Privacy Concerns and Disclosure of Biometric and Behavioral Data for Travel[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

Yang Lu
School of Computing & Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)
University of Kent, United Kingdom
Email: y.lu@kent.ac.uk

Accepted for publication in
International Journal of Information Management
26th March 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., Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. International Journal of Information Management.

Privacy Concerns and Disclosure of Biometric and Behavioral Data for Travel

Abstract

In light of mounting privacy concerns over the increasing collection and use of biometric and behavioral information for travel facilitation, this study examines travelers' online privacy concerns (TOPC) and its impact on willingness to share data with travel providers. A proposed theoretical model explaining antecedents and outcomes of TOPC related to biometric and behavioral data sharing was tested using structural equation modeling with data collected from 685 travelers. The results extend the Antecedents – Privacy Concerns – Outcomes (APCO) framework by identifying a set of salient individual factors that shape TOPC. The findings provide empirical evidence confirming the context dependence of privacy preferences, showing that although travelers are concerned over their information privacy they are still willing to share their behavioral data; while in the case of biometric information, the disclosure decision is dependent upon expected benefits rather than privacy concerns. This study offers insights into privacy behavior of online consumers in the travel context and constitutes one of the few focusing on the social aspects of biometric authentication.

Keywords: privacy concerns, travel, willingness to share, information disclosure, biometrics, behavioral

1. Introduction

Technological advances such as machine learning and artificial intelligence, big data, internet of things, smart devices, robots, sensors, and virtual and augmented reality have introduced radical disruptions in the travel and tourism industry, changing both business operations and consumer behaviors (Femenia-Serra & Neuhofer, 2018; Sigala, 2018). Since the interactions between travelers and travel providers are often mediated by the use of technologies (e.g., online booking before trip, mobile payment during trip, online review after trip) (Sigala, 2018; Wozniak, Schaffner, Stanoevska-Slabeva, & Lenz-Kesekamp, 2018), businesses focusing on offering unique personalized travel experiences are highly dependent on the collection of consumers' personal information. The widespread adoption of multiple interconnected devices such as smartphones, laptops, tablets, and wearable devices that are sensor rich and computationally powerful allows a ubiquitous data gathering (Harari et al., 2016), including capturing non-transactional behavioral data, such as location, personal preferences, lifestyle, and personality characteristics. Using the combination of these data, service providers such as hotels, airlines, and travel agents are able to create more detailed and targeted customer profiles or 'digital identities' (Mathews-Hunt, 2016), allowing them to expand their customer base through customized

advertising, tailored travel services, and personalized recommendations (Themistocleous, Smith, & Wagner, 2014).

Moreover, as indicated by various global initiatives on universal digital identification, automated border control, and other related programs (WEF, 2018; WTTC, 2019), the travel and tourism sector has started to make use of travelers' biometric information intensively for travel facilitation (Callahan, 2019). Travel authorities and providers collect and use travelers' fingerprints and face images in exchange for ease in crossing national borders, gaining access to restricted areas in airports (e-gates), and saving time with faster processing (Morosan, 2018). For example, British Airways claims that the adoption of biometric boarding solutions using facial recognition technology will streamline its processes, allowing the boarding process for a plane of 400 passengers to be completed in just 22 minutes (Doherty, 2019). Cruise providers have followed, adopting similar technologies to speed up boarding processes; cameras equipped with computer vision algorithms capture passengers' faces and compare them with photographic identification previously submitted online. While the benefits of sharing biometric and behavioral data are apparent for both consumers and providers, the collection and use of personal data perceived as sensitive can create complexities exacerbating consumer concerns over data privacy, and mounting serious issues in the travel and tourism sector (Bachman, 2019; Millward, 2019).

Indeed, privacy concerns in the travel context encompass idiosynchrasies that demand a more in depth examination due to the type of information being requested (e.g., biometric) as well as the means of collection of the information (e.g., wearable device). Therefore, it is imperative to understand the underlying factors that affect travellers concerns over data privacy and subsequently their willingness to share their personal information with service providers. While the need to explore travelers' privacy concerns has been highlighted in the literature (Anuar & Gretzel, 2011), very few privacy studies have focused on the travel context (C. H. Lee & Cranage, 2011; Tussyadiah, Li, & Miller, 2019; Wozniak et al., 2018); studying either privacy breach issues associated with location-based social media and publicly available data (Vu, Law, & Li, 2018), examining the role of security and privacy in smart tourism destinations (Jeong & Shin, 2019), the impact of psychological antecedents on consumer behavior during travel (Wozniak et al., 2018), the intention to transact online (Bonsón Ponte, Carvajal-Trujillo, & Escobar-Rodríguez, 2015; C.-C. Liang & Shiau, 2018) and create user generated content (Hew, Tan, Lin, & Ooi, 2017). In particular, there is a lack of empirical studies that comprehensively investigate antecedents and outcomes of travelers' privacy concerns in light of the introduction of new technological solutions requiring the sharing of a new class of personal information such as face scan or activity data. Most privacy research has examined information disclosure based on basic demographic information (e.g., name, email address) or financial information (e.g., credit card).

A wealth of existing theoretical work has suggested that privacy levels, along with privacy perceptions, regulation behaviors, and information disclosure are inherently context-dependent and vary across situations (Masur, 2018). "Privacy is a subjective perception resulting from the characteristics of the environment in which an individual happens to be at a given time" (Masur, 2018, p. 312). Indeed, Acquisti et al. (2015) suggest that privacy preferences, and cost–benefit trade-offs in privacy decisions, are context-dependent: depending on the situation, individuals will vary their privacy behavior ranging from very extreme concerns to complete apathy. Masur (2018) supports the situationality of privacy and disclosure, showing that the level of privacy is determined by perception of the environment. Different online environments encompass distinct peculiarities, offering different circumstances of communication, and thus different levels of privacy. Depending on the type of the digital platform or application, different environmental factors will influence one's privacy disclosure decisions (Masur, 2018). Recently, Smith et al. (2011) argued that further research on the parameterization of the Antecedents – Privacy Concerns – Outcomes (APCO) model is essential in cases where contextual differences are salient; different contexts can be either emerging technological applications (e.g., location-based services), different types of information collected (e.g., behavioral, biometric) and the use of information by different sectors (e.g., travel, healthcare, finance). The online travel environment encompasses all these contextual differences. However, there is a lack of comprehensive understanding and empirical evidence on the cost–benefit privacy trade-off in online travel environments.

To address this, the present study aims to apply the privacy calculus theory and the APCO framework to contribute to the understanding of privacy concerns and online self-disclosure in the travel context using two different types of personal information: biometric and behavioral information. The objectives of this study are twofold: (1) to understand the factors that contribute to travelers' online privacy concerns and (2) to explore the impacts of privacy concerns and other relevant factors on the disclosure of biometric and behavioral information. The findings will benefit a wide range of travel stakeholders, such as hotels, airline companies, and destination management organizations, to identify the drivers and inhibitors of travelers' privacy behavior in order to offer customer solutions that can effectively counteract consumers' privacy concerns, while enable the co-creation of value and unique personalized experiences that lead to satisfied customers and increased business profits.

2. Theoretical background and research hypotheses

2.1 Privacy

Privacy as a concept has been defined and presented in numerous ways across different disciplines: as a moral or legal right (Warren & Brandeis, 1890), a commodity (Bennett, 1995), or a state (Westin, 1967). In the Information Systems (IS) domain, information privacy is understood to describe the desire and ability to control the acquisition and secondary uses of one's personal information (Bélanger & Crossler, 2011). Several assessment methods have been proposed to measure the complex concept of

privacy. According to Smith, Dinev and Xu, (2011), "because of the near impossibility of measuring privacy itself" (p. 997), most empirical studies on privacy rely on a proxy to measure the concept. A central construct that has been widely used is privacy concerns, which represent individuals' perceptions of what will happen to the information they provide to different providers (Dinev & Hart, 2006). There have been several attempts to operationalize the measure of privacy concerns (Jung & Park, 2018). The most commonly used scales are the Concern for Information Privacy (CFIP) instrument (Smith, Milberg, & Burke, 1996), which measures four data-related dimensions of privacy concerns: collection, error, secondary uses, and unauthorized access (Bélanger & Crossler, 2011). Further, the Internet Users' Information Privacy Concerns (IUIPC) instrument was developed in the context of e-commerce environments (Malhotra, Kim, & Agarwal, 2004). Since then, several studies have attempted to improve and provide more precise versions of the aforementioned instruments, either by re-evaluating the scales or by adapting them in different contexts (Buchanan, Paine, Joinson, & Reips, 2007; Malhotra et al., 2004; Stewart & Segars, 2002; Taddicken, 2010).

Research in IS has investigated the differences in levels of privacy concerns and their impact on a number of dependent variables such as willingness to provide information and intention to transact online (Bélanger & Crossler, 2011; Yu, Li, He, Wang, & Jiao, 2019). In their interdisciplinary review of privacy research, Smith, Dinev and Xu (2011) summarized existing privacy research into the Antecedent – Privacy Concern – Outcome (APCO) framework of information privacy, with privacy concerns as the central element, accompanied by its antecedents and outcomes; suggesting that further research on the identification of the factors that contribute to privacy concerns is essential. Further, Li (2011) systematically reviewed existing empirical studies on privacy and found several antecedents of privacy concerns. These are: (a) individual factors (demographics, personality traits, knowledge and experience, self-efficacy), (b) social factors (e.g., social norms), (c) organizational factors (privacy policies, website informativeness, company reputation), (d) macro-environmental factors (culture, regulatory structures), and (e) information contingencies (information sensitivity, type of information) (Bélanger & Crossler, 2011; Li, 2011; Miltgen & Peyrat-Guillard, 2014). For some factors (e.g., privacy experiences having a positive impact on privacy concerns), results have been cross-validated across studies, while for others (e.g., internet use and fluency and the big five personality traits), results have been inconsistent (Y. Li, 2011). Therefore, it is essential to conduct further research to examine the impact of different antecedents on privacy concerns.

