

## Effects of privacy concern, risk, and information control in a smart tourism destination

Olayinka Olasumbo Afolabi , Ali Ozturen & Mustafa Ilkan

To cite this article: Olayinka Olasumbo Afolabi , Ali Ozturen & Mustafa Ilkan (2021): Effects of privacy concern, risk, and information control in a smart tourism destination, Economic Research-Ekonomiska Istraživanja, DOI: [10.1080/1331677X.2020.1867215](https://doi.org/10.1080/1331677X.2020.1867215)

To link to this article: <https://doi.org/10.1080/1331677X.2020.1867215>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 06 Jan 2021.



Submit your article to this journal [↗](#)



Article views: 279



View related articles [↗](#)



View Crossmark data [↗](#)

# Effects of privacy concern, risk, and information control in a smart tourism destination

Olayinka Olasumbo Afolabi<sup>a</sup>, Ali Ozturen<sup>a</sup>  and Mustafa Ilkan<sup>b</sup>

<sup>a</sup>Faculty of Tourism, Eastern Mediterranean University, Famagusta, North Cyprus, Turkey; <sup>b</sup>School of Computing and Technology, Eastern Mediterranean University, Famagusta, North Cyprus, Turkey

## ABSTRACT

Smart tourism destinations are growing, with the use and implementation of technology to make travel more enjoyable. Still, the tourist's information privacy concerns generated by the big data available to the destination and service providers is a significant problem for smart tourism, which can affect the sustainability and economic benefit of the smart tourism destination. This study investigates privacy concern, perceived risk, control of information, service provider trust in a smart tourism destination, and the resulting behavioural intentions. The results were obtained using an online survey of 384 respondents that have visited the smart tourism destination Dubai. The results indicated that use context as an environmental factor helps mitigate the tourists' negative privacy concerns and perceived risk towards trust in a smart tourism destination. Furthermore, previous privacy violation experience as a personal factor was negatively related to trust in the smart tourism destination and the service providers. The study provides meaningful contributions on smart tourism to destination management organizations (DMO's) and service providers on what influences and mitigates the privacy concern of the tourists using mobile application location-based services available in a smart tourism destination, building on the social cognitive theory.

## ARTICLE HISTORY

Received 16 July 2020  
Accepted 16 December 2020

## KEYWORDS


Smart tourism destination; service providers; trust; privacy concern; mobile application; location-based services

## JEL CLASSIFICATIONS

C12; C52; M15; M31; Z32

## 1. Introduction

The tourism industry affects the economic (Huete Alcocer & López Ruiz, 2019), environmental (Wang et al., 2020) and social aspects of a destination (Sedarati & Baktash, 2017). The use of personalized services with the implementation of technology is necessary for keeping up with current and future developments of tourism (Kontogianni & Alepis, 2020). The number of users using mobile technology is increasing, and developing innovative applications to meet the various tourist's needs is the focus of service providers and different stakeholders in a smart destination

**CONTACT** Olayinka Olasumbo Afolabi  [olayinka.afolabi@cc.emu.edu.tr](mailto:olayinka.afolabi@cc.emu.edu.tr)

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

(Chang & Shen, 2018; Wang & Lin, 2017). Mobile technology has changed the tourism industry, tourists take pictures and share with their friends (Buhalis & Foerste, 2015), gather information, make better decisions (Wang et al., 2014), and find nearest places of interest (Neuhofer et al., 2015). They now use mobile phones as they had previously used their desktop and laptops (Ozturk et al., 2017). Data is used by the service provider in a smart tourism destination to suggest sightseeing locations, send events notifications, provide location-based advertising, use real-time personalized services based on the tourist location and preference (Femenia-Serra et al., 2019). Information can easily be available to the tourist using their mobile phone location-based service in a smart tourism destination (Garcia et al., 2019). The personal information about tourists is made available to multiple stakeholders and service providers by the technology implemented in the smart tourism destination (Femenia-Serra et al., 2019). A research gap that has not been explored is the privacy concerns of the tourists towards the use of their data, and this is a critical gap as the tourists could influence the growth, economic benefit and sustainability of the smart tourism destination (Pradhan et al., 2018). This study introduces the privacy paradox to the smart tourism domain by considering the technology mobile application location-based services, the tourists, and the context of the environment that is the smart tourism destination. The study aims to investigate the factors that influence and mitigate privacy concerns of mobile application location-based services in a smart tourism destination to develop trust and positive behavioural intentions.

## **2. Literature review**

### **2.1. Social cognitive theory**

Social cognitive theory (SCT) suggests that mutual, reciprocal interaction exists between behaviour, environment, and personal factors (Bandura, 1989). Several studies have used the SCT to explain individual factors' influence on behaviours (Boateng et al., 2016; Hoffmann et al., 2015). The theory suggests that environmental factors influence both behavioural and personal factors, the environment can affect a person's expectation and beliefs, and the environment can be physical and social (Boateng et al., 2016). This study employs this relationship with use-context which is 'the very concrete environment in which technology is going to be used' (Van de Wijngaert & Bouwman, 2009, p. 86) and the smart tourism destination which is a smart connected environment (Femenia-Serra et al., 2019). SCT has been used in the study for technology adoption and tourism sustainability (Font et al., 2016; Rana & Dwivedi, 2015). Considering the interrelationship between the three factors that makes up the SCT, this study uses this theory to build on the hypothesized relationship.

### **2.2. Smart tourism destination and mobile application location-based services**

For a tourism destination to be considered smart, stakeholders should be automatically interconnecting, using technology and intelligent systems as a platform for tourism-related activities and instant information exchange (Buonincontri & Micera,

2016; Del Chiappa & Baggio, 2015). The technology platform used in smart tourism destinations has several interfaces that can enable different end-users to use the system to dynamically share information in real-time (Choe & Fesenmaier, 2017). Smart tourism uses cloud computing, Internet of things, big data and smart devices (Buhalis & Amaranggana, Buhalis & Amaranggana, 2015). For instance, destinations install chips in entrance and transportation tickets that allow the service provider to know tourist's consumption behaviour, location information, and in turn use this information to provide location-based and real-time advertising (Lin et al., 2016). In Dubai, one of their most popular service providers Etisalat provides near field communication that lets mobile phones access bus stations' locations, arrival time, and make payments (Khan et al., 2017). Researches on smart tourism destinations are just gaining attention, and few studies have investigated tourist behaviour as regards privacy concerns (Pradhan et al., 2018).

### **2.3. Privacy concern**

Privacy concern deals with how a user is concerned about the disclosure and accessibility of their personal information (Ooi et al., 2018). The fear can be that they do not trust the service providers to access, use, and store their personal information correctly (Zhou & Li, 2014). Privacy concerns have been studied to negatively influence affective trust (Ngelambong et al., 2018), and service provider trust (Ozturk et al., 2017). Privacy concerns negatively influence people's trust in disclosing their personal information (Bansal et al., 2015). Therefore, we hypothesize:

**H1:** Privacy concern is negatively related to (a) trust in a smart tourism destination, (b) trust in location-based services (LBS) provider.

