chung Hun, and David A. Cranage. 2011. “Personalisation-Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites.” *Tourism Management*. doi:10.1016/j.tourman.2010.08.011.

Li, Yuan. 2011. “Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework.” *Communications of the Association for Information Systems* 28 (28): 453–96. doi:http://aisel.aisnet.org/cais/vol28/iss1/28.

Li, Y. (2014) ‘The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns’, Decision Support Systems. Elsevier B.V., 57(1), pp. 343–354. doi: 10.1016/j.dss.2013.09.018.

Mackenzie, Scott B, Philip M Podsakoff, and Nathan P Podsakoff. 2011. “Construct Measurement and Validation Procedures in MIS and Behavioral Research : Integrating New and Existing Techniques.” *MIS Quarterly* 35 (2): 293–334. doi:10.2307/23044045.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Casual Model.” *Information Systems Research* 15 (4): 336–55. doi:10.1287/isre.l040.0032.

Mcknight, D Harrison, Larry L Cummings, and Norman L Chervany. 1998. “Initial Trust Formation In New Organizational Relationships.” *Academy of Management. The Academy of Management Review* 23 (3): 473–90.

Micallef, Nicholas, and G Misra. 2018. “Towards Designing a Mobile App That Creates Avatars for Privacy Protection." In *MobileHCI '18 Adjunct, September 3–6, 2018,* 79–86.

Morosan, Cristian. 2018. "Information Disclosure to Biometric E-Gates: The Roles of Perceived Security, Benefits, and Emotions." *Journal of Travel Research* 57 (5): 644–57. doi:10.1177/0047287517711256.

Morosan, C. (2019) 'Disclosing facial images to create a consumer's profile', International Journal of Contemporary Hospitality Management, ahead-of-p(ahead-of-print), pp. 3149–3172. doi: 10.1108/ijchm-08-2018-0701.

Mudrack, P. 2007. "Individual Personality Factors That Affect Normative Beliefs About the Rightness of Corporate Social Responsibility." *Business & Society* 46 (1): 33–62. https://curriculum.gov.bc.ca/competencies/social-responsibility.

Ozdemir, Zafer D., H. Jeff Smith, and John H. Benamati. 2017. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study." *European Journal of Information Systems* 26 (6). Palgrave Macmillan UK: 642–60. doi:10.1057/s41303-017-0056-z.

Ozturk, Ahmet Bulent, Khaldoon Nusair, Fevzi Okumus, and Dipendra Singh. 2017. "Understanding Mobile Hotel Booking Loyalty: An Integration of Privacy Calculus Theory and Trust-Risk Framework." *Information Systems Frontiers* 19 (4). Information Systems Frontiers: 753–67. doi:10.1007/s10796-017-9736-4.

Pavlou, Paul, H Liang, and Y Xue. 2007. "Understanding And Mitigating Uncertainty In Onine Exchange Relationships: A Principal Agent Perspective." *MIS Quarterly* 31 (1): 105–36.

Podsakoff, Philip M., Scott B. MacKenzie, Jeong Yeon Lee, and Nathan P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879–903. doi:10.1037/0021-9010.88.5.879.

Preibusch, Sören. 2013. "Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments." *International Journal of Human Computer Studies* 71 (12). Elsevier: 1133–43. doi:10.1016/j.ijhcs.2013.09.002.

Sigala, Marianna. 2018. "New Technologies in Tourism: From Multi-Disciplinary to Anti-Disciplinary Advances and Trajectories." *Tourism Management Perspectives* 25 (December 2017). Elsevier: 151–55. doi:10.1016/j.tmp.2017.12.003.

Smith, H. Jeff, Tamara Dinev, and Heng Xu. 2011. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4): 1063–78. doi:10.2307/41409970.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* 20 (2): 167. doi:10.2307/249477.

Sorrells, M. (2019) ‘Could digital ID be the key to achieving a frictionless travel experience?’, *PhocusWire*. Available at: https://www.phocuswire.com/GBTA-convention-digital-identity-frictionless-travel (Accessed: 2 June 2020).

Stewart, Kathy A, and Albert H Segars. 2002. “An Empirical Examination of the Concern for Information Privacy Instrument.” *Information Systems Research* 13 (1): 36–49. doi:DOI 10.1287/isre.13.1.36.97.