2.2 Privacy Calculus

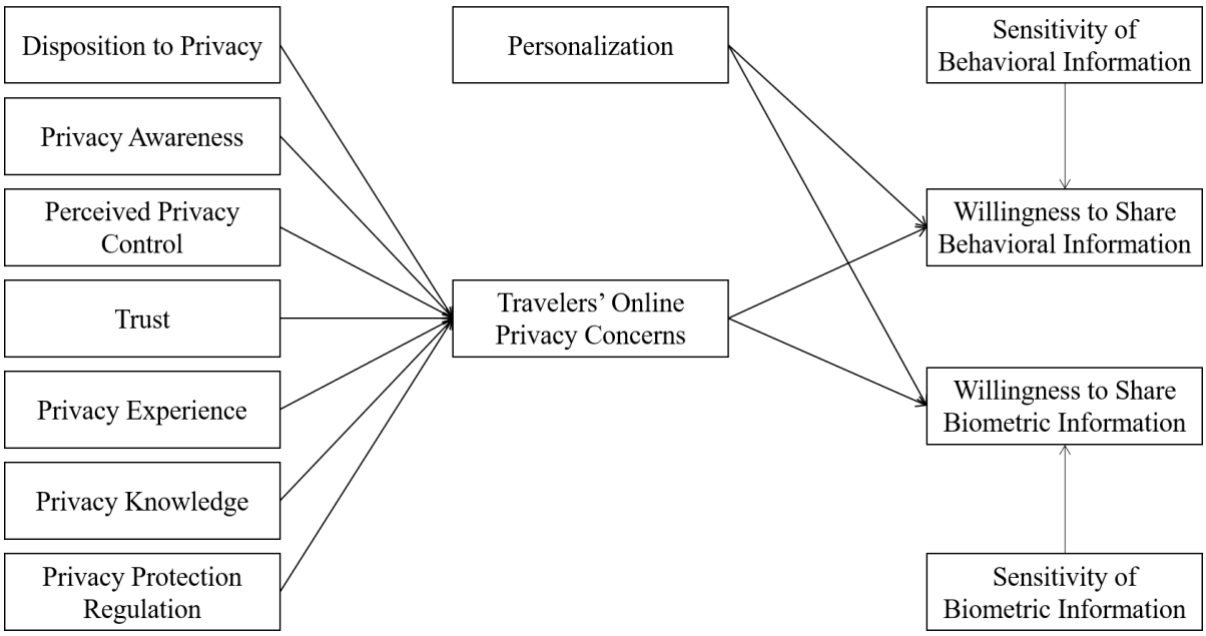
The privacy calculus theory suggests that people perform a cognitive evaluation of the consequences of their choices during privacy decision making by weighing the potential costs and benefits of each situation. As a result, based on this trade-off calculus analysis if perceived benefits exceed costs, then individuals are more likely to disclose their personal information (X. Li, 2008; Wang, Duong, & Chen,

2016; Q. Yang, Gong, Zhang, Liu, & Lee, 2020). In the online context, the privacy calculus refers to privacy concerns as the operationalization of costs and gratifications (e.g. personalization services*)* as the operationalization of benefits (Trepte, Scharkow, & Dienlin, 2020). Furthermore, Acquisti et al. (2015) argue that privacy calculus is context-dependent as in some situations individuals are willing to share their personal information in exchange for certain benefits (e.g., discounts), while during other times and situations they take extreme measures in order to protect their privacy. A wealth of literature has adopted the privacy calculus model to understand privacy perceptions and behaviors of consumers in various settings, such as health, e-commerce, and social networking sites (SNS) (Bol et al., 2018). However, they remain scarce in the travel context. An exception is Ozturk, Nusair, Okumus, and Singh (2017)'s study, which integrates in the privacy calculus the personalization-privacy paradox, privacy concerns, trust, and risk in predicting loyalty in mobile hotel booking. Further research is therefore necessary to understand privacy calculus in the context of online travel environments. This study adopts the privacy calculus theory as the conceptual basis, proposing that competing factors such as perceived personalization benefits and information sensitivity are weighted when an individual is considering possible outcomes from disclosing different types of personal information.

In direct contrast with the privacy calculus theory stands the privacy paradox, the discrepancy between individuals' stated privacy concerns and their actual information disclosure. Although consumers might report high concerns over their information privacy, they do very little to protect it (Gerber, Gerber, & Volkamer, 2018). In fact, it has been demonstrated that users are willing to share their personal passwords with strangers in exchange for a small piece of chocolate (Happ, Melzer, & Steffgen, 2016). However, many studies have debated the existence of privacy paradox. For example, in their recent meta-analytic review of 166 studies from 34 countries, Baruh, Secinti, and Cemalcilar (2017) showed that online users with higher privacy concerns were less likely to share their personal information online and divulging less information, supporting the privacy calculus theory.

Based on the privacy calculus theory and following the APCO framework, a theoretical model was developed to conceptualize the effect of several antecedents on travelers' online privacy concerns (TOPC) and the impact of TOPC on willingness to provide biometric and behavioral information to online travel service providers (Figure 1). The antecedents considered relevant to privacy decision making in online environments were included: (1) individual or psychological factors (i.e., disposition to privacy, privacy awareness, perceived privacy control, trust), (2) knowledge and experience (i.e., privacy knowledge, privacy experience), (3) contextual factors (i.e., information sensitivity, perceived personalization benefits) and (4) macro-environmental factors (i.e., privacy protection regulation). The impacts of privacy concerns as well as information sensitivity, and perceived benefits of personalization on willingness to disclose biometric and behavioral information were also conceptualized.

Figure 1. The theoretical model



2.3 Understanding the antecedents of travelers' online privacy concerns in privacy calculus

a. Individual Factors

Disposition to privacy, referring to a person's inherent need and tendency to preserve his information privacy space or "restrain the disclosure of personal information across a broad spectrum of situations and contexts" (Xu, Dinev, Smith, & Hart, 2011, p. 805), has been considered as a major determinant of privacy concerns. Previous studies have indicated that an individual's disposition can influence their tolerance or thresholds for privacy threats in online environments (Xu, Dinev, Smith, & Hart, 2011). Disposition to privacy can contribute to the development of higher information privacy concerns in cases where an individual feels threatened and needs to preserve their personal privacy space. It can also lead to lower privacy concerns in situations where one feels comfortable sharing information with service providers. Travelers with higher disposition to privacy are more protective of their information privacy space as they inherently cherish their personal boundaries. Thus, they are more sensitive and cautious with information requests from travel service providers and perceive these requests as privacy intrusion. Thus, it can be hypothesized that:

H1a: Disposition to privacy is positively associated with travelers' online privacy concerns.

Privacy awareness refers to "the knowledge of the technical elements related to information privacy, the understanding that the elements exist in the environment and projection of their impacts in the future" (Correia & Compeau, 2017, p. 4). The elements include the technology, the regulations and practices used by companies regarding the collection and use of personal information; the environment constitutes where the data flow, i.e., from one's device to all destinations (Correia & Compeau, 2017). Privacy awareness can be cultivated and enhanced through own personal experiences, exposure to

media coverage on topics concerning privacy and data security issues (Benamati, Ozdemir, & Smith, 2017; Smith, Dinev & Xu, 2011; Xu, Dinev, Smith, & Hart, 2008), talks, privacy campaigns, tutorials, and privacy policies of providers (Pötzsch, 2009). Privacy awareness can be supported by technical tools and mechanisms, such as digital nudging, reminding users to be conscious and mindful of their privacy when interacting with online providers (Gluck et al., 2016; Hughes-roberts, 2015). An example of such tools is Privacy Bird, an application that evaluates the matching between one's privacy stated preferences and the website's privacy policy (Pötzsch, 2009).

In travel, privacy awareness can stem from popular media that tend to focus more on broadcasting threats related to traveler information privacy (e.g., Marriott's data breach exposing records of 500 million customers), as well as personal negative experiences of travel scams being shared online in social media platforms (e.g., Airbnb travel scam stories). The use of videos to explain privacy policy, which constitutes nudging through presentation (Lee, Au, & Law, 2013) can enrich travelers' privacy awareness. Previous studies have shown that individuals who are highly privacy-aware and acquainted with privacy-related topics are more concerned of their individual privacy. Thus, it is expected that travelers with higher privacy awareness are more likely to show higher privacy concerns when interacting with online travel providers. Therefore, the following hypothesis is suggested:

H1b: Privacy awareness is positively associated with travelers' online privacy concerns.

Perceived privacy control refers to the amount of control that individuals believe they have over the disclosure and subsequent use of their personal information (Xu et al., 2008). Perceived privacy control has been widely used in privacy studies and demonstrated to reduce privacy concerns (Xu et al., 2008). For instance, in their study on social networking sites (SNS) and data disclosure, Zlatolas, Welzer, Heričko, & Hölbl, 2015 found that users who felt in good control over their privacy settings on Facebook have less privacy concerns. In the travel context, Anuar and Gretzel, (2011) argue that the inherent differences of the various technological solutions that travelers use (e.g., location-based services) provide different extent of control over the information that is collected or shared (e.g., settings), thus resulting in different levels of privacy concerns. It can be argued that travelers who feel greater control over the disclosure and subsequent use of their personal data in online travel environments will demonstrate less privacy concerns. Consequently, it can be hypothesized that:

H1c: Perceived privacy control is negatively associated with travelers' online privacy concerns.

Trust is defined as one's "willingness to be vulnerable to the actions of another" (Benamati, Ozdemir, & Smith, 2017, p. 588). Trust in an online provider involves accepting the vulnerability of disclosing personal information and considering the provider to be competent to protect personal information from improper access and unauthorized secondary use. Thus, consumers who are willing to trust an online provider may be more likely to have fewer concerns regarding their privacy (Pavlou, Liang, & Xue, 2007). Although consumer trust has been deemed as a major predictor of consumer

decision making in e-commerce there is a paucity of research on the impact of trust in the online context of travel and tourism products (Agag & El-Masry, 2017).

In the travel context, studies have shown that hotel providers considered as more trustworthy can increase consumers' online information disclosure (Morosan & DeFranco, 2015); trust is a significant antecedent of travel customers' behavior such as attitude towards an online travel provider as well as intention to purchase through an online travel website (Agag & El-Masry, 2017). However, there is a paucity of research examining the impact of trust on travelers' privacy concerns. As a sub-category of e-commerce environments, the online travel context might trigger higher information privacy concerns due to the use of certain technologies such as the biometric authenticators as well as requests for more sensitive information, including web history or activity sensor data. Evidence shows that travelers are highly concerned about their privacy and potential misuse of their data when interacting with online travel providers (Yoo, Kwon, Na, & Chang, 2017). As a result, we expect that a trustworthy relationship between travelers and online travel providers will have a significant negative impact on privacy concerns:

H1d: Trust is negatively associated with travelers' online privacy concerns.

b. Knowledge and Experience

Personal knowledge and experiences constitute important sources of information about general privacy and organizational data management practices. Individuals who have accumulated knowledge and skills about privacy issues from various resources, and those with previous negative privacy invasion experiences are more likely to have higher privacy concerns (Malhotra, Kim, & Agarwal, 2004; Yeh et al., 2018; Youn, 2009). The ability to perceive threats in a certain situation and accurately evaluate the factors in the environment that might incur loss of privacy require certain knowledge, that might stem from experience about these threats (Masur, 2018). Existing research has argued that people who have experienced privacy infringement in the past such as unauthorized collection and use of personal information from online providers, show more concerns over their information privacy (Yeh et al., 2018). As a result, we expect that travelers who interact with various online travel providers, having past privacy experiences and prior knowledge on privacy related matters, will be more sensitive and concerned about the information practices of online travel providers. Thus, it can be hypothesized that:

H2a: Privacy knowledge is positively associated with travelers' online privacy concerns.