### **2.4. Perceived privacy risk**

Perceived privacy risk is defined as the negative perceptions, which customers feel towards a service or a product making them conclude that ambiguous and unwanted outcomes would precede their transaction with their personal information (Zhou, 2012). Users have been known to have a high level of risk perceptions when they are exposed to completing their activities with new technology (Ozturk, 2016). Perceived privacy risk has been studied to hinder the adoption of LBS (Wang & Lin, 2017). Perceived risk is influential in predicting tourist's behaviour (Choi et al., 2016). Ozturk et al. (2017) reports that privacy risk would negatively influence trust and privacy concerns. Therefore, we hypothesize:

**H2:** Perceived privacy risk is negatively related to (a) trust in a smart tourism destination, (b) trust in LBS provider.

### **2.5. Information control**

Perceived ability to control one's information is defined as the power of users to decide what information about them they allow to be used, or not used (Taylor et al.,

2009). When consumers believe they have control over how their personal information is shared, it helps foster trust (Mosteller & Poddar, 2017). Secondary control of information is positively related to trust in social media websites, and negatively related to consumer's privacy concerns (Mosteller & Poddar, 2017). Perceived control of information is positively associated with sharing information online (Hajli & Lin, 2016). Therefore, we hypothesize:

**H3:** Perceived ability to control information is positively related to (a) trust in a smart tourism destination, (b) trust in LBS provider.

## **2.6. Use context**

The rationale behind the decision making of user's online technology use is extended beyond the traditional cost and benefit analysis but governed by different contexts (Gambino et al., 2016). In the domain of information systems, context is an important concept (Kim et al., 2019), especially with mobile application (Chang, 2015). The use of mobile technology is exposed to shifting use contexts, and use context has been described as an essential factor influencing the adoption of mobile innovations (Afolabi et al., 2020). Yang et al. (2012) found that use context affects the formation of attitude and behaviour towards information technology. User behaviour with technology can be influenced by the situation in which technology is being used (De Reuver et al., 2013). The smart tourism destination is a technology-centric environment, and the use context of technology would be very high, therefore using the social cognitive theory, we hypothesize that:

**H4:** Use context moderates the relationship between (a) privacy concern and destination trust, (b) privacy concern and LBS provider trust.

**H5:** Use context moderates the relationship between (a) perceived risk and destination trust, (b) perceived risk and LBS provider trust.

**H6:** Use context moderates the relationship between (a) perceived ability to control information and destination trust, (b) perceived ability to control information and LBS provider trust.

## **2.7. Privacy violation experience**

A social contract is initiated when a user provides their information to service providers or online companies. An understood social contract is that the organization will be responsible for managing the user's personal information ethically and adequately (Phelps et al., 2000). A user can perceive that their privacy is violated if their personal information or data is exploited or the social contract is breached (Culnan, 1995; Phelps et al., 2000). Users learn from their personal experiences, and a negative experience can lead to mistrust of websites that solicit or provide the same service and require similar information (Mosteller & Poddar, 2017). Users who have been a victim of personal information privacy violation have more vital privacy violation concern (Xu et al., 2011). Therefore, we hypothesize:

**H7:** Privacy violation experience moderates the relationship between (a) privacy concern and destination trust, (b) privacy concern and LBS provider trust.

**H8:** Privacy violation experience moderates the relationship between (a) perceived risk and destination trust, (b) perceived risk and LBS provider trust.

**H9:** Privacy violation experience moderates the relationship between (a) perceived ability to control information and destination trust, (b) perceived ability to control information and LBS provider trust.

## **2.8. Trust and behavioural intention**

Trust, in general, can be perceived as a positive perception, belief, and attitude towards another party (Taylor et al., 2009). Trust is defined as the ability to depend and have confidence in an exchange partner (Moorman et al., 1993). Trust is related to belief in an exchange partner's credibility, integrity, and reliability (Doney & Cannon, 1997). In the service organization, there is a need for the consumers to have trust in the service provider (Wang & Lin, 2017) and the destination (Choi et al., 2016). Artigas et al. (2017) investigated destination trust. They concluded that if a destination does not have trust from the tourists, even if the touristic experience is beautiful without trust, it is useless. Destination trust is defined as the ability of the destination to provide its advertised functions (Abubakar & Ilkan, 2016). Technology users, who do not have trust in the service provider, have very high privacy concerns (Kokolakis, 2017). The behavioural intention which is the ability of a person to accomplish or perform a specific behaviour (Davis, 1989), in this study the behaviour would be for the tourist to recommend the destination to family and friends, and to revisit the destination. Therefore, we hypothesize:

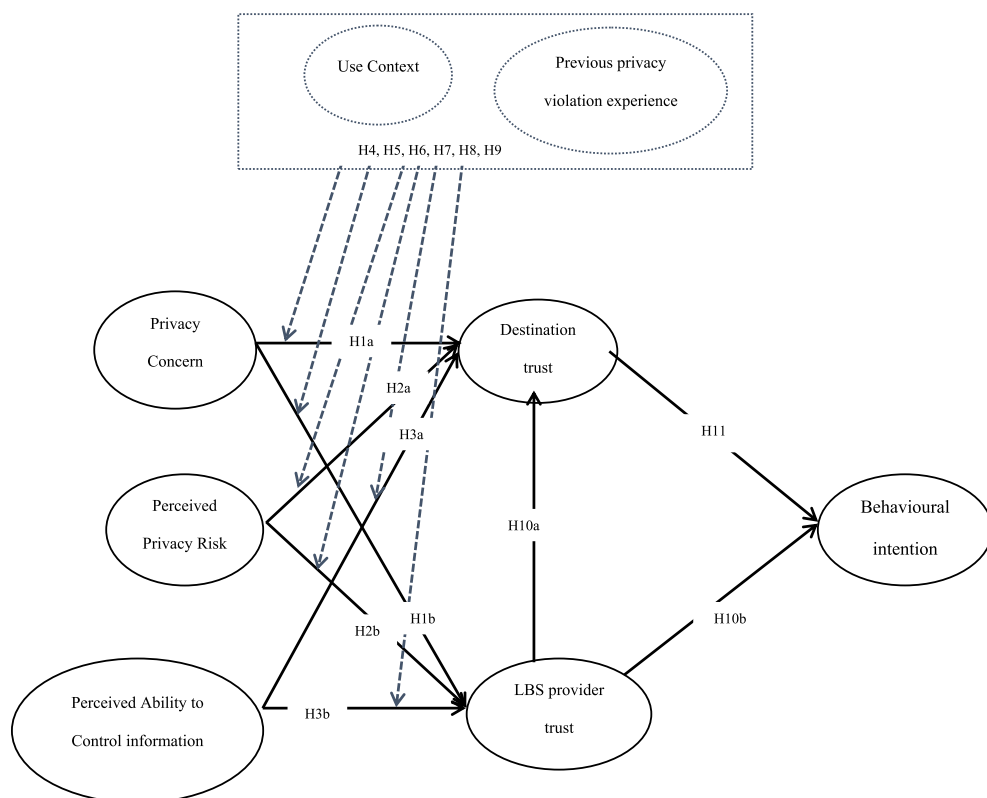
**H10:** LBS trust is positively related to (a) destination trust, (b) behavioural intention.