Street, Francesca. 2019. "How facial recognition is taking over airports." CNN. https://edition.cnn.com/travel/article/airports-facial-recognition/index.html

Taddicken, Monika Michaela Martina. 2010. “Measuring Online Privacy Concern and Protection in the (Social) Web: Development of the APCP and APCP-18 Scale.” In *International Communication Association, Suntec Singapore International Convention & Exhibition Centre, Suntec City, Singapore, Jun 22, 2010*.

Tussyadiah, Iis, Shujun Li, and Graham Miller. 2019. “Privacy Protection in Tourism: Where We Are and Where We Should Be Heading For.” In *Pesonen J., Neidhardt J. (Eds) Information and Communication Technologies in Tourism 2019*, 278–90. doi:10.1007/978-3-7091-1142-0.

Vinod, Ben. 2016. “Big Data in the Travel Marketplace.” In *Journal of Revenue and Pricing Management*, 15:352–59. Palgrave Macmillan Ltd. doi:10.1057/rpm.2016.30.

Vu, Huy Quan, Rob Law, and Gang Li. 2018. “Breach of Traveller Privacy in Location-Based Social Media.” *Current Issues in Tourism* 0 (0). Taylor & Francis: 1–16. doi:10.1080/13683500.2018.1553151.

Warren, Samuel D, and Louis D Brandeis. 1890. “The Right to Privacy.” *Law Review* 4 (5): 193–220.

WEF. (2018). The Known Traveller Unlocking the potential of digital identity for secure and seamless travel. Retrieved from http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

Westin, Alan F. 1967. *Privacy And Freedom*. New York: Atheneum. doi:https://doi.org/10.1177/000271626837700157.

World Tourism Organization (2019), International Tourism Highlights, 2019 Edition, UNWTO, Madrid. DOI: https://doi.org/10.18111/9789284421152

Worthington, Roger L., and Tiffany A. Whittaker. 2006. “Scale Development Research: A Content Analysis and Recommendations for Best Practices.” *The Counseling Psychologist* 34 (6): 806–38. doi:10.1177/0011000006288127.

Wozniak, T., Schaffner, D., Stanoevska-Slabeva, K. and Lenz-Kesekamp, V. (2018) ‘Psychological antecedents of mobile consumer behaviour and implications for customer journeys in tourism’, Information Technology and Tourism. Springer Berlin Heidelberg, 18(1–4), pp. 85–112. doi: 10.1007/s40558-017-0101-8.

Xiang, Z., D. Wang, J.T. O'Leary, and D.R. Fesenmaier. 2015. "Adapting to the Internet: Trends in Travelers' Use of the Web for Trip Planning." *Journal of Travel Research* 54 (4): 511–27. doi:10.1177/0047287514522883.

Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View." *International Conference on Information Systems (ICIS)*, no. October: 1–16. doi:citeulike-article-id:5770148.

Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. "Information Privacy Concerns : Linking Individual Perceptions with Institutional Privacy Assurances." *Journal of the Association for Information Systems* 12 (12): 798–824.

Table 1. Exploratory Factor Analysis (EFA) refinement steps

Step	**Item deleted**	**Reason for deletion**	**Number of remaining factors**
1	Q11_2	poor loading < 0.5	4
2	Q5_3	high cross loadings > 0.3	3
3	Q5_7	high cross loadings > 0.3	3
4	Q5_5	poor loading < 0.5	2
5	Q5_6	poor loading < 0.5	2