H2b: Privacy experience is positively associated with travelers' online privacy concerns.

c. Macro-environmental factor

The involvement of governments in privacy regulations plays a critical role in shaping people's concerns about the protection of their personal information. Privacy protection regulation can be

described as the perceived regulatory policies that governmental agencies devise and apply regarding business practices on the online collection and use of individuals' personal information (Lwin, Wirtz, & Williams, 2007). Consumers with limited knowledge or access to privacy and security resources often rely on governmental regulations regarding the protection of their individual privacy rights, thus constituting regulations imperative. Literature suggests that the perceived level of government effectiveness in enforcing privacy regulations (e.g., GDPR) directly reduces levels of consumers' privacy concerns (Lwin et al., 2007). Since different countries have devised different privacy regulations (such as GDPR or the California Consumer Privacy Act), consumers originating from countries without any or limited privacy regulations show higher concerns about disclosure and secondary use of their personal information (Bellman, Johnson, Kobrin, & Lohse, 2004; Lwin et al., 2007). Travelers using online applications and crossing boundaries might have to adapt to new privacy regulatory frameworks for privacy protection and information disclosure, which might exacerbate privacy concerns (Tussyadiah et al., 2019). In a recent study, most consumers stated moderately aware of GDPR and their individual rights (Presthus & Sorum, 2018). Since GDPR has priority over the laws of individual states and it can increase perceived control over one's personal data (Presthus & Sorum, 2018; van Ooijen & Vrabec, 2019), it is expected that travelers will feel more protected regarding their information privacy. Therefore, the following hypothesis is suggested:

H3: Privacy protection regulation perceptions are negatively associated with travelers' online privacy concerns.

2.4 Understanding the impact on willingness to share information in privacy calculus

Previous studies have used privacy cost-benefit trade-off analysis, rooted in the Privacy Calculus theory (Laufer & Wolfe, 1977), to identify factors that influence intention to disclose information (Gerber, Gerber, & Volkamer, 2018; Smith, Dinev & Xu, 2011). Among these, online privacy concerns were found to negatively influence behavioral intention towards information disclosure (Wozniak, Schaffner, Stanoevska-Slabeva, & Lenz-Kesekamp, 2018; Zlatolas, Welzer, Heričko, & Hölbl, 2015). Rational individuals perform an internal cost-benefit analysis during every decision making; this logic can be applied to the decision making process that takes places in the travel and tourism context when travelers interact with online travel providers, such as it applies everywhere else (Yoo et al., 2017). In their study, Oliveira, Araujo, & Tam, (2020) found that security and privacy reasons are one of the top lurking motives, while also the most explanatory inhibitor of sharing travel experiences in social media (i.e., online users preferring to stay anonymous in order to preserve their privacy and safety). While interacting with online travel providers, travelers are concerned about their information privacy and potential misuse or leaks of personal information (Yoo et al., 2017). Especially in the context of biometric information, these concerns are amplified due to the nature of information. Biometric information refers to information about a person's physical characteristics that rarely or never change,

are unique to each individual, and thus can be used to determine their identity, such as fingerprint, voice sample, face scan, and iris/retina image (Morosan, 2018; Mothersbaugh, Foxx, Beatty, & Wang, 2012).This type of information might exacerbate privacy concerns as it is highly sensitive and descriptive of the individual (can reveal medical conditions, race and gender), it is irrevocable thus cannot be changed if compromised, and cannot be controlled by the user once disclosed (Morosan, 2019). According to Smith, Milberg and Burke (1996), individuals who are concerned about their information privacy will be more likely to protect biometric information and thus engage in preventive behaviors. Recently, it has been revealed that travelers who are concerned about their privacy are less willing to share biometric information at e-gates in airports (Morosan, 2018) and facial images with hotels (Morosan, 2019). As a result, we can hypothesize that:

H4a: TOPC is negatively associated with willingness to share biometric information.

Behavioral data refers to the information about the behavioral patterns of individuals that can include browsing patterns and search history (e.g., cookies), personal interests and preferences such as room selection in a hotel or dietary requirements, as well as location and activity data (e.g., number of steps, floors climbed). This type of data is extremely important for business providers; by collecting behavioral data, businesses can deliver more targeted, 'consumer centric marketing' offering more relevant information as well as personalized and customized products and services, tailored to match individual needs and interests; however, these targeted solutions have given rise to privacy concerns, as individuals feel 'creeped out' and their privacy being invaded (Dwivedi et al., 2019; Mathews-Hunt, 2016). For example, while location-based services (LBS) can offer significant values to users, such as locatability and personalization by placing information, transactions and entertainment in a location specific context, they also present a threat to users. LBS offer several conveniences for travelers, such as locating resources and points of interest (e.g., ATMs and restaurants) when traveling, navigating to a destination, social networking (e.g., finding friends), receiving alerts about traffic or location based advertisements (Saravanan & Sadhu Ramakrishnan, 2016). However, privacy concerns over aggregated consumer location data arise from the fear of possible breach of confidentiality, where the location information can reveal the actual position of the user in real time that is considered as an intrusion of personal privacy (Xu, Teo, Tan, & Agarwal, 2009). Although the tourism context heightens perceived benefits, tourism activities (e.g., information requests) usually happen in unfamiliar places facilitated by unknown providers that might create concerns over information privacy (Anuar & Gretzel, 2011). As a result, we expect that travelers who are more sensitive about their behavioral data will be less willing to share this type of information:

H4b: TOPC is negatively associated with willingness to share behavioral information

Information sensitivity can be defined as the potential loss associated with the disclosure of that information, which can be psychological (e.g., mental well-being), physical (e.g., health), or material (e.g., financial) loss (Mothersbaugh et al., 2012). For consumers, information that is more personally

identifying is considered as more sensitive and thus more uncomfortable to divulge (Schomakers, Lidynia, Müllmann, & Ziefle, 2019). Few studies have examined the role of information sensitivity in influencing information disclosure (Kokolakis, 2017). Existing evidence shows that the higher the degree of the information sensitivity the higher the resulting protection behaviors thus reducing willingness to share personal information (S. Yang & Wang, 2009). Likewise, travelers are more willing to share generic data (e.g., age, gender, nationality) than more personal data (e.g., real time location, expenses in places, social media profile, smartphone search history) with tourism providers (Femenia-Serra, Perles-Ribes, & Ivars-Baidal, 2018), demonstrating the important role of information sensitivity in information disclosure. Recognizing that the disclosure of different types of information (e.g., financial versus biographical information) is associated with different levels of risk (Malhotra et al., 2004), travelers are likely to feel more protective over more sensitive types of information. The specific context of information disclosure (type of information requested) significantly affects the calculation of benefits–risks during privacy decision making, as more sensitive information is associated with more perceived risk (Morosan, 2019). Since both biometric and behavioral information are considered highly sensitive types of information, travelers are likely to be more sensitive and protective of these types of data, thus showing less willingness to share these with online travel providers. Therefore, it can be hypothesized that:

H5a: Information sensitivity is negatively associated with willingness to share biometric information.

H5b: Information sensitivity is negatively associated with willingness to share behavioral information.

By collecting consumer information, businesses can provide personalize their services, providing meaningful experiences and offers that fit perfectly each traveler's unique needs, wishes and desires, ultimately achieving the highest customer satisfaction (Masseno, 2019). Travel providers can offer tailored travel packages and promotions based on consumers' previous travel purchases (e.g., booked trips) and other information, such as dietary restrictions, using artificial intelligence to establish basic preferences regarding the size and rate of hotel rooms, products in the minibar, etc. (Gilliland, 2017). For example, Accor Hotels recently introduced a tool that can measure guests' behavioral activity as well as biometric responses, such as brain activity, heart rate, and galvanic skin response against multi-sensory stimuli to determine the most appealing travel experiences and preferences. The algorithm is able to build a psychological and personality profile of the user, matching them to types of holidays that are later suggested to the user (WTTC, 2018). As such, personalization can create benefits for customers, such as convenience, reduced costs, efficiency, and individualization (C. H. Lee & Cranage, 2011). Although, some consumers might refuse to use personalized services in fear of loss of privacy and potential misuse of personal information, the ultimate tradeoff between privacy and personalization depends on the value that consumers feel they can obtain from using personalized

services (Karwatzki, Dytynko, Trenz, & Veit, 2017). Personalization enables a fit between tailor made services and travelers' needs, thus increasing their perception of service quality while also enhancing their intention to use such online travel providers (Huang, Goo, Nam, & Yoo, 2017).

During the cognitive analysis of a privacy decision, individuals weigh in the perceived benefits and perceived risks of the situation to make a decision. When individuals anticipate greater benefits, they perceive greater value in the potential gains from disclosing personal information to providers, resulting in a higher disclosure intention (Mothersbaugh et al., 2012; C.-H. Yeh et al., 2018). Consumers prefer to share personal information when receiving highly personalized services that target their individual needs (Karwatzki et al., 2017; Ozturk, Nusair, Okumus, & Singh, 2017) thus personalization is perceived as a benefit. Recently, a significant positive impact of expected benefits on air travelers' intention to share biometric information at e-gates has been found (Morosan, 2018). Consequently, travelers are more likely to share their biometric and behavioral information in exchange for personalization benefits (e.g., faster boarding process, tailored offers, personalized solutions and experiences). The following hypotheses are therefore suggested:

H6a: Personalization is positively associated with willingness to share biometric information.

H6b: Personalization is positively associated with willingness to share behavioral information.

2.5 Demographics as control variables

Prior research has suggested several demographic factors that can influence the intention towards information disclosure. Since our primary focus is not on these factors, they are included as control variables in the data analysis of the proposed theoretical model. These variables are gender, age, and levels of education (Wakefield, 2013).

3. Methodology

This study developed a theoretical model to understand the factors influencing traveler's online privacy concerns and compare individual's privacy decision-making when (1) biometric information is requested and (2) behavioral information is requested from online travel providers. To test the proposed research model, an online survey was distributed by a professional research survey company to a panel of UK residents in May 2019, targeting travelers who use online travel environments. Also, the survey included a set of screening questions to confirm participants' travel and online booking experience in the last six months (i.e., they have booked flight or accommodation online). Items for information sensitivity and willingness to share information with online travel companies were self-developed for the purposes of the study. Participants were asked to state the degree of sensitivity of as well as the degree of willingness to share biometric and behavioral information. All other measurement items were

derived from existing privacy literature, thus have established their validity and reliability (see Appendix B), but further tested them in the online travel context. All items were anchored on a 5-point Likert scale ranging from 1="strongly disagree" to 5="strongly agree". For information sensitivity, a 5-point semantic scale was used where 1="not sensitive" to 5="very sensitive"; while for willingness to share information the semantic scale ranged from 1="not willing" to 5="very willing".

A total of 836 responses were collected; after excluding responses with missing data and those who did not pass the attention check questions, the usable sample size was 685. Among the respondents, 47.2% were male, with most of them between 26 and 45 years old (45%) and having finished high school (38.8%) (see Table A1 in Appendix A). The statistical analysis was conducted by using covariance-based structural equation modeling (CB-SEM) with IBM SPSS Amos version 25. For the information sensitivity constructs, an exploratory factor analysis (EFA) was performed to classify the types of personal information based on sensitivity. Then, a confirmatory factor analysis (CFA) was performed to estimate the measurement model and to check the reliability and validity of the all measurement scales. Finally, SEM was conducted to test the structural model.