**H11:** Destination trust is positively related to behavioural intention.

A research model has been constructed to reflect the proposed hypotheses that are shown in [Figure 1](#).

## **2.9. Dubai**

Data was collected from tourists that have visited Dubai, a city located in the United Arab Emirates (UAE). Dubai is one of the significant and fastest developing cities in North Africa, and the Middle East, concerning economic development and growth in the tourism regions (Kaur & Maheshwari, 2016). The Government acknowledges the strategic importance of the tourism industry and how it has contributed to the economy. The smart city initiative and vision by Dubai has been the foundation for the building of a 'city of the future' using smart technologies (Efthymiopoulos, 2016). Smart tourism which is a subset of a smart city is a medium in which Dubai has used, and continues to use technology to accomplish their tourism development goals which align with the smart city initiative.



**Figure 1.** Research model. Source: Authors.

### 3. Methodology

#### 3.1. Study setting

The study was conducted using an online survey. Using an online survey for the questionnaire have been popularly used in the domain of current tourism research (Morgan-Thomas & Veloutsou, 2013). The questionnaire targeted respondents that have visited Dubai smart tourism destination in the past two years, using Instagram, and Facebook holiday pictures location tags, and also Dubai travel and tourism pages on social media. The survey starts with a question asking the respondent if they have visited Dubai and a yes or no option was provided. If the respondent chooses no, then the survey ends without any further questions, and the response is discarded. If the respondent selects yes, then a new page is opened containing the questionnaire items.

#### 3.2. Measurements

Privacy concern was measured using four items (Son & Kim, 2008), Previous privacy experience was measured using two items (Smith et al., 1996), perceived ability to control personal information was measured using four items (Liu et al., 2005). Destination trust was measured using eight items (Abubakar & Ilkan, 2016). LBS

provider trust was measured using three items (Pavlou & Gefen, 2004). The behavioural intention was measured using three items (Liu et al., 2005), perceived risk was measured using three items (Pavlou & Gefen, 2004), use context was measured using five items (Mallat et al., 2009). The items were worded to suit this study context. All the variables were measured using a 1–7 Likert scale, except destination trust was measured using a 1–5 Likert scale.

### **3.3. Data collection**

The survey was available online using google forms from February to May. A sample of 384 tourists that have visited the smart tourism destination was reached. A statistical calculation was used to choose the sample size with the Creative Research Systems (2019, <http://www.surveysystem.com/sscalc.htm>) using confidence level 95% and a significance interval of 5%, with the number of tourists visiting the smart tourism destination Dubai is millions (Tabachnick & Fidell, 2014). The sufficient number of respondents was calculated as 384. 427 respondents clicked the survey, but 43 choose no they have not been to Dubai, making their response discarded. Finally, after reaching 384 respondents that have been in Dubai and the data was extracted and used for data analysis.

### **3.4. Data validity and reliability**

Results of Confirmatory factor analysis performed in AMOS 20.0 showed that all items converged on their underlying construct except for one item from destination trust and one item from behavioural intention construct which was discarded. The model fit statistics ( $\chi^2 = 891.933$ ,  $df = 375$ ,  $\chi^2/df = 2.38$ ; CFI = 0.96; PNFI = 0.80; RMSEA = 0.060) indicated a good fit and all standardized loadings exceeded the minimum requirement of 0.5, the t-statistics of all loaded factors is greater than 1.96, thus, confirming convergent validity. Composite reliability (CR) score and average variance extracted (AVE) for each construct were above the 0.7, and 0.5 minimum required values, respectively. Table 1 shows the details. Further, we performed a bivariate Pearson correlation with a 2-tailed significant test. The result, as shown in Table 2, indicates that all constructs are moderately correlated. The diagonal figures represent the square root of AVE, which is greater than the inter-construct correlation, thus confirming the discriminant validity of the data (Chih & Lin, 2019). Preliminary checks of the data provided an initial understanding of the significance of the study variables.

## **4. Results**

### **4.1. Respondents profile**

Table 3 shows the demographic profile of the respondents. Majority of the respondents, 42% are 30 years or older. In terms of gender, the distribution is almost equal with the females slightly more than the males at fifty-two per cent. The respondents are quite educated as the majority of them (73.3%) are graduated from either



**Table 1.** Scale items and measurement properties.

Construct and items	Standardized loadings	t-values	AVE	CR	$\alpha$
<b>Destination trust</b>			0.701	0.942	0.94
I feel confident in Dubai as a smart tourism destination	.867	18.562			
Dubai tourism destination guarantees satisfaction	.906	25.226			
Dubai as a smart tourism destination meets my expectation	.820	30.884			
Dubai as a tourism destination would make an effort to satisfy me	.850	22.221			
I was not disappointed with Dubai tourism services	.804	20.107			
Dubai smart tourism destination would be honest and sincere in addressing my concerns	.823	20.975			
I could depend on Dubai as a tourism destination to meet all my touristic needs	.783	19.233			
Dubai as a tourism destination would compensate me in some way in case of data misuse	–				
<b>Privacy concern</b>			0.876	0.966	0.97
I am concerned that the information about me which is private can be found by another person on the Internet	.922	32.382			
I am concerned about what other people might do to my information which is private if I provide them to service providers	.948	35.304			
I am concerned that my information which is personal would be used in a way I did not permit by the service providers	.934	33.529			
I am concerned about misuse of my information which is disclosed to service providers	.940	34.224			
<b>Use context</b>			0.710	0.923	0.92
I use location based services in a destination if using location based services is the best way to get to my destination	.955	18.326			
I use location based services in a destination if I am in a hurry to get to my destination	.918	34.533			
I use location based services in a destination if I do not know where I am going	.926	35.652			
I use location based services in a destination if using location based services would not cost me money	.747	20.129			
I use location based services in a destination if my location information has no value	.616	14.472			
<b>Perceived ability to control personal information</b>			0.698	0.901	0.90
The service provider explained the reason my personal/private information is being collected at any time	.915	20.258			
The service provider describes how personal information about me would be collected and used	.919	27.896			
I am aware of the personal information the service provider would collect about me	.821	22.227			
The service provider gives me an option to accept or decline before using my personal information	.661	15.311			
<b>Perceived risk</b>			0.891	0.961	0.96
There will be much uncertainty associated with providing personal information to service provider	.967	34.264			