Table 2. Exploratory Factor Analysis (EFA) results

	Item	**Factor 1**	**Factor 2**
SPC_1	I am concerned that the information I submit to online travel companies could be misused.	0.850	
SPC_2	I am concerned that others can find private information about me from online travel companies.	0.883	
SPC_3	I am concerned about providing personal information to online travel companies, because it could be used in a way I did not foresee.	0.894	
SPC_4	I don't feel comfortable when I do not have control over personal data I disclose to online travel companies.	0.782	
SPC_5	I don't feel comfortable when I do not have control or autonomy over decisions about how my personal information is collected, used, and possibly shared by online travel companies.	0.731	
SPC_6	It usually bothers me when online travel companies ask me for personal information.	0.864	
SPC_7	When online travel companies ask me for personal information, I sometimes think twice before providing it.	0.771	
SPC_8	It bothers me to give personal information to so many online travel companies.	0.829	
SPC_9	I'm concerned that online companies are collecting too much information about me.	0.706	
SPC_10	I don't feel comfortable to share information about my current location with online travel companies.	0.652	
SPC_11	I am concerned with the security of sensitive information when I use online travel companies.	0.716	
NPC_1	When people give personal information to an online travel company for some reason, the online company should never use the information for any other reason.		0.835
NPC_2	Online travel companies should never sell the personal information in their computer databases to companies.		0.816
NPC_3	Online travel companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.		0.861
NPC_4	Online travel companies should devote more time and effort to preventing unauthorized access to personal information.		0.607
NPC_5	Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.		0.825
NPC_6	Online travel companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.		0.795

Table 3. Types of personal information

Item	**Factor 1 Biometric Information**	**Factor 2 Identifiers**	**Factor 3 Biographic Information**	**Factor 4 Behavioral Data**
Iris/retina pattern	0.981			
Face scan/image	0.889			
Voice sample	0.853			
Fingerprint	0.644			
Credit card information		0.938		
Bank account information		0.928		
Passport number		0.681		
Driver license number		0.564		
Name			0.814	
Date of birth			0.753	
Home address			0.730	
Email address			0.696	
Phone number			0.576	
Specific expenses during travel				0.853
Activity sensor data				0.689
Smartphone search history				0.662
Real time position				0.615
Personal preferences				0.589
Hobbies				0.528

Table 4. Psychometric properties of the variables

	Cronbach's Alpha	CR	AVE	Mean	Std. Dev
Self-privacy concerns	0.949	0.950	0.633	3.310	0.800
Normative privacy concerns	0.887	0.886	0.569	2.390	0.930
Trust	0.933	0.935	0.783	3.520	0.810
Risk	0.923	0.922	0.665	2.860	0.820
WTS biometric information	0.973	0.973	0.902	1.680	1.060
WTS identifiers	0.829	0.832	0.554	2.420	1.070
WTS biographic information	0.902	0.902	0.650	3.300	0.920
WTS behavioral data	0.876	0.876	0.589	2.400	0.930

Note: WTS = willingness to share; CR = composite reliability; AVE = average variance extracted

Table 5. Fornell-Larcker Criterion (correlation coefficients)

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
(1) Self-privacy concerns	**0.754**							
(2) Normative privacy concerns	0.238	**0.754**						
(3) Trust	-0.448	-0.161	**0.885**					
(4) Risk	0.654	-0.055	-0.360	**0.806**				
(5) WTS biometric information	-0.070	-0.284	0.158	0.052	**0.950**			
(6) WTS identifiers	-0.358	-0.165	0.237	-0.249	0.449	**0.744**		
(7) WTS biographic information	-0.417	0.047	0.260	-0.361	0.177	0.654	**0.806**	
(8) WTS behavioral data	-0.099	-0.346	0.200	0.011	0.731	0.386	0.185	**0.767**

Note: Square roots of average variance extracted (AVE) in the diagonal; WTS = willingness to share

Table 6. Results of hypothesis testing

Hypothesis	**b**	**p**	**Result**
H1a: Self-privacy concerns → Trust	-0.409	***	Supported
H1b: Normative privacy concerns → Trust	-0.104	0.041	Supported
H2a: Self-privacy concerns → Risk	0.588	***	Supported
H2b: Normative privacy concerns → Risk	-0.252	***	Not Supported
H3: Trust → Risk	-0.078	0.014	Supported
H4a: Trust → Willingness to share biometric information	0.317	***	Supported
H4b: Trust → Willingness to share identifiers	0.257	***	Supported
H4c: Trust → Willingness to share biographic information	0.215	***	Supported
H4d: Trust → Willingness to share behavioral data	0.317	***	Supported
H5a: Risk → Willingness to share biometric information	0.186	0.009	Not Supported
H5b: Risk → Willingness to share identifiers	-0.371	***	Supported
H5c: Risk → Willingness to share biographic information	-0.395	***	Supported
H5d: Risk → Willingness to share behavioral data	0.121	0.069	Not Supported