4. Results

An exploratory Factor Analysis (EFA) was performed to uncover the underlying structure of the biometric and behavioral information constructs. Maximum Likelihood (ML) with Promax rotation based on eigenvalues more than one was used as the factor extraction method. Items with factor loadings less than 0.5 were discarded to determine a simple factor structure. Bartlett's test of sphericity was conducted ensuring chi-square value significant at 0.05 level (chi-square = 9965.325, Sig<0.001) and Kaiser-Meyer-Olkin (KMO) value higher than 0.60 (0.9), indicating that the selection of the extraction method was appropriate and suitable (Carpenter, 2018; Hair et al. 2010). Cronbach's Alpha value for the biometric data was 0.917, while that for the behavioral data was 0.838, indicating high reliability. Table A2 in the Appendix A presents the loadings of the items on the factors.

The descriptive analysis results (see Tables 1-2) showed that participants consider biometric information as highly sensitive, with the fingerprint ranked the most sensitive data item (M=4.69); overall behavioral information is perceived as less sensitive than biometrics. Interestingly, participants consider data such as hobbies (M=2.84) as not very sensitive, while real time location (M=3.57) and smartphone search history (M=4.01) are considered more sensitive. Regarding information disclosure intention, travelers claim to be very reluctant to share any types of biometric information (M=1.69), with almost equal means across all data items, and less reluctant to disclose behavioral information (M=2.39). However, participants reported to be willing to share their personal preferences (M=3.61).

Table 1. Mean estimates for information sensitivity

	Information Sensitivity	Mean	Std. Deviation
Biometric information	fingerprint	4.69	0.776
	voice sample	4.45	0.953
	face image	4.53	0.901
	iris pattern	4.53	0.920
	Overall	4.55	0.89
Behavioral information	hobbies	2.84	1.158
	personal preferences	2.68	1.000
	real time position	3.57	1.180
	smartphone search history	4.01	1.116
	activity sensor data	3.42	1.316
	specific expenses	3.87	1.131
	Overall	3.40	1.150

Table 2. Mean estimates for willingness to share information

	Willingness to share information	Mean	Std. Deviation
Biometric information	fingerprint	1.69	1.117
	voice sample	1.70	1.108
	face image	1.69	1.103
	iris pattern	1.67	1.093
	Overall	1.69	1.110
Behavioral information	hobbies	2.42	1.376
	personal preferences	3.61	1.315
	real time position	2.39	1.224
	smartphone search history	1.79	1.126
	activity sensor data	2.00	1.202
	specific expenses	2.14	1.263
	Overall	2.39	1.250

4.1 Estimation of the Measurement model: confirmatory factor analysis (CFA)

Before testing the proposed model, preliminary tests for normality, linearity, multicollinearity, and homoscedasticity were performed (see Tables A3-A5 in Appendix A). Then, a confirmatory factor analysis (CFA) was conducted to assess whether the data fit the proposed theoretical model and to check for the validity and reliability of the measured constructs. The reliability and construct validity of the measurement model were evaluated by checking composite reliability (CR), average variance extracted (AVE), and Cronbach's alpha values. AVE and CR were calculated to check for the scale reliability and internal consistency. AVE values should exceed 0.50, while CR values above 0.70 (Hair, Black, Babin, Anderson, & Tatham, 2010). The results suggest adequate convergent validity and construct reliability (see Tables A5 and A6 in Appendix A). Discriminant validity was tested ensuring that the square root of AVE for each construct is larger than the corresponding Squared Inter-construct Correlations (SIC) (Fornell & Larcker, 1981). All AVE values exceed the relative SIC (see Table A6 in Appendix A), establishing discriminant validity.

The goodness-of-fit indices fall between the suggested thresholds suggesting that the data fit the model well (Hair et al., 2010) (see Table 3). Furthermore, tests were conducted to check for

Common Method Variance (CMV) on the observed relationships among the measured variables (Mackenzie, Podsakoff, Podsakoff, & Mackenzie, 2011; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Harman's single factor test was performed; only 20% of variance in all variables is explained by a single factor, demonstrating that CMV is not a concern in this study. Moreover, another test was conducted to ensure that no correlations exceed 0.90, which could indicate a possible bias in the collected data. Results show that none of the calculated correlations exceed the suggested threshold, thus CMV does not pose a serious concern in this study. Also, the common latent factor method was conducted in order to capture common variance among all observed variables in the model. The zero constrained test showed that the null hypothesis cannot be rejected (i.e., the constrained and unconstrained models are the same), demonstrating that there is no specific response bias affecting the model (Serrano Archimi, Reynaud, Yasin, & Bhatti, 2018). Furthermore, following Podsakoff, MacKenzie, Lee, and Podsakoff (2003) and Liang, Saraf, Hu, and Xue, (2007), as shown Table A7 in Appendix, we compared the standardized regression weights with and without the common factor, as well as the method factor loadings. Results showed that (1) the differences in regression weights are very small (0<.200) (Serrano Archimi et al., 2018), (2) the average variance of indicators (0.818) is substantially greater than the average method variance (-0.026). Therefore, we can argue that common method bias is unlikely to be a serious concern for this study. Thus, the rest of the analysis can continue without the addition of a common latent factor.

Table 3. Measurement model fit indices

Evaluation of Models	CMIN/DF	CFI	RMSEA	GFI	AGFI	CMIN
CFA model	2.463	0.930	0.046	0.835	0.813	3459.9

4.2 Estimation of the Structural Model

The structural model was estimated to test the proposed hypotheses. Control variables (age, gender, and education) were introduced to account for potential confounding factors that can influence the dependent variables in the proposed model. Results showed that gender, age and education do not have a significant effect on the willingness to share biometric data; however, gender and age showed a significant impact on willingness to share behavioral data thus were retained in the model. Goodness-of-fit indices were evaluated to check the overall fit of the model. Results show that the data fits the final model well; the fit indices fall between the suggested thresholds (Hair et al., 2010) (see Table 4). All but four hypotheses were validated (see Table 5 and Figure 2).

Table 4. Fit indices of the structural model

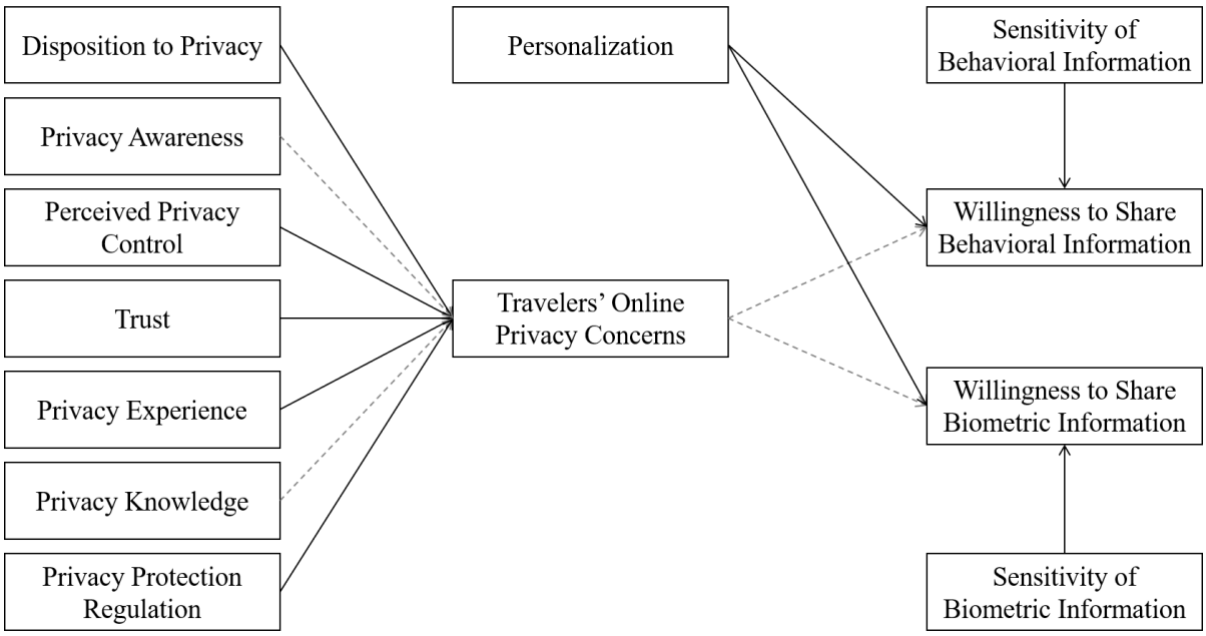
Evaluation of Models	CMIN/DF	CFI	RMSEA	GFI	AGFI	CMIN
Structural Model	2.764	0.915	0.051	0.817	0.795	3938.7
Structural Model with controls	2.711	0.913	0.050	0.817	0.794	4107.4

Table 5. Hypotheses testing of the proposed theoretical model

Hypothesis	Estimate	Result
H1a: Disposition to Privacy → (+) TOPC	0.644***	Supported
H1b: Privacy Awareness → (+) TOPC	0.011NS	*Not Supported*
H1c: Perceived Privacy Control → (-) TOPC	-0.104**	Supported
H1d: Trust → (-) TOPC	-0.214***	Supported
H2a: Privacy Knowledge → (+) TOPC	-0.075NS	*Not Supported*
H2b: Privacy Experience → (+) TOPC	0.138***	Supported
H3: Privacy Protection Regulation → (-) TOPC	-0.087**	Supported
H4a: TOPC → (-) Willingness to Share Biometric Information	0.225NS	*Not Supported*
H4b: TOPC → (-) Willingness to Share Behavioral Information	0.163***	*Not Supported*
H5a: Sensitivity of Biometric Information → (-) Willingness to Share Biometric Information	-0.621***	Supported
H5b: Sensitivity of Behavioral Information → (-) Willingness to Share Behavioral Information	-0.447***	Supported
H6a: Personalization → (+) Willingness to Share Biometric Information	0.469***	Supported
H6b: Personalization → (+) Willingness to Share Behavioral Information	0.446***	Supported

Note: **$p<0.05$, ***$p<0.001$, NS = not significant

Figure 2. Final estimation model



5. Discussion and Implications

5.1 Key findings

The key contribution of this study constitutes in providing empirical evidence on the context dependence of privacy preferences (Acquisti et al., 2015), expanding current understanding of the privacy calculus theory in the travel context. The same individual might be extremely concerned in certain situations, but at other times totally oblivious to privacy issues (Acquisti et al., 2015). This study offers a better understanding of the cost–benefit trade-off analysis (personalization vs. privacy concerns and information sensitivity) performed during privacy decision making for the disclosure of two sensitive types of information: biometric and behavioral information, to online travel service providers. The findings add to the limited base of research on travelers' privacy behavior, clarifying that although concerned about their privacy, travelers are still willing to share their behavioral data with online travel providers. In the case of biometric data disclosure, the sensitivity of biometric information is a significant hindrance to disclosure, while personalization benefits contribute significantly (positively) to disclosure intention.