*(continued)*

**Table 1.** Continued.

Construct and items	Standardized loadings	t-values	AVE	CR	$\alpha$
There will be much potential loss associated with providing personal information to service provider	.928	38.397			
It is risky to provide personal information to service provider	.937	40.103			
<b>Location based service (LBS) provider trust</b>			0.886	0.959	0.96
The service provider in the smart tourism destination keeps its promise	.975	33.375			
The service provider in the smart tourism destination is trustworthy	.926	39.309			
The service provider in the smart tourism destination keeps tourists interest in mind	.922	38.431			
<b>Previous privacy experience</b>			0.637	0.778	0.78
How often have you personally been a victim of what you felt was an invasion of privacy	.763	10.256			
How often have you heard or read during the last year about the use and potential misuse of personal information about tourists	.832	14.235			
<b>Behavioural intention</b>			0.761	0.864	0.91
I would revisit Dubai tourism destination	.834	15.369			
I would recommend Dubai as a tourism destination to my friends	.909	19.591			
I have positive things to say about this tourism destination	---				

Model fit statistics:  $\chi^2 = 891.933$ ,  $df = 375$ ,  $\chi^2/df = 2.38$ ; CFI = 0.96; PNFI = 0.80; RMSEA = 0.060.  
 Notes: All loadings were significant. AVE = Average variance extracted; CR = Composite reliability; CFI = Comparative fit index; PNFI = Parsimony normed fit index; RMSEA = Root mean square error of approximation.  
 Source: Authors.

**Table 2.** Descriptive statistics and correlation of observed variables.

Constructs	Age	Gender	Education	Income	PPE	DESTTR	PC	UCT	PCTRL	RISK	LBSTRU	BI
Age												
Gender	.068											
Education	.362**	.131*										
Income	.450**	.103*	.226**									
PPE	.086	.039	.039	-.030	<b>0.798</b>							
DESTTR	-.153**	-.107*	-.060	-.126*	-.310**	<b>0.837</b>						
PC	.230**	.107*	.058	.148**	.0597**	-.321**	<b>0.936</b>					
UCT	-.215**	-.138**	-.042	-.139**	-.096*	0.457**	-.150**	<b>0.843</b>				
PCTRL	-.361**	-.134**	-.096	-.242**	0.014	0.366**	-.232**	0.385**	<b>0.836</b>			
RISK	.230**	.033	.075	.228**	0.523**	-.252**	0.656**	-.0171**	-.246**	<b>0.944</b>		
LBSTRU	-.334**	-.151**	-.116*	-.260**	-.164**	0.591**	-.394**	0.383**	0.493**	-.326**	<b>0.941</b>	
BI	-.205**	-.116*	-.106*	-.154**	-.304**	0.723**	-.250**	0.407**	0.286**	-.216**	0.534**	<b>0.872</b>
Mean	2.77	1.52	2.87	5.34	3.25	4.15	4.98	5.76	4.08	4.94	4.54	5.80
STD	1.84	0.50	1.00	3.32	1.88	0.812	1.90	1.34	1.67	1.76	1.54	1.42

Notes. (2-tailed test); Square root of AVE is given in bold face across the diagonal; PPE = Previous privacy experience; DESTTR = destination trust; PC = privacy concern; UCT = use context; PCTRL = perceived ability to control information; RISK = perceived privacy risk; LBSTRU = location-based service provider trust; BI = behavioural intention.  
 \*\*p < 0.001.  
 \*p < 0.005.  
 Source: Authors.

university or hold a graduate certificate. (55.2%) are first-time visitors to the smart destination. The full demographic profile of the respondents is shown in Table 3.

**4.2. Hypothesis testing**

To test hypotheses H1 to H3, linear regression analysis (LRA) was performed using SPSS. In the first linear regression equation (LRE), privacy concern negatively and

**Table 3.** Respondents' profile (n = 384).

	Frequency	%
<b>Age</b>		
18–23	133	34.6
24–29	93	24.2
30–34	36	9.4
35–40	27	7.0
41–46	40	10.4
47 above	55	14.3
<b>Gender</b>		
Male	183	47.7
Female	201	52.3
<b>Education</b>		
High school	53	13.8
College (two-year program)	60	15.6
University (four-year program)	152	39.6
Graduate degree (masters or PhD)	119	33.7
<b>Frequency of visit</b>		
First time (once)	212	55.2
Second time (twice)	71	18.5
More than twice	101	26.3
<b>Nationality</b>		
Nigeria	99	25.8
United Kingdom	34	8.9
United States	31	8.1
Turkey	19	4.9
Kenya	19	4.9
Ghana	17	4.4
Pakistan	14	3.6
Iran	12	3.1
Zimbabwe	12	3.1
Oman	10	2.6
Others	117	30.6

Source: Authors.

significantly predicted destination trust,  $R^2 = .103$ ,  $R^2_{adj} = .101$ ,  $F(1, 382) = 43.81$ ,  $p < .001$ . In the second equation, privacy concern negatively and significantly predicted LBS provider trust,  $R^2 = .155$ ,  $R^2_{adj} = .153$ ,  $F(1, 382) = 70.09$ ,  $p < .001$ . Thus, H1a and H1b were supported.

To test hypotheses 2. In the first LRE, perceived privacy risk negatively and significantly predicted destination trust,  $R^2 = .064$ ,  $R^2_{adj} = .061$ ,  $F(1, 382) = 25.95$ ,  $p < .001$ . In the second equation, perceived privacy risk negatively and significantly predicted LBS provider trust,  $R^2 = .106$ ,  $R^2_{adj} = .104$ ,  $F(1, 382) = 45.49$ ,  $p < .001$ . Thus, H2a and H2b were supported.

To test the positive effect of information control, in the first linear regression equation, PCTRL positively and significantly predicted destination trust,  $R^2 = .134$ ,  $R^2_{adj} = .132$ ,  $F(1, 382) = 59.01$ ,  $p < .001$ . In the second equation, PCTRL positively and significantly predicted LBS provider trust,  $R^2 = .243$ ,  $R^2_{adj} = .241$ ,  $F(1, 382) = 122.50$ ,  $p < .001$ . Thus, H3a and H3b were supported.

### 4.3. Moderation

For the investigation of hypotheses H4 to H9, we performed a number of moderated hierarchical regression analyses (HRA). To minimize the potential of multicollinearity issue, all predicting variables were mean-centred before the cross-products of the

predictors were computed for the examination of all interaction effects (Aiken et al., 1991).

The first HRA where privacy concern  $\times$  context interaction predicted destination trust showed 27.2% ( $R^2_{adj}$ ) of the change in the regression equation,  $F(3, 380) = 48.81$ ,  $p < .001$ . The initial step (concern) showed 10.1% of the change,  $F(1, 382) = 43.81$ ,  $p < .001$ , although in the second step, context showed 17.1% of the change,  $F(1, 381) = 90.00$ ,  $p < .001$ . The privacy concern  $\times$  context interaction in the third step showed an added .04%,  $F(1, 380) = 2.02$ ,  $p = .16$ , of the total change. The results showed that there exists main influence of privacy concern ( $\beta = -.25$ ,  $p < .001$ ) and context ( $\beta = .43$ ,  $p < .001$ ), and the partially significant interaction influence of privacy concern  $\times$  context ( $\beta = -.06$ ,  $p < .16$ ). Thus, the partial significant interaction indicates that high use context reduces the negative effect of privacy concern on destination trust. Therefore, H4a was supported.