Note: *** significant at *p*<.001

Table 7. The effects of demographic variables on willingness to share personal information

	b	p	Results
Gender → Willingness to share biometric information	-0.191	0.018	Significant
Gender → Willingness to share identifiers	-0.312	***	Significant
Gender → Willingness to share biographic information	-0.140	0.024	Significant
Gender → Willingness to share behavioral data	-0.185	0.012	Significant
Age → Willingness to share biometric information	-0.053	0.042	Significant
Age → Willingness to share identifiers	-0.093	***	Significant
Age → Willingness to share biographic information	0.014	0.478	Not Significant
Age → Willingness to share behavioral data	-0.047	0.049	Significant
Education → Willingness to share biometric information	-0.074	0.034	Significant
Education → Willingness to share identifiers	0.070	0.061	Not Significant
Education → Willingness to share biographic information	0.008	0.756	Not Significant
Education → Willingness to share behavioral data	-0.019	0.544	Not Significant

Note: *** significant at $p<.001$

Table 8. R_2 values of endogenous variables in the structural model

	R_2
Willingness to share biometric information	0.044
Willingness to share identifiers	0.092
Willingness to share biographic information	0.149
Willingness to share behavioral data	0.054

Figure 1. Two-factor first order model of TOPC

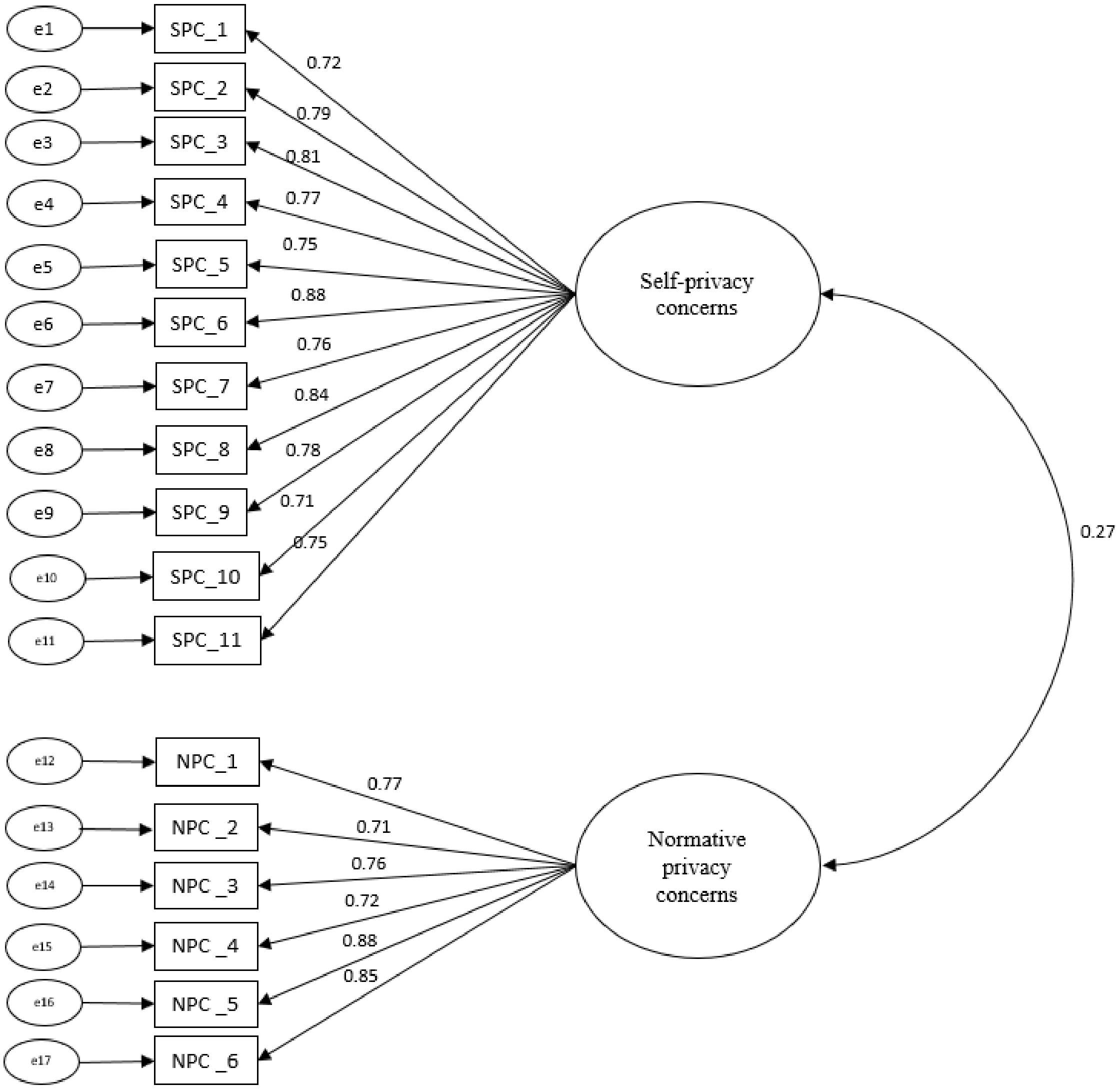
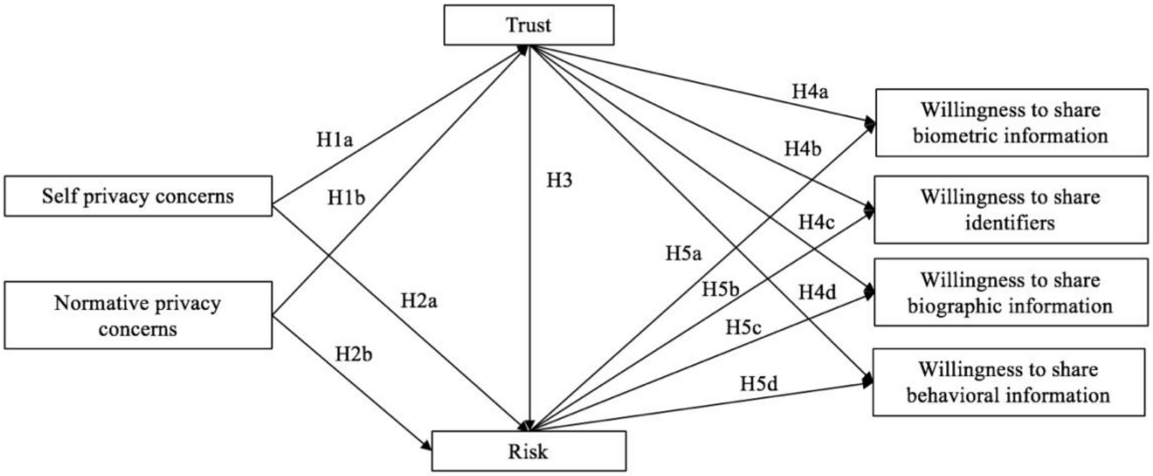


Figure 2. The proposed model of travelers' privacy decision


Trust
Self privacy concerns
Normative privacy concerns
Risk
Willingness to share biometric information
Willingness to share identifiers
Willingness to share biographic information
Willingness to share behavioral information
H1a
H1b
H2a
H2b
H3
H4a
H4b
H4c
H4d
H5a
H5b
H5c
H5d

Appendix A

Table A1. Demographic characteristics of participants in Stage 1 and Stage 2 studies

Characteristics	**Items**	**Stage 1: Pilot** (*N* = 277) Percent (%)	**Stage 1: Cross-validation** (*N* = 287) Percent (%)	**Stage 2** (*N* = 685) Percent (%)
Gender	Male	46.6	57.1	47.2
	Female	53.4	42.9	52.4
	Other	-	-	0.4
Age	18-25	4.0	13.6	4.8
	26-35	20.2	51.6	23.9
	36-45	23.5	20.9	12.3
	46-55	17.7	10.8	17.2
	56-65	19.5	2.8	22.2
	>65	15.2	0.3	19.6
Education	Less than high school	-	-	2.9
	High School	48.4	20.6	38.8
	Bachelor	28.2	64.5	34.5
	Master	15.9	12.5	14.3
	Doctoral	2.9	1.0	3.9
	Other	4.0	1.4	5.5