5.2 Theoretical contributions

This study aims to provide a deeper understanding of the privacy concerns and information disclosure in online travel environments. Using the privacy calculus theory and the APCO framework, this study examines several factors as antecedents of travelers' online privacy concerns (TOPC) as well as the relationships of these concerns with willingness to provide biometric and behavioral information, along

with sensitivity of information and benefits of personalization. The online travel environment represents a unique environment involving its own complexities and distinct specificities due to the nature of information being requested (e.g., biometric) and the means of the information being collected (e.g., emerging technologies). Privacy behavior has been deemed as highly context dependent thus the investigation of these relationships that are fundamental to online information disclosure are advancing existing scientific knowledge and enhancing the travel and privacy literature.

Antecedents of privacy concerns

Results reveal that several salient individual factors, including disposition to privacy, privacy control, and privacy experience, as well as trusting beliefs and perceived privacy protection regulation significantly impact privacy concerns. These results complement and expand existing privacy literature suggesting that individual factors constitute major determinants of privacy concerns (Benamati, Ozdemir, & Smith, 2017; Zlatolas, Welzer, Heričko, & Hölbl, 2015) thus enhancing current knowledge on the influence of individual characteristics and perceptions on traveler privacy behavior.

More specifically, the results confirm previous studies in the US demonstrating that privacy experience and disposition to privacy are important predictors of privacy concerns (Y. Li, 2014; Xu et al., 2011; Xu, Gupta, Rosson, & Carroll, 2012). They are also in accordance with studies in Europe demonstrating that the lack of individual privacy control triggers anxiety and thus privacy concerns (Miltgen & Peyrat-Guillard, 2014), including a study in UK on the important role of trust in mitigating privacy concerns (Miltgen & Smith, 2015). However, the results come in disagreement with previous research on the role of privacy protection regulation. Studies have argued that in individualistic countries (e.g., France, the UK) people are skeptical about the efficacy of privacy regulations (Miltgen & Peyrat-Guillard, 2014), thus worry about their information privacy. This seems not to be valid today, as demonstrated by this study findings. Travelers from the UK have reported feeling protected by existing privacy regulations, showing less privacy concerns. Since 2014, privacy perceptions may have changed in the UK due to the recent introduction of GDPR and the radical changes in data legislation. GDPR headlines have been very prominent during the last two years, showcasing the enforcement of the new data law by authorities with huge penalties and fines imposed to big companies (e.g., $57 million to Google) (Satariano, 2019). Thus, this supports the efficacy of privacy protection regulations and enhancing privacy perceptions for UK citizens.

The study results demonstrate that privacy awareness and privacy knowledge show no influence on travelers' privacy concerns. It was expected that travelers who are more aware of privacy-related topics and more knowledgeable about the collection and use of personal information practices will be more sensitive and protective over their online privacy (Benamati et al., 2017). However, previous studies have found mixed results (Benamati et al., 2017; Xu et al., 2011). Xu et al. (2011) argue that privacy cognitive processes are complex, multi-faceted, and context-specific, thus privacy

beliefs should be related to consumers' own information experiences and social contexts. Distributing an online survey to users of four different websites (e-commerce, social media, finance, and healthcare), Xu et al.'s study showed that privacy awareness varies across the different websites. For example, a positive effect of privacy awareness on privacy concerns was found in e-commerce, while a negative association was reported in social networking. Our results confirm that privacy is a context-dependent phenomenon, demonstrating the null effect of privacy awareness on individual concerns. It might be that as travelers become more aware of travel-related privacy issues, they become more apt to find ways to protect themselves from privacy threats and risks, thus feel no concerns over their online privacy (Li, 2011). Another explanation is that privacy knowledge and privacy experience are not directly associated with privacy concerns, but these relationships are mediated or moderated by other factors. More research is therefore essential to explain these relationships, elucidating how privacy awareness and knowledge affect privacy concerns.

Overall, our results reveal that certain antecedents (i.e., disposition to privacy, privacy control, experience, and trust) can be considered as universal factors in affecting privacy concerns, with individuals in different countries and different contexts sharing the same concerns, while privacy awareness and privacy knowledge appear to be more context specific. Our results enhance current knowledge enforcing the notion supported by previous research that certain factors (e.g., individual characteristics) remain stable and do not vary across situations, while others, both stable and non-stable factors, influence privacy behavior, thus should be examined simultaneously (Masur, 2018). Thus, this constitutes one of the first studies investigating and establishing the stability as well as situationality of certain antecedents of privacy concerns in online travel environments.

Information disclosure intention

This study provides empirical evidence suggesting that consumers perceive various types of personal information differently and attribute different valuations to them (Kokolakis, 2017), while also confirming the context dependence of privacy preferences. As highlighted by previous research (Acquisti, Brandimarte, & Loewenstein, 2015; Kokolakis, 2017), privacy behavior is a highly contextual phenomenon, thus individuals should not be expected to exhibit similar behaviors in different contexts. Contradictory results are expected when studies are conducted in different contexts.

In contrary to previous research, a positive impact of privacy concerns on willingness to share behavioral information was found. These findings support previous research supporting the 'privacy paradox', the discrepancy between users' concerns and information disclosure. The privacy paradox claims that individuals who are concerned about their privacy being infringed are still willing to share personal information with business providers as long as they would gain something in return. The findings in this study support this notion; although travelers claim to be concerned about their information privacy, they are still willing to share their behavioral data with online travel providers in

exchange for personalization benefits. Weighing the costs and benefits of information disclosure, travelers perceive the disclosure of behavioral information as the enabler of high-value personalization services for their travel, which 'override' their existing privacy concerns. Another explanation might lie in the regulatory focus theory (RFT) (Higgins, 1997) that predicts the persuasiveness of rewards for encouraging information disclosure. As promotion-focused individuals weigh differently costs and benefits than prevention-focused consumers, they are focused more on maximizing gains from information disclosure requests. Thus, promotion-focused travelers might view the disclosure as a gain rather than a loss, weighing more the perceived personalization benefits that online travel providers are offering. More research is essential to advance current knowledge about the role of RFT in privacy behavior, especially in the travel context.

While the subject of privacy concerns over biometric information collection for travel facilitation has been highly debated in the media, this study did not find the link between travelers' privacy concerns and their willingness to share biometric information with travel providers. The privacy calculus in traveler's decision making related to biometric information disclosure does not involve a simultaneous trade-off of concerns and benefits, as disclosure intention is mostly influenced by perceived benefits of personalization and information sensitivity. Our findings demonstrate that travelers do not consider privacy concerns during their privacy decision making process (as suggested in the privacy calculus theory), but instead they weigh in the sensitivity of biometric information and the expected benefits of disclosing them in the travel environments. In support of previous studies showing that benefits override privacy concerns (Chellapa & Sin, 2005; Yeh et al., 2018), our findings reveal the important role of perceived benefits in travelers' privacy decision making involving sensitive data (i.e., biometric information), thus contributing to the under-developed research area on the social aspects of biometrics. The findings contradict previous studies in the physical travel context (Morosan, 2018) reporting a negative impact of privacy concerns on intention to disclose biometric information. One explanation could lie in the fact that travelers might associate biometric information being collected physically (e.g., e-gates at airports) rather than online (e.g., web or mobile applications). While biometric verification is used in airports, cruise ships, hotels, and rental car companies around the world both physically and online, respondents might relate more to the physical biometric authentication rather than the online one.

Furthermore, our findings enforce the important role of information sensitivity in the privacy calculus, which has not been considered in previous studies (Kokolakis, 2017) as they have mostly focused on investigating the impact of information sensitivity on privacy concerns (Li, 2011). By placing information sensitivity as a specific type of risk within the model, our study contributes to the privacy calculus theory by demonstrating that travelers are more protective over personal information they consider more sensitive. By doing so, we provide a more comprehensive and holistic understanding of the conceptualization of the privacy calculus.

5.2 Practical implications

The results offer the travel sector a foundation to make informed business decisions with regards to the collection and use of biometric and behavioral information of travelers. This can apply to a wide range of providers, not only airlines, travel agents, car rental and cruise companies, but also government authorities and entertainment businesses catering to travelers. The collection of data constitutes one of the major drivers and sources of profit for business providers, thus our findings can help companies to understand in more depth user privacy preferences and concerns. Consequently, they can enhance their knowledge on their customer bases and offer a wider range of data sharing options as well as adjustments of privacy-preservation practices.

Our findings highlight the important role of personalization in inducing information disclosure. Organizations can intensify efforts to improve existing as well as develop new, innovative personalization services. In a recent study (Loo, 2017), 57% of tourists believe that companies should tailor their information and personalize experiences based on personal preferences and past behaviors, while 36% of them would be willing to pay more for such tailored and personalized services. Therefore, it becomes apparent that there is a strong drive for more customized, meaningful experiences (Loo, 2017). For example, when travelers are planning a trip, thousands of options regarding flights or accommodation are available; personalized search tools based on budget, preferred amenities, and personal preferences can quickly match individual customer needs, will offer significant value. Personalized recommendations including detailed itineraries based on previous activity, search history, and personal interests could enhance value as well. The findings in this study help business providers to understand how offering more attractive content or rewards can entice user willingness to provide personal information. However, businesses should also provide explicit details on their websites on how data acquisition and personalization can be beneficial and create value for users, while at the same time provide assurances on the privacy collection practices of the organization.

Moreover, this study encourages the travel industry to become more aware of the differential concerns regarding different types of information requests, thus catering for individual needs. While travelers might be willing to share behavioral data, it is not always the case for biometric information. Consequently, business providers should distinguish between different categories of personal information during the design and development of tools or platforms requesting such information for personalization or other purposes (e.g., entertainment). Requests for information should be distinctively separate for each information type rather than a bundle, avoiding the risk that the user will reject sharing any personal information altogether. A potential solution would be the development of privacy enhancing technologies as standalone applications or add-ons, where users undertake a risk assessment over the service providers (i.e., whether providers are risky or trustworthy) and determine the amount

and type of personal data they are willing to share with them. The consideration of individual privacy preferences, encompassing users' sensitivity to different types of personal information, in the development of technological solutions would allow for the establishment of online environments that are perceived as more secure, where users have more control over their personal data and personalization features, increasing trust in service providers, minimizing privacy concerns, and thus encouraging information disclosure.