In the second HRA, the interaction between privacy concern  $\times$  context predicted LBS provider trust. The total model showed 25.7% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 383) = 45.10$ ,  $p < .001$ . Privacy concern in the initial step showed 15.3% of the change,  $F(1, 382) = 70.09$ ,  $p < .001$ , although in the second step use context showed 10.70% of the change,  $F(1, 381) = 55.45$ ,  $p = .001$ , finally the interaction privacy concern  $\times$  context showed an added 0.1% of the total change,  $F(1, 380) = 8.63$ ,  $p < .75$ . The results demonstrated a main effect of the privacy concern ( $\beta = -.34$ ,  $p < .01$ ) and use context ( $\beta = .33$ ,  $p < .01$ ) variables. However, the interaction effect of privacy concern  $\times$  context was not statistically significant. Therefore, H4b was not supported.

For testing hypothesis 5, the first HRA, the interaction between perceived privacy risk  $\times$  context predicted destination trust, showed 27.2% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 380) = 25.95$ ,  $p < .001$ . The first step (risk) showed 6.1% of the change,  $F(1, 382) = 43.81$ ,  $p < .001$ , although in the second step, context showed 17.7% of the change,  $F(1, 381) = 88.68$ ,  $p < .001$ . The perceived privacy risk  $\times$  context interaction in the third step showed an additional 3.7%,  $F(1, 380) = 19.53$ ,  $p = .001$ , of the total change. The results indicate that there were main effects of perceived privacy risk ( $\beta = -.71$ ,  $p < .001$ ) and context ( $\beta = .44$ ,  $p < .001$ ), and a significant interaction effect of perceived privacy risk  $\times$  context ( $\beta = -.91$ ,  $p < .001$ ). The significant interaction indicated that the negative relation between privacy risk and destination trust was weaker when the use context levels were high; therefore, H5a was supported.

In the second HRA, the perceived privacy risk  $\times$  context interaction was used to predict LBS provider trust. The total model showed 21.5% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 383) = 67.27$ ,  $p < .001$ . Perceived privacy risk in the first step showed 10.6% of the change,  $F(1, 382) = 45.49$ ,  $p < .001$ , whereas in the second step context showed 11.0% of the change,  $F(1, 381) = 53.62$ ,  $p = .001$ . Finally the interaction perceived privacy risk  $\times$  context showed an added 0.4% of the total change,  $F(1, 380) = 2.08$ ,  $p < .15$ . The results established a main effect of the perceived privacy risk ( $\beta = -.32$ ,  $p < .01$ ) and context ( $\beta = -.27$ ,  $p < .01$ ) variables; the effect of privacy risk  $\times$  context interaction was significant statistically ( $\beta = -.30$ ,  $p < .15$ ). The significant interaction indicated that high use context weakens the negative privacy risk–LBS provider trust relation. Therefore, H5b was supported.

The first HRA where perceived ability to control  $\times$  context interaction predicted destination trust showed 24.9% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 380) = 43.43, p < .001$ . The initial step (control) showed 13.2% of the change,  $F(1, 382) = 59.01, p < .001$ , although in the second step, context showed 11.8% of the change,  $F(1, 381) = 59.94, p < .001$ ; the interaction perceived ability to control information  $\times$  context in the third step showed an added .4%,  $F(1, 380) = 1.94, p = .16$ , of the total change. The results indicate there were direct effects of PCTRL ( $\beta = .37, p < .001$ ) and context ( $\beta = .22, p < .001$ ), and a non-significant interaction effect of PCTRL  $\times$  context. The result shows that PCTRL and use context individually exert a significant effect on destination trust. The non-significant interaction effect indicated that the effect of the ability to control information – destination trust was unaffected by changes in levels of use context.

In the second HRA, the perceived ability to control information  $\times$  context interaction was used to predict LBS provider trust. The total model showed 28.2% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 383) = 51.22, p < .001$ . PCTRL in the first step showed 24.3% of the change,  $F(1, 382) = 122.50, p < .001$ , although in the second step context showed 4.3% of the change,  $F(1, 381) = 23.44, p = .001$ , and finally the interaction PCTRL  $\times$  context showed an added 0.1% of the total change,  $F(1, 380) = .68, p < .42$ . The results established a main effect of the PCTRL ( $\beta = .26, p < .01$ ) and context ( $\beta = -.24, p < .01$ ) variables; the effect of PCTRL  $\times$  context interaction was not statistically significant. The non-significant interaction effect, indicated that changes in levels of use context did not alter the control–LBS provider trust relation. Thus, hypothesis 6a and 6b were rejected. See [Table 4](#) for the moderated regression results.

Hypotheses H7, to H9 constructed to investigate the moderating effect of previous privacy experience on the mean-centred predictors and dependent variables.

In hypotheses H7, in the initially moderated regression, privacy concern  $\times$  experience interaction predicted destination trust showed 12.5% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 380) = 19.19, p < .001$ . The initial step (concern) showed 10.1% of the change,  $F(1, 382) = 43.81, p < .001$ , although in the second step, previous experience showed 2.2% of the change,  $F(1, 381) = 9.52, p < .002$ ; the interaction privacy concern  $\times$  previous experience in the third step showed an added 0.7%,  $F(1, 380) = 2.99, p = .08$ , of the total change. The results establish that there were main effects of privacy concern ( $\beta = -.15, p < .001$ ) and previous experience ( $\beta = -.24, p < .001$ ), and a partially significant effect of privacy concern  $\times$  previous experience interaction ( $\beta = -.10, p < .08$ ).

In the subsequent HRA, privacy concern  $\times$  previous experience interaction were used to predict LBS provider trust. The total model showed 16.0% ( $R^2_{adj}$ ) of the change in the regression equation,  $F(3, 383) = 25.27, p < .001$ . Privacy concern in the first step showed 15.3% of the change,  $F(1, 382) = 70.08, p < .001$ , although in the second step previous experience showed 0.8% of the change,  $F(1, 381) = 3.61, p = .05$ . Finally the interaction privacy concern  $\times$  experience showed an added 0.3% of the total change,  $F(1, 380) = 1.53, p < .22$ . The results established a main effect of the privacy concern ( $\beta = -.42, p < .01$ ) and experience ( $\beta = .11, p < .05$ ) variables; the effect of privacy concern  $\times$  experience interaction was however partially