Table A2. Results from exploratory factor analysis in Stage 1 and Stage 2 Studies

	Stage 1: Cross-validation	**Stage 2**
Bartlett's test of sphericity	χ_2=4006.126 p<0.001	χ_2=9965.325 p<0.001
Kaiser-Meyer-Olkin (KMO)	0.912	0.900
% Variance		
Factor 1	43.500	34.300
Factor 2	20.700	21.800
Factor 3		6.600
Factor 4		4.400

Appendix B. Measurement Items

Trust (Benamati, Ozdemir, & Smith, 2017)

"When it comes to sharing my personal information such as name, email address, purchase history online and knowing it will be protected...

TRUST1 – ... *I feel comfortable with online travel companies."*

TRUST2 – ... *I can rely on online travel companies."*

TRUST3 – ... *I can count on online travel companies."*

TRUST4 – ... *I can depend on online travel companies."*

Privacy Risk (Keith, Thompson, Hale, Lowry, & Greer, 2013)

RISK1 – *"Providing online travel companies with my personal information would involve many unexpected problems."*

RISK2 – *"It would be risky to disclose my personal information to online travel firms."*

RISK3 – *"There would be high potential for loss in disclosing my personal information to online travel companies."*

RISK4 – *"Providing online travel companies with my location data would involve many unexpected problems."*

RISK5 – *"It would be risky to disclose my location data to online travel firms."*

RISK6 – *"There would be high potential for loss in disclosing my location data to online travel companies."*

Travelers' Online Privacy Concerns (TOPC) (Smith, Milberg, & Burke, 1996; Xu, Dinev, Smith, & Hart, 2011;Wozniak, Schaffner, Stanoevska-Slabeva, & Lenz-Kesekamp, 2018)

Self-Privacy Concerns

SPC1 – “*I am concerned that the information I submit to online travel companies could be misused.”*

SPC2 – “*I am concerned that others can find private information about me from online travel companies.”*

SPC3 – “*I am concerned about providing personal information to online travel companies, because it could be used in a way I did not foresee.”*

SPC4 – “*I don’t feel* comfortable when I do not have control over personal data I disclose to *online travel companies.”*

SPC5 – “*I don’t feel comfortable when I do not have control or autonomy over decisions about how my personal information is collected, used, and possibly shared by online travel companies.”*

SPC6 – “*It usually bothers me when online travel companies ask me for personal information.”*

SPC7 – “*When online travel companies ask me for personal information, I sometimes think twice before providing it.”*

SPC8 – “*It bothers me to give personal information to so many online travel companies.”*

SPC9 – “*I'm concerned that online travel companies are collecting too much information about me.”*

SPC10 – “*I don’t feel comfortable to share information about my current location with online travel companies.”*

SPC11 – “*I am concerned with the security of sensitive information when I use online travel companies.”*

Normative Concerns

NPC1 – "*When people give personal information to an online travel company for some reason, the online company should never use the information for any other reason.*"

NPC2 – "*Online travel companies should never sell the personal information in their computer databases to companies.*"

NPC3 – "*Online travel companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.*"

NPC4 – "*Online travel companies should devote more time and effort to preventing unauthorized access to personal information.*"

NPC5 – "*Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.*"

NPC6 – "*Online travel companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.*"

Willingness to Share Personal Information *(*self-developed)

"How willing are you to share the following information with online travel companies?"

WTS1 – Name
WTS2 – Date of birth
WTS3 – Home address
WTS4 – Email address
WTS5 – Phone number
WTS6 – Profession
WTS7 – Education
WTS8 – Credit card information
WTS9 – Bank account information
WTS10 – Contacts in address book

WTS11 – Passport number
WTS12 – Driver license number
WTS13 – Fingerprint
WTS14 – Voice sample
WTS15 – Face scan/image
WTS16 – Iris/retina pattern
WTS17 – Social media profile data
WTS18 – Hobbies/personal interests
WTS19 – Personal preferences (room selection in a hotel, dietary requirements)
WTS20 – Real time position
WTS21 – Smartphone search history (cookies)
WTS22 – Activity sensor data (body movements, number of steps, floors etc)
WTS23 – Specific expenses in places travelled and services purchased