5.3 Limitations and future directions

This study has examined the impact of a set of antecedents on travelers' online information privacy concerns. However, many factors have been identified in existing literature as potential antecedents to privacy concerns. As a result, further research is essential in examining the impact of additional factors such as self-efficacy, perceived enjoyment, and personality traits, as well as additional macro environment factors, such as culture and social norms, on privacy concerns. Moreover, this study used self-reported measures for capturing individual privacy perspectives and behavioral intentions. However, sometimes individuals might misreport their own behavior. Thus, further research should consider measuring actual information disclosure, comparing it with behavioral intention to explore whether privacy paradox, the divergence between consumers' statements and actual actions, exists in the context of travel and information disclosure. Another limitation of this study lies in the construct of personalization, which captures the overall perception of benefits of personalization services rather than specific benefits. Future research needs to examine the impact of specific types of personalization benefits (e.g., offers, recommendations, advertising messages) on information disclosure.

6. Conclusion

This study expands existing privacy literature by confirming a set of factors that shape the privacy concerns of travelers and providing a more comprehensive explanation of the APCO framework (Smith et al., 2011) in the travel context. By examining biometric and behavioral information disclosure, this study highlights the profound role of information sensitivity in the privacy calculus, an observation that has been notably absent in existing research (Mothersbaugh et al., 2012). Contrary to hypotheses, perceived expected benefits outweigh privacy concerns when travelers are faced with such privacy decisions, emphasizing the important role of incentives in the collection of personal information. Also, as most research have investigated the technical aspects of biometric authentication, our study extends research on the social aspects of biometrics. Overall, this study enhances both IS and management literature by offering a deeper understanding of travelers' privacy behavior as well as the behavioral outcomes of sharing sensitive personal data.

References

Agag, G. M., & El-Masry, A. A. (2017). Why Do Consumers Trust Online Travel Websites? Drivers and Outcomes of Consumer Trust toward Online Travel Websites. *Journal of Travel Research*, *56*(3), 347–369. https://doi.org/10.1177/0047287516643185

Anuar, F. I., & Gretzel, U. (2011). Privacy Concerns in the Context of Location-Based Services for Tourism. *Short Paper, Presented at ENTER 2011, Innsbruck (Austria), January 26-28*.

Bachman, J. (2019). *The Struggle to Turn Your Face Into Secure Travel ID - Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-07-01/the-struggle-to-turn-your-face-into-secure-travel-id

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.1159/000360196

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science*, *43*(5), 583–600. https://doi.org/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*.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Bonsón Ponte, E., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management*, *47*, 286–302. https://doi.org/10.1016/j.tourman.2014.10.009

Buchanan, T., Paine, C., Joinson, A., & Reips, U. D. (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), 157–165. https://doi.org/10.1002/asi

Callahan, J. (2019). *How The Travel Industry Is Driving Biometric Security Innovation*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/01/09/how-the-travel-industry-is-

driving-biometric-security-innovation/#1780a1166572

Chellapa, R., & Sin, R. G. (2005). Personalisation vs. Privacy: An empirical Examination of the online Consumers' Dilemma. *Information Technology and Management*, *6*(2–3), 181–202.

Correia, J., & Compeau, D. (2017). Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. *HICSS 2017 Proceedings*. Retrieved from http://hdl.handle.net/10125/41646

Dinev, T., & Hart, P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

Doherty, A. (2019). How biometrics is reshaping the travel experience. *TTGMEDIA*. Retrieved from https://www.ttgmedia.com/news/technology/how-biometrics-is-reshaping-the-travel-experience-17642

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., … Williams, M. D. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Femenia-Serra, F., & Neuhofer, B. (2018). Smart tourism experiences: Conceptualisation, key dimensions and research agenda. *Investigaciones Regionales*, *2018*(42), 129–150.

Femenia-Serra, F., Perles-Ribes, J. F., & Ivars-Baidal, J. A. (2018). Smart destinations and tech-savvy millennial tourists: hype versus reality. *Tourism Review*. https://doi.org/10.1108/TR-02-2018-0018

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.1177/002224378101800313

Gao, S., Mokhtarian, P., & Johnston, R. (2008). *Non-normality of Data in Structural Equation Models*. *Transportation Research Record*, 2082(1), 116-124.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gilliland, N. (2017). How six travel & hospitality brands use personalisation to enhance the customer experience – Econsultancy. Retrieved February 21, 2020, from: https://econsultancy.com/how-six-travel-hospitality-brands-use-personalisation-to-enhance-the-customer-experience/

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How Short Is Too Short ? Implications of Length and Framing on the Effectiveness of Privacy Notices. *Symposium On Usable Privacy and Security (SOUPS)*, (Soups), 321–340.

Hair, J. F., Black, W., Babin, B., Anderson, R., & Tatham, R. (2010). *Multivariate data analysis* (6th ed.). Pearson Prentice Hall.

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat - Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61*, 372–377. https://doi.org/10.1016/j.chb.2016.03.026

Harari, G. M., Lane, N. D., Wang, R., Crosier, B. S., Campbell, A. T., & Gosling, S. D. (2016). Using Smartphones to Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and Challenges. *Perspectives on Psychological Science*, *11*(6), 838–854. https://doi.org/10.1177/1745691616650285

Hew, J. J., Tan, G. W. H., Lin, B., & Ooi, K. B. (2017). Generating travel-related contents through mobile social tourism: Does privacy paradox persist? *Telematics and Informatics*, *34*(7), 914–935. https://doi.org/10.1016/j.tele.2017.04.001

Higgins, E. T. (1997). Beyond pleasure and pain. *American Psychologist*, *52*(12), 1280–1300. https://doi.org/10.1037/0003-066x.52.12.1280

Huang, C. D., Goo, J., Nam, K., & Yoo, C. W. (2017). Smart tourism technologies in travel planning: The role of exploration and exploitation. *Information and Management*, *54*(6), 757–770. https://doi.org/10.1016/j.im.2016.11.010

Hughes-roberts, T. (2015). Privacy as a secondary goal problem : an experiment examining control. *Information and Computer Security*, *23*(4), 382–393. https://doi.org/10.1108/ICS-10-2014-0068

Jeong, M., & Shin, H. H. (2019). Tourists' Experiences with Smart Tourism Technology at Smart Destinations and Their Behavior Intentions. *Journal of Travel Research*, 1–14. https://doi.org/10.1177/0047287519883034

Jung, Y. and Park, J. (2018) 'An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services', International Journal of Information Management. Elsevier, 43(May), pp. 15–24. doi: 10.1016/j.ijinfomgt.2018.05.007.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, *34*(2), 369–400. https://doi.org/10.1080/07421222.2017.1334467

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, C. H., & Cranage, D. A. (2011). Personalisation-privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, *32*(5), 987–994. https://doi.org/10.1016/j.tourman.2010.08.011

Lee, H. A., Au, N., & Law, R. (2013). Presentation Formats of Policy Statements on Hotel Websites

and Privacy Concerns: A Multimedia Learning Theory Perspective. *Journal of Hospitality and Tourism Research*, *37*(4), 470–489. https://doi.org/10.1177/1096348012436384

Li, X. (2008). Will it be Disclosure or Fabrication of Personal Information? An Examination of Persuasion Strategies on Prospective Employees. *International Journal of Information Security and Privacy*, *2*(4), 91–113.

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, *28*(28), 453–496. https://doi.org/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*, *57*(1), 343–354. https://doi.org/10.1016/j.dss.2013.09.018

Liang, C.-C., & Shiau, W.-L. (2018). Moderating effect of privacy concerns and subjective norms between satisfaction and repurchase of airline e-ticket through airline-ticket vendors. *Asia Pacific Journal of Tourism Research*, *23*(12), 1142–1159. https://doi.org/10.1080/10941665.2018.1528290

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: Management Information Systems*, *31*(1), 59–87. https://doi.org/10.2307/25148781

Loo, J. (2017). The future of travel: New consumer behavior and the technology giving it flight. Retrieved February 20, 2020, from Think with Google website: https://www.thinkwithgoogle.com/marketing-resources/new-consumer-travel-assistance/

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. https://doi.org/10.1007/s11747-006-0003-3

Mackenzie, S. B., Podsakoff, P. M. and Podsakoff, N. P.. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research : Integrating New and Existing Techniques. *MIS Quarterly*, *35*(2), 293–334. https://doi.org/10.2307/23044045

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Casual Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.l040.0032

Masseno, M. D. (2019). Personalization and Profiling of Tourists in Smart Tourism. *Revista Argumentum-Argumentum Journal of Law*, *20*(3), 1–215.

Masur, P. K. (2018). Situational privacy and self-disclosure: Communication processes in online environments. Springer. https://doi.org/10.1007/978-3-319-78884-5_1

Mathews-Hunt, K. (2016). CookieConsumer: Tracking online behavioural advertising in Australia. *Computer Law and Security Review*, *32*(1), 55–90. https://doi.org/10.1016/j.clsr.2015.12.006

Millward, D. (2019). *Facial recognition technology is worrying US air passengers – and it's coming*

to Britain. Retrieved from https://www.telegraph.co.uk/travel/news/facial-recognition-airports-concerns/

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125. https://doi.org/10.1057/ejis.2013.17

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information and Management*, *52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Morosan, C. (2018). Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions. *Journal of Travel Research*, *57*(5), 644–657. https://doi.org/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), 3149–3172. https://doi.org/10.1108/ijchm-08-2018-0701

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*. https://doi.org/10.1016/j.ijhm.2015.03.008

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research*, *15*(1), 76–98. https://doi.org/10.1177/1094670511424924

Oliveira, T., Araujo, B., & Tam, C. (2020). Why do people share their travel experiences on social media? *Tourism Management*, *78*(November 2017), (in press). https://doi.org/10.1016/j.tourman.2019.104041

Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers*, *19*(4), 753–767. https://doi.org/10.1007/s10796-017-9736-4

Pallant, J. (2010). *SPSS survival manual : a step by step guide to data analysis using SPSS*. Open University Press/McGraw-Hill.

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding And Mitigating Uncertainty In Onine Exchange Relationships: A principal Agent Perspective. *MIS Quarterly*, *31*(1), 105–136.

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. https://doi.org/10.1037/0021-9010.88.5.879

Pötzsch, S. (2009). Privacy Awareness: A Means to Solve the Privacy Paradox? In *The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology, vol 298* (pp. 226–236). Springer.

Presthus, W., & Sorum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey

Emphasizing the General Data Protection Regulation. *Procedia*, *138*, 603–611.

Saravanan, S., & Sadhu Ramakrishnan, B. (2016). Preserving privacy in the context of location based services through location hider in mobile-tourism. *Information Technology and Tourism*, *16*(2), 229–248. https://doi.org/10.1007/s40558-016-0056-1

Satariano, A. (2019). Google Is Fined $57 Million Under Europe's Data Privacy Law - The New York Times. *The New York Times*. Retrieved from https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Schomakers, E. M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, *46*(November 2018), 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Serrano Archimi, C., Reynaud, E., Yasin, H. M., & Bhatti, Z. A. (2018). How Perceived Corporate Social Responsibility Affects Employee Cynicism: The Mediating Role of Organizational Trust. *Journal of Business Ethics*, *151*(4), 907–921. https://doi.org/10.1007/s10551-018-3882-6

Sigala, M. (2018). New technologies in tourism: From multi-disciplinary to anti-disciplinary advances and trajectories. *Tourism Management Perspectives*, *25*(December 2017), 151–155. https://doi.org/10.1016/j.tmp.2017.12.003

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 1063–1078. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/DOI 10.1287/isre.13.1.36.97

Taddicken, M. M. M. (2010). Measuring Online Privacy Concern and Protection in the (Social) Web: Development of the APCP and APCP-18 Scale. *International Communication Association, Suntec Singapore International Convention & Exhibition Centre, Suntec City, Singapore, June 22, 2010*.