**Table 4.** Moderated hierarchical regression analyses of context predicting destination trust and location base trust.

Variables	Model 1( $\beta$ )		Model 2( $\beta$ )		Model 3( $\beta$ )	
	DESTTRU	LBSTRU	DESTTRU	LBSTRU	DESTTRU	LBSTRU
Privacy Concerns	-.321**	-.394**	-.258**	-.344**	-.248**	-.342**
Context			.419**	.331**	.425**	.333**
Privacy concerns X Context					-.063	-.014
R <sup>2</sup>	.103	.155	.274	.262	.278	.263
Change in R <sup>2</sup>			.171	.107	.004	.001
Change in F			90.005	55.453	2.021	.098
Significant F change (p <)			.001	.001	.156	.754
Perceived Privacy Risk	-.252**	-.326**	-.179**	-.268**	.708**	.032
Context			.427**	.337**	.435**	.340**
Perceived Privacy Risk X Context					-.906**	-.307*
R <sup>2</sup>	.064	.106	.240	.217	.278	.221
Change in R <sup>2</sup>			.177	.110	.037	.004
Change in F			88.680	53.617	19.530	2.078
Significant F change (p <)			.001	.001	.001	.150
Perceived ability to Control Info	.336**	.493**	.223**	.405**	-.039	.257**
Context			.372**	.227**	.393**	.239**
Perceived ability to Control Info X Context					.261	.149
R <sup>2</sup>	.134	.243	.252	.287	.255	.288
Change in R <sup>2</sup>			.118	.044	.003	.001
Change in F			59.935	23.446	1.935	.658
Significant F change (p <)			.001	.001	.164	.418

Note. (2-tailed test). DESTTRU (Destination Trust), LBSTRU (location based service provider trust).

\*\*p < 0.001.

\*p < 0.005.

Source: Authors.

statistically significant ( $\beta = -.07$ ,  $p < .22$ ). The partially significant interaction shows that the negative privacy concern-LBS provider trust relation was slightly strengthened by previous privacy experience. Thus, H7a and H7b were supported.

For hypothesis H8 in the initially moderated regression, perceived privacy risk  $\times$  experience interaction predicted destination trust showed 14.7% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 380) = 22.94$ ,  $p < .001$ . The initial step (risk) showed 6.1% of the change,  $F(1, 382) = 25.95$ ,  $p < .001$ . In the second step, previous experience showed 4.4% of the change,  $F(1, 381) = 18.65$ ,  $p < .001$ ; the interaction perceived privacy risk  $\times$  previous experience in the third step showed an added 4.6%,  $F(1, 380) = 20.64$ ,  $p = .001$ , of the total change. The results established there were main effects of perceived privacy risk ( $\beta = -.25$ ,  $p < .001$ ) and experience ( $\beta = -.31$ ,  $p < .001$ ), and a significant effect of perceived privacy risk  $\times$  previous experience interaction ( $\beta = .23$ ,  $p < .001$ ). The significant interaction effect indicated that the negative risk-destination trust relation was strengthened in situations with previous experiences.

In the subsequent HRA, perceived privacy risk, experience, and the interaction perceived privacy risk  $\times$  experience was used to predict LBS provider trust. The total model showed 15.4% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 383) = 24.18$ ,  $p < .001$ . Perceived privacy risk in the initial step showed 10.4% of the change,  $F(1, 382) = 45.49$ ,  $p < .001$ , although in the second step previous experience showed 0.2% of the change,  $F(1, 381) = 0.029$ ,  $p = .87$ . Finally, the interaction perceived privacy risk  $\times$  previous experience showed an added 5.2% of the total change,  $F(1,$

**Table 5.** Moderated hierarchical regression analyses of previous privacy experience (PPE) predicting destination trust and location base trust.

Variables	Model 1 ( $\beta$ )		Model 2 ( $\beta$ )		Model 3 ( $\beta$ )	
	DESTTRU	LBSTRU	DESTTRU	LBSTRU	DESTTRU	LBSTRU
Privacy Concerns	-.321**	-.394**	-.211**	-.460**	-.146**	-.415**
PPE			-.184**	.111*	-.235**	.076
Privacy concerns X PPE					.098*	.069
R <sup>2</sup>	.103	.155	.125	.163	.132	.166
Change in R <sup>2</sup>			.022	.008	.007	.003
Change in F			9.516	3.606	2.989	1.530
Significant F change ( $p <$ )			.002	.058	.085	.217
Perceived Privacy Risk	-.252**	-.326**	-.124**	-.331**	-.026	-.225**
PPE			-.245**	.010	-.309**	-.059
Perceived Privacy Risk X PPE					.231**	.249**
R <sup>2</sup>	.064	.106	.107	.106	.153	.160
Change in R <sup>2</sup>			.044	.000	.046	.054
Change in F			18.654	.029	20.642	24.360
Significant F change ( $p <$ )			.001	.865	.001	.001
Perceived Ability to Control Info	.366**	.493**	.362**	.491**	.348**	.473**
PPE			-.305**	-.157**	-.319**	-.169**
Perceived Ability to Control Info X PPE					.107**	.092**
R <sup>2</sup>	.134	.243	.227	.267	.238	.276
Change in R <sup>2</sup>			.093	.025	.011	.008
Change in F			45.853	12.788	5.543	4.291
Significant F change ( $p <$ )			.001	.001	.019	.039

Notes.(2-tailed test). DESTTRU (Destination Trust), LBSTRU (location based service provider trust).

\*\* $p < 0.001$ .

\* $p < 0.005$ .

Source: Authors.

380) = 24.36,  $p < .001$ . The results established a main effect of the perceived privacy risk ( $\beta = -.23$ ,  $p < .01$ ) and previous experience ( $\beta = -.06$ ,  $p < .04$ ) variables; the effect of privacy risk  $\times$  previous experience interaction was statistically significant ( $\beta = .25$ ,  $p < .001$ ). The significant interaction indicated that the negative privacy risk-LBS provider trust relation was strengthened by previous experience of an information violation. Thus, H8a and H8b were supported.

In hypothesis H9, the PCTRL  $\times$  experience interaction predicted destination trust showed 23.2% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 380) = 39.56$ ,  $p < .001$ . The initial step (control) showed 13.2% of the change,  $F(1, 382) = 59.01$ ,  $p < .001$ , although in the second step, previous experience showed 9.3% of the change,  $F(1, 381) = 45.85$ ,  $p < .001$ ; the interaction PCTRL  $\times$  experience in the third step showed an added 1.1%,  $F(1, 380) = 5.54$ ,  $p = .01$ , of the total change. The results show there were main effects of PCTRL ( $\beta = .35$ ,  $p < .001$ ) and experience ( $\beta = -.32$ ,  $p < .001$ ), and a significant interaction effect of PCTRL  $\times$  experience ( $\beta = .11$ ,  $p < .01$ ). The significant interaction effect indicated that the positive control-destination trust relation was weakened in situations with previous privacy experiences.