Themistocleous, C., Smith, A., & Wagner, C. (2014). The ethical dilemma of implicit vs explicit data collection: Examining the factors that influence the voluntary disclosure of information by consumers to commercial organizations. *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, ETHICS 2014*, 1–6. https://doi.org/10.1109/ETHICS.2014.6893403

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, 106115. https://doi.org/10.1016/j.chb.2019.08.022

Tussyadiah, I., Li, S., & Miller, G. (2019). Privacy Protection in Tourism: Where We Are and Where

We Should Be Heading For. *Pesonen J., Neidhardt J. (Eds) Information and Communication Technologies in Tourism 2019*, (January), 278–290. https://doi.org/10.1007/978-3-7091-1142-0

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Vu, H. Q., Law, R., & Li, G. (2018). Breach of traveller privacy in location-based social media. *Current Issues in Tourism*, *0*(0), 1–16. https://doi.org/10.1080/13683500.2018.1553151

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003

Wang, T., Duong, T. D. and Chen, C. C. (2016) 'Intention to disclose personal information via mobile applications: A privacy calculus perspective', International Journal of Information Management, 36(4). doi: 10.1016/j.ijinfomgt.2016.03.003.

Warren, S. D., & Brandeis, L. D. (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, A. F. (1967). *Privacy And Freedom*. https://doi.org/https://doi.org/10.1177/000271626837700157

Wozniak, T., Schaffner, D., Stanoevska-Slabeva, K., & Lenz-Kesekamp, V. (2018). Psychological antecedents of mobile consumer behaviour and implications for customer journeys in tourism. *Information Technology and Tourism*, *18*(1–4), 85–112. https://doi.org/10.1007/s40558-017-0101-8

WTTC. (2018). Four Ways Biometrics Are Making Travel Smarter. *Medium*. Retrieved from https://medium.com/@WTTC/four-ways-biometrics-are-making-travel-smarter-47ea99333bf4

WTTC. (2019). Majority of travellers willing to share data for a more seamless experience | WTTC. Retrieved January 15, 2020, from https://www.wttc.org/about/media-centre/press-releases/press-releases/2019/majority-of-travellers-willing-to-share-data-for-a-more-seamless-experience/

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *International Conference on Information Systems (ICIS)*, (October), 1–16. https://doi.org/citeulike-article-id:5770148

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.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). *Measuring mobile users' concerns for information privacy*.In *ICIS 2012 Orlando.*

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information*

Systems, *26*(3), 135–174. https://doi.org/10.2753/MIS0742-1222260305

Yang, Q., Gong, X., Zhang, K. Z. K., Liu, H. and Lee, M. K. O. (2020) 'Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms', International Journal of Information Management. Elsevier, (November 2019), p. 102065. doi: 10.1016/j.ijinfomgt.2019.102065.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database*, *40*(1), 38. https://doi.org/10.1145/1496930.1496937

Yeh, C., Wang, Y.-S., Lin, S.-J., Tseng, T. H., Lin, H.-H., Shih, Y.-W., & Lai, Y.-H. (2018). What drives internet users' willingness to provide personal information? *Online Information Review*, *42*(6), 923–939. https://doi.org/10.1108/OIR-09-2016-0264

Yoo, C., Kwon, S., Na, H., & Chang, B. (2017). Factors affecting the adoption of gamified smart tourism applications: An integrative approach. *Sustainability (Switzerland)*, *9*(12), 1–22. https://doi.org/10.3390/su9122162

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy. *The Journal of Consumer Affairs*, *43*(3), 389–418.

Yu, L., Li, H., He, W., Wang, F. and Jiao, S. (2019) 'A meta-analysis to explore privacy cognition and information disclosure of internet users', International Journal of Information Management, 51(September), p. 102015. doi: 10.1016/j.ijinfomgt.2019.09.011.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

Appendix A

Table A1. Descriptive statistics of respondents

	Item	Frequency	Percentage (%)
Gender	Male	323	47
	Female	359	53
Age	<26	33	5
	26-35	164	24
	36-45	84	12
	46-55	118	17
	56-65	152	22
	>65	134	20
Education	Less than High School	20	3
	High School	266	39
	Bachelor	236	35
	Master	98	14
	PhD	27	4
	Other	38	5

Table A2. Factor loadings for biometric and behavioral information

Item	Factor 1 Biometric Information	Factor 2 Behavioural Data
Iris/retina pattern	0.981	
Face scan/image	0.889	
Voice sample	0.853	
Fingerprint	0.644	
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

Several tests were performed in order to ensure for the univariate and multivariate normality of the data. Skewness and kurtosis values were calculated regarding univariate normality, while Mardia's coefficient was estimated in order to check for multivariate normality.

Regarding univariate normality, we ensured that skewness and kurtosis fall between the accepted thresholds of -2 and +2 (see Table A3). Few items exceeded the suggested range values and can be deemed as non-normal, however large sample sizes reduce the detrimental effects of non-normality (Hair et al, 2010), while according to Tabachnick and Fidell (2014), in large sample sizes (N>200) the impact of departure from zero kurtosis diminishes. Therefore, these variables were retained with the assumption that non-normality in the data will not cause a major issue in our analysis. As a result, normality has been established in the collected dataset.

Mardia's multivariate normality test showed a critical ratio value of 30.5, exceeding the threshold of 5, thus suggesting small departure from normality (see Table A4). Following Gao, Mokhtarian, & Johnston, (2008), since the univariate skewness and kurtosis fall below the moderate non-normality thresholds (2 and 8 respectively), the critical ratio threshold should not be strictly applied in order to conform to multivariate normality. In their study, the authors argue that normality is rarely found in real datasets and demonstrate that by meeting the thresholds of univariate normality and achieving a critical ratio that is not extreme (~29) it can be accepted as the biases for the estimates of parameters and standard errors of the parameter estimates are controlled. As a result, we conclude that the collected data can be analyzed using structural equation modeling assuming normality.

Multicollinearity tests also showed that VIF values for all independent variables of the model ranged from 1.026 to 1.678 thus below the threshold of 3, confirming that multicollinearity is not an issue for our data (Pallant, 2010). In order to check for homoscedasticity, values of dependent variables were plotted against their residuals, indicating that their variances are homogenous. Also, ANOVA as well as curve estimation tests were conducted in order to assess the linearity between the independent and dependent variables of the proposed model. Results showed that all relationships are sufficiently linear.

Table A3. Univariate Normality

Item	Skewness	Kurtosis	Item	Skewness	Kurtosis
Disposition to Privacy			**Travelers Online Privacy Concerns**		
DP1	-0.057	-0.391	TOPC1	-0.469	-0.387
DP2	-0.546	0.003	TOPC2	-0.255	-0.652
DP3	-0.079	-0.529	TOPC3	-0.356	-0.590
Privacy Awareness			TOPC4	-0.347	-0.402
PA1	-0.887	2.789	TOPC5	-0.525	-0.157
PA2	-0.852	0.769	TOPC6	-0.051	-0.602
PA3	-0.651	0.480	TOPC7	-0.545	-0.467
Perceived Privacy control			TOPC8	-0.278	-0.614
PC1	-0.085	-0.626	TOPC9	-0.220	-0.573
PC2	-0.114	-0.771	TOPC10	-0.118	-0.737
PC3	-0.015	-0.729	TOPC11	-0.374	-0.387
PC4	-0.159	-0.693	TOPC12	-1.358	2.047
Trust			TOPC13	-1.787	3.325
TR1	-0.741	0.774	TOPC14	-1.675	2.759
TR2	-0.654	0.715	TOPC15	-0.584	-0.073
TR3	-0.644	0.632	TOPC16	-1.064	0.553
TR4	-0.527	0.093	TOPC17	-0.957	0.512
Privacy Experience			**Sensitivity of Biometric Information**		
PEX1	0.724	-0.309	STB1	-2.951	8.901
PEX2	0.943	0.113	STB2	-1.891	3.132
PEX3	0.541	-0.690	STB3	-2.121	4.182
Privacy Knowledge			STB4	-2.214	4.605
PK1	-0.433	-0.181	**Sensitivity of Behavioral Information**		
PK2	-0.273	-0.516	STBH1	0.112	-0.594
PK3	-0.464	-0.194	STBH2	0.269	-0.654
Privacy Protection Regulation			STBH3	-0.481	-0.608
PR1	-0.337	-0.480	STBH4	-1.137	0.674
PR2	-0.257	-0.274	STBH5	-0.370	-0.947
PR3	0.046	-0.626	STBH6	-0.783	-0.158
Personalization			**Willingness to Share Biometric Information**		
PE1	-0.752	1.220	WB1	1.571	1.466
PE2	-0.617	0.735	WB2	1.543	1.471
PE3	-0.672	0.527	WB3	1.552	1.493
			WB4	1.559	1.456
			Willingness to Share Behavioral Information		
			WBH1	0.470	-1.069
			WBH2	-0.689	-0.619
			WBH3	0.359	-0.894
			WBH4	1.345	0.877
			WBH5	0.892	-0.331
			WBH6	0.745	-0.616

Table A4. Multivariate Skewness and Kurtosis

Variable	Skewness	CR	Kurtosis	CR
Disposition to privacy	-0.209	-2.233	-0.058	-0.309
Privacy Awareness	-0.693	-7.403	0.847	4.525
Perceived Privacy Control	-0.124	-1.323	-0.577	-3.084
Trust	-0.668	-7.140	0.894	4.776
Privacy Experience	0.702	7.498	-0.232	-1.237
Privacy Knowledge	-0.336	-3.589	-0.125	-0.668
Privacy Protection Regulation	-0.136	-1.450	-0.206	-1.102
TOPC	-0.310	-3.314	-0.234	-1.249
Personalization	-0.510	-5.453	1.030	5.501
Sensitivity of Biometric Information	-2.200	-23.509	4.989	26.653
Sensitivity of Behavioral Information	-0.779	-8.324	0.287	1.531
Willingness to Share Biometric Information	1.533	16.383	1.420	7.588
Willingness to Share Behavioral Information	0.942	10.066	0.246	1.315
Multivariate			46.114	30.558