In the subsequent hierarchical regression analysis, the PCTRL  $\times$  experience interaction was used to predict LBS provider trust. The total model showed 27.0% ( $R^2_{adj}$ ) of the change in the regression comparison,  $F(3, 383) = 83.92$ ,  $p < .001$ . PCTRL in the initial step shows 24.1% of the change,  $F(1, 382) = 122.5$ ,  $p < .001$ , although in

the second step previous experience showed 2.5% of the change,  $F(1, 381) = 12.79$ ,  $p = .001$ . Finally, the interaction  $PCTRL \times$  previous experience showed an added 0.8% of the total change,  $F(1, 380) = 4.29$ ,  $p < .04$ . The results established a main effect of the perceived control ( $\beta = -.48$ ,  $p < .01$ ) and previous experience ( $\beta = -.17$ ,  $p < .001$ ) variables; the interaction effect of  $PCTRL \times$  experience was statistically significant ( $\beta = .09$ ,  $p < .001$ ). The significant interaction indicated that the positively perceived ability to control-LBS provider trust relation was weakened by previous violation experience. Thus, H9a and H9b were supported. Overall, hypotheses H7, H8, and H9 were supported. See Table 5 for the moderated regression results.

For Hypotheses H10 a simple LRA was conducted. In the first linear regression equation, LBS provider trust positively and significantly predicted destination trust,  $R^2 = .349$ ,  $R^2_{adj} = .347$ ,  $F(1, 382) = 204.83$ ,  $p < .001$ . In the second equation, LBS provider trust positively and significantly predict tourists' behavioural intention,  $R^2 = .285$ ,  $R^2_{adj} = .283$ ,  $F(1, 382) = 151.99$ ,  $p < .001$ . Thus, H10a and H10b were supported.

Hypothesis H11 proposed a direct effect of destination trust on behavioural intention. The result indicated that destination trust positively and significantly predicted tourist's behavioural intention to a smart destination,  $R^2 = .523$ ,  $R^2_{adj} = .522$ ,  $F(1, 382) = 418.43$ ,  $p < .001$ . Therefore, hypothesis H11 was supported.

## 5. Discussions and conclusions

The destination management organization (DMO), the service provider, and the tourist are three major stakeholders that are involved in smart tourism destinations (Femenia-Serra, 2018). This study provides implications for smart tourism DMO's, technology service providers, and for smart tourism destination stakeholders. Building trust with service providers is essential for the development and sustainability of a smart tourism destination. As the results of this study have shown that trust in the service provider would influence trust in the destination and influence tourists to revisit and recommend the destination.

Information privacy risk and privacy concern of mobile application LBS are negatively related to destination and service provider trust. This result is consistent with previous studies on privacy concern and perceived risk relationship to trust, in the context of mobile advertising (Okazaki et al., 2012), in the context of mobile hotel booking (Ozturk et al., 2017) and the context LBS adoption (Zhou, 2012). The service providers and DMO's in smart tourism destinations should take effective measures to mitigate this concern when implementing and developing mobile LBS in the tourism destination. This can be done by providing better security and privacy settings for the tourist; they should always emphasize and guarantee confidentiality, and creating more user-friendly applications with manuals and user guides with different language options.

Alternatively, information control has been seen to be positively related to trust. This result is consistent with previous studies on control and trust as providing an equitable relationship (Mosteller & Poddar, 2017). The destination managers, service providers, and other stakeholders in the smart tourism destination should work



together with software developers towards developing software applications used in the destination with the control where the users can accept or decline for their information to be used, and understand how and why their information is used.

Additionally, the results of this study have shown that privacy concern and privacy risk can be mitigated with the use context. DMO's should emphasize the importance, purpose, and use of personal information and technology in smart tourism destinations. For instance, if the service provider informs the tourist how their location information is used to help them find their way if they get lost, they would reduce the privacy concern of the tourist towards their location data collection. Future studies should further investigate use-context mitigation of user's privacy concern as to how to mitigate the effect of privacy concern seems to be a black box (Zhou, 2016)

Furthermore, this study provides implications for service providers as regards use context for technology adoption. Service providers need to keep track of tourists' behaviour and usage when it comes to using LBS. They should consider the time, the availability, the place, the convenience, the social and environmental factors that influence the usage of LBS by the tourists. This can help them provide advertisements, alerts, and personalization that would not be intrusive to the tourists. They can also be able to understand the challenges that the tourist faces when using mobile application location based services under different contexts (Kim et al., 2019).

Finally, the results showed that location-based service provider trust is positively related to destination trust and behavioural intention. When there is trust in the service provider, there would be trust in the destination, and it would lead to positive behaviour intentions, which makes service provider trust in a smart tourism destination important.

### **5.1. Limitations and future research**

One of the limitations of this study is its focus on the privacy concern of mobile application LBS. However, there are different technologies used in smart tourism destinations. Future studies can research the privacy concern of tourists towards the other mobile technologies different from location-based services used in the smart tourism destination and the effects on service providers. The results of this study have shown that previous violation experience negatively influences user beliefs towards trust in a smart tourism destination and location-based service provider. Future studies can consider a longitudinal study comparing if a violation in one smart tourism destination influences privacy concern in another smart tourism destination. Finally, the influence of use context can also be studied concerning the privacy paradox.

### **Disclosure statement**

No potential conflict of interest was reported by the authors.