Table A5. Descriptive statistics, reliability, and validity

Variable	Mean	St. Deviation	Alpha	AVE	CR
Disposition to Privacy	3.392	0.781	0.775	0.548	0.782
Privacy Awareness	3.757	0.668	0.816	0.622	0.828
Perceived Privacy Control	3.035	0.925	0.942	0.803	0.942
Trust	3.529	0.812	0.933	0.783	0.935
Privacy Experience	2.218	0.991	0.903	0.759	0.904
Privacy Knowledge	3.216	0.826	0.870	0.697	0.873
Privacy Protection Regulation	3.041	0.860	0.852	0.660	0.853
TOPC	3.696	0.616	0.924	0.550	0.938
Personalization	3.543	0.679	0.833	0.626	0.834
Sensitivity of Biometric Information	4.551	0.796	0.917	0.739	0.919
Sensitivity of Behavioral Information	3.339	0.883	0.838	0.509	0.805
Willingness to Share Biometric Information	3.427	0.987	0.973	0.902	0.973
Willingness to Share Behavioral Information	2.392	0.937	0.843	0.590	0.877

Note: AVE = average variance extracted; CR = composite reliability

Table A6. Discriminant Validity: Fornell-Larcker Criterion

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
(1) Disposition to Privacy	**0.740**												
(2) Privacy Awareness	0.448	**0.789**											
(3) Perceived Privacy Control	0.071	0.261	**0.896**										
(4) Trust	-0.189	0.121	0.412	**0.885**									
(5) Privacy Experience	0.327	0.063	-0.080	-0.281	**0.871**								
(6) Privacy Knowledge	0.104	0.388	0.565	0.319	-0.002	**0.835**							
(7) Privacy Protection Regulation	-0.140	0.085	0.578	0.488	-0.126	0.464	**0.812**						
(8) TOPC	0.635	0.181	-0.255	-0.448	0.411	-0.175	-0.374	**0.742**					
(9) Personalization	-0.096	0.198	0.422	0.492	-0.108	0.467	0.502	***	**0.791**				
(10) Sensitivity of Biometric Information	0.078	0.107	-0.032	-0.058	0.020	0.006	-0.101	0.120	-0.020	**0.860**			
(11) Sensitivity of Behavioral Information	0.272	0.133	-0.052	-0.179	0.194	-0.052	-0.220	0.405	-0.076	0.503	**0.713**		
(12) Willingness to Share Biometric Information	0.018	-0.036	0.170	0.158	0.088	0.128	0.245	***	0.193	-0.349	-0.121	**0.950**	
(13) Willingness to Share Behavioral Information	0.042	-0.006	0.205	0.200	0.086	0.164	0.291	-0.102	0.260	-0.257	-0.357	0.730	**0.768**

Note: Square roots of average variance extracted (AVE) in the diagonal

Table A7. Common Method Bias Analysis

Construct	Indicator	Factor loading (R1)	R1^2	Factor loading with CLF	Delta	Method Factor Loading (R2)	R2^2
Disposition to Privacy	DP1	0.726	0.527	0.738	-0.012	-0.067	0.004
	DP2	0.641	0.411	0.569	0.072	-0.410	0.168
	DP3	0.841	0.707	0.823	0.018	-0.165	0.027
Privacy Awareness	PA1	0.604	0.365	0.564	0.040	-0.257	0.066
	PA2	0.815	0.664	0.789	0.026	-0.163	0.027
	PA3	0.915	0.837	0.924	-0.009	-0.110	0.012
Perceived Privacy Control	PC1	0.861	0.741	0.854	0.007	0.108	0.012
	PC2	0.887	0.787	0.885	0.002	0.075	0.006
	PC3	0.919	0.845	0.907	0.012	0.154	0.024
	PC4	0.916	0.839	0.909	0.007	0.114	0.013
Trust	TR1	0.772	0.596	0.764	0.008	0.116	0.013
	TR2	0.915	0.837	0.912	0.003	0.076	0.006
	TR3	0.931	0.867	0.929	0.002	0.074	0.005
	TR4	0.912	0.832	0.905	0.007	0.122	0.015
Privacy Experience	PEX1	0.834	0.696	0.833	0.001	0.076	0.006
	PEX2	0.894	0.799	0.892	0.002	0.050	0.003
	PEX3	0.884	0.781	0.886	-0.002	-0.011	0.000
Privacy Knowledge	PK1	0.831	0.691	0.829	0.002	-0.065	0.004
	PK2	0.902	0.814	0.902	0.000	-0.025	0.001
	PK3	0.765	0.585	0.764	0.001	-0.040	0.002
Privacy Protection Regulation	PR1	0.848	0.719	0.812	0.036	0.240	0.058
	PR2	0.757	0.573	0.758	-0.001	0.110	0.012
	PR3	0.829	0.687	0.793	0.036	0.245	0.060
Travelers Privacy Concerns	TOPC1	0.823	0.677	0.780	0.043	-0.255	0.065
	TOPC2	0.790	0.624	0.740	0.050	-0.273	0.075
	TOPC3	0.829	0.687	0.782	0.047	-0.268	0.072
	TOPC4	0.721	0.520	0.682	0.039	-0.238	0.057
	TOPC5	0.708	0.501	0.672	0.036	-0.226	0.051
	TOPC6	0.821	0.674	0.829	-0.008	-0.102	0.010
	TOPC7	0.707	0.500	0.705	0.002	-0.116	0.013
	TOPC8	0.827	0.684	0.817	0.010	-0.160	0.026
	TOPC9	0.848	0.719	0.813	0.035	-0.244	0.060
	TOPC10	0.753	0.567	0.753	0.000	-0.116	0.013
	TOPC11	0.873	0.762	0.845	0.028	-0.223	0.050
Personalization	PE1	0.792	0.627	0.793	-0.001	-0.063	0.004
	PE2	0.811	0.658	0.813	-0.002	-0.007	0.000
	PE3	0.770	0.593	0.768	0.002	0.022	0.000
Sensitivity of Biometric Information	SB1	0.763	0.582	0.737	0.026	-0.198	0.039
	SB2	0.854	0.729	0.834	0.020	-0.185	0.034
	SB3	0.934	0.872	0.908	0.026	-0.216	0.047
	SB4	0.882	0.778	0.863	0.019	-0.185	0.034
Sensitivity of Behavioral Information	SBH3	0.709	0.503	0.677	0.032	-0.136	0.018
	SBH4	0.736	0.542	0.747	-0.011	-0.194	0.038
	SBH5	0.738	0.545	0.711	0.027	-0.079	0.006
	SBH6	0.666	0.444	0.650	0.016	-0.209	0.044
Willingness to Share Biometric Information	WB1	0.939	0.882	0.908	0.031	0.239	0.057
	WB2	0.953	0.908	0.928	0.025	0.220	0.048
	WB3	0.938	0.880	0.913	0.025	0.215	0.046
	WB4	0.968	0.937	0.938	0.030	0.242	0.059
	WBH1	0.660	0.436	0.634	0.026	0.184	0.034
	WHB3	0.697	0.486	0.658	0.039	0.231	0.053

Construct	Indicator	Factor loading (R1)	R1^2	Factor loading with CLF	Delta	Method Factor Loading (R2)	R2^2
Willingness to Share Behavioral Information	WHB4	0.825	0.681	0.794	0.031	0.227	0.052
	WHB5	0.848	0.719	0.815	0.033	0.239	0.057
	WHB6	0.791	0.626	0.753	0.038	0.238	0.057
Average		**0.818**	**0.677**			**-0.026**	**0.033**

Appendix B

Measurement Items

Disposition to Privacy (Xu, Dinev, Smith, & Hart, 2011)

DP1 – "*Compared to others, I am more sensitive about the way online travel companies handle my personal information."*

DP2 – "*To me, it is the most important thing to keep my information privacy".*

DP3 – "*Compared to others, I tend to be more concerned about threats to my information privacy".*

Privacy Awareness (Xu, Dinev, Smith, & Hart, 2011)

PA1 – "*I am aware of the privacy issues and practices in our society."*

PA2 – "*I follow the news and developments about the privacy issues and privacy violations."*

PA3 – "*I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy."*

Perceived Privacy Control (Xu, Dinev, Smith, & Hart, 2011)

PC1 – *"I believe I have control over who can get access to my personal information collected by online travel companies."*

PC2 – "*I think I have control over what personal information is released by online travel firms."*

PC3 – "*I believe I have control over how personal information is used by online travel companies."*

PC4 – "*I believe I can control my personal information provided to online travel firms."*

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...

TR1 – *... I feel comfortable with online travel companies."*

TR2 – *... I can rely on online travel companies."*

TR3 – *... I can count on online travel companies."*

TR4 – *... I can depend on online travel companies."*

Privacy Experience (Li, 2014)

PEX1 – *"I have had bad experiences with regard to my online privacy before."*

PEX2 – "*I was a victim of online privacy invasion."*

PEX3 – "*I believe that my online privacy was invaded by other people or organizations."*

Privacy Knowledge (Youn, 2009)

"*When using an online travel website in order to research, plan and or book a trip, …*

PK1 – *… I am aware of how my information will be used."*

PK2 – *… I am aware of the extent to which my information will be accessible to other companies."*

PK3 – *… I am aware of whether or not the website requires valid permission when collecting information from me."*

Privacy Protection Regulation (Lwin, Wirtz, & William, 2007)

PR1 – "*The existing laws in my country are sufficient to protect consumers' online privacy."*

PR2 – "*There are stringent international laws to protect personal information of individuals on the Internet."*

PR3 – "*The government is doing enough to ensure that consumers are protected against online privacy violations."*

Personalization (Huang et al., 2017)

PE1 – "*Online travel companies allow me to receive tailored information."*

PE2 – "*I can interact with online travel companies to get personalized information."*

PE3 – "*The personalized information provided by online travel companies meets my needs."*

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

TOPC1 – "*I am concerned that the information I submit to online travel companies could be misused."*

TOPC2 – "*I am concerned that others can find private information about me from online travel companies."*

TOPC3 – "*I am concerned about providing personal information to online travel companies, because it could be used in a way I did not foresee."*

TOPC4 – "*I don't feel comfortable when I do not have control over personal data I disclose to online travel companies."*

TOPC5 – "*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."*

TOPC6 – "*It usually bothers me when online travel companies ask me for personal information."*

TOPC7 – "*When online travel companies ask me for personal information, I sometimes think twice before providing it."*

TOPC8 – "*It bothers me to give personal information to so many online travel companies."*

TOPC9 – "*I'm concerned that online travel companies are collecting too much information about me."*

TOPC10 – "*I don't feel comfortable to share information about my current location with online travel companies."*

TOPC11 – "*I am concerned with the security of sensitive information when I use online travel companies."*

TOPC12 – "*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."*

TOPC13 – "*Online travel companies should never sell the personal information in their computer databases to companies."*

TOPC14 – "*Online travel companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information."*

TOPC15 – "*Online travel companies should devote more time and effort to preventing unauthorized access to personal information."*

TOPC16 – "*Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs."*

TOPC17 – "*Online travel companies should take more steps to make sure that unauthorized people cannot access personal information in their computers."*

Sensitivity of Information (self-developed)

"For the following items listing different types of personal information, please tell us how sensitive you think the information is."

Willingness to Share Information *(*self-developed)

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