### **ORCID**

Ali Ozturen  <http://orcid.org/0000-0001-8879-1916>

## References

- Abubakar, A. M., & Ilkan, M. (2016). Impact of online WOM on destination trust and intention to travel: A medical tourism perspective. *Journal of Destination Marketing & Management*, 5(3), 192–201. <https://doi.org/10.1016/j.jdmm.2015.12.005>
- Afolabi, O. O., Adeshola, I., Ozturen, A., & Ilkan, M. (2020). The influence of context on privacy concern in smart tourism destinations. *PEOPLE: International Journal of Social Sciences*, 6(1), 282–293. <https://doi.org/10.20319/pijss.2020.61.282293>
- Aiken, L. S., West, S. G., & Reno, R. R. (1991). *Multiple regression: Testing and interpreting interactions*. Sage.
- Artigas, E. M., Yrigoyen, C. C., Moraga, E. T., & Villalón, C. B. (2017). Determinants of trust towards tourist destinations. *Journal of Destination Marketing & Management*, 6(4), 327–334. <https://doi.org/10.1016/j.jdmm.2017.03.003>
- Bandura, A. (1989). Human agency in social cognitive theory. *The American Psychologist*, 44(9), 1175–1184. <https://doi.org/10.1037/0003-066x.44.9.1175>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 24(6), 624–644. <https://doi.org/10.1057/ejis.2014.41>
- Boateng, H., Adam, D. R., Okoe, A. F., & Anning-Dorson, T. (2016). Assessing the determinants of internet banking adoption intentions: A social cognitive theory perspective. *Computers in Human Behavior*, 65, 468–478. <https://doi.org/10.1016/j.chb.2016.09.017>
- Buhalis, D., & Amaranggana, A. (2015). Smart tourism destinations enhancing tourism experience through personalization of services. In *Information and communication technologies in tourism 2015* (pp. 377–389). Cham: Springer.
- Buhalis, D., & Foerste, M. (2015). SoCoMo marketing for travel and tourism: Empowering co-creation of value. *Journal of Destination Marketing & Management*, 4(3), 151–161. <https://doi.org/10.1016/j.jdmm.2015.04.001>
- Buonincontri, P., & Micera, R. (2016). The experience co-creation in smart tourism destinations: A multiple case analysis of European destinations. *Information Technology & Tourism*, 16(3), 285–315. <https://doi.org/10.1007/s40558-016-0060-5>
- Chang, C. C. (2015). Exploring mobile application customer loyalty: The moderating effect of use contexts. *Telecommunications Policy*, 39(8), 678–690. <https://doi.org/10.1016/j.telpol.2015.07.008>
- Chang, S. E., & Shen, W. C. (2018). Exploring smartphone social networking services for mobile tourism. *International Journal of Mobile Communications*, 16(1), 63–81. <https://doi.org/10.1504/IJMC.2018.088273>
- Chih, C., & Lin, C. P. (2019). The impact of employees' perceptions of HR practices on identification with the company and citizenship behaviour. *Employee Relations: The International Journal*, 42(6), 1238–1255. <https://doi.org/10.1108/ER-08-2018-0217>
- Choe, Y., & Fesenmaier, D. R. (2017). The quantified traveler: Implications for smart tourism development. In *Analytics in smart tourism design* (pp. 65–77). Cham: Springer.
- Choi, M., Law, R., & Heo, C. Y. (2016). Shopping destinations and trust–tourist attitudes: Scale development and validation. *Tourism Management*, 54, 490–501. <https://doi.org/10.1016/j.tourman.2016.01.005>
- Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, 9(2), 10–19. <https://doi.org/10.1002/dir.4000090204>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- De Reuver, M., Ongena, G., & Bouwman, H. (2013). Should mobile Internet be an extension to the fixed web? Fixed-mobile reinforcement as mediator between context of use and future use. *Telematics and Informatics*, 30(2), 111–120. <https://doi.org/10.1016/j.tele.2012.02.002>

- Del Chiappa, G., & Baggio, R. (2015). Knowledge transfer in smart tourism destinations: Analyzing the effects of a network structure. *Journal of Destination Marketing & Management*, 4(3), 145–150. <https://doi.org/10.1016/j.jdmm.2015.02.001>
- Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of Marketing*, 61(2), 35–51.
- Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: The case of Dubai. *Journal of Innovation and Entrepreneurship*, 5(1), 11. <https://doi.org/10.1186/s13731-016-0036-x>
- Femenia-Serra, F. (2018). Smart tourism destinations and higher tourism education in Spain. Are we ready for this new management approach? In *Information and communication technologies in tourism 2018* (pp. 437–449). Cham: Springer.
- Femenia-Serra, F., Neuhofer, B., & Ivars-Baidal, J. A. (2019). Towards a conceptualization of smart tourists and their role within the smart destination scenario. *The Service Industries Journal*, 39(2), 109–133. <https://doi.org/10.1080/02642069.2018.1508458>
- Font, X., Garay, L., & Jones, S. (2016). A social cognitive theory of sustainability empathy. *Annals of Tourism Research*, 58, 65–80. <https://doi.org/10.1016/j.annals.2016.02.004>
- Garcia, A., Linaza, M. T., Gutierrez, A., & Garcia, E. (2019). Gamified mobile experiences: Smart technologies for tourism destinations. *Tourism Review*, 74(1), 30–49. <https://doi.org/10.1108/TR-08-2017-0131>
- Gambino, A., Kim, J., Sundar, S. S., Ge, J., & Rosson, M. B. (2016, May). *User disbelief in privacy paradox: Heuristics that determine disclosure* [Paper presentation]. Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA (pp. 2837–2843). ACM. <https://doi.org/10.1145/2851581.2892413>
- Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, 133(1), 111–123. <https://doi.org/10.1007/s10551-014-2346-x>
- Hoffmann, C. P., Lutz, C., & Meckel, M. (2015). Content creation on the Internet: A social cognitive perspective on the participation divide. *Information, Communication and Society*, 18(6), 696–716. <https://doi.org/10.1080/1369118X.2014.991343>
- Huete Alcocer, N., & López Ruiz, V. R. (2019). The role of destination image in tourist satisfaction: The case of a heritage site. *Economic Research-Ekonomska Istraživanja*, 33, 1–18.
- Kaur, M. J., & Maheshwari, P. (2016, March). *Building smart cities applications using IoT and cloud-based architectures* [Paper presentation]. 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), Sharjah, United Arab Emirates (pp. 1–5). IEEE. <https://doi.org/10.1109/ICCSII.2016.7462433>
- Khan, M., Woo, M., Nam, K., & Chathoth, P. (2017). Smart city and smart tourism: A case of Dubai. *Sustainability*, 9(12), 2279. <https://doi.org/10.3390/su9122279>
- Kim, J., Chang, Y., Chong, A. Y. L., & Park, M. C. (2019). Do perceived use contexts influence usage behaviour? An instrument development of perceived use context. *Information and Management*, 56(7), 103155.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Kontogianni, A., & Alepis, E. (2020). Smart tourism: State of the art and literature review for the last six years. *Array*, 6, 100020. <https://doi.org/10.1016/j.array.2020.100020>
- Lin, T. T., Paragas, F., & Bautista, J. R. (2016). Determinants of mobile consumers' perceived value of location-based advertising and user responses. *International Journal of Mobile Communications*, 14(2), 99–117.
- Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—A privacy-trust-behavioural intention model of electronic commerce. *Information & Management*, 42(2), 289–304. <https://doi.org/10.1016/j.im.2004.01.003>
- Mallat, N., Rossi, M., Tuunainen, V. K., & Öörni, A. (2009). The impact of use context on mobile services acceptance: The case of mobile ticketing. *Information & Management*, 46(3), 190–195. <https://doi.org/10.1016/j.im.2008.11.008>

- Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of Marketing*, 57(1), 81–101. <https://doi.org/10.1177/002224299305700106>
- Morgan-Thomas, A., & Veloutsou, C. (2013). Beyond technology acceptance: Brand relationships and online brand experience. *Journal of Business Research*, 66(1), 21–27. <https://doi.org/10.1016/j.jbusres.2011.07.019>
- Mosteller, J., & Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviours. *Journal of Interactive Marketing*, 39, 27–38. <https://doi.org/10.1016/j.intmar.2017.02.003>
- Neuhofer, B., Buhalis, D., & Ladkin, A. (2015). Smart technologies for personalized experiences: A case study in the hospitality domain. *Electronic Markets*, 25(3), 243–254. <https://doi.org/10.1007/s12525-015-0182-1>
- Ngelambong, A., Nor, N. M., Abdullah, D., & Kamal, S. B. M. (2018). Perceived privacy concern, affective relationship trust and relationship risk in airlines brand online community: The moderating role of perceived benefit and risk-taking behaviour. *International Journal of Academic Research in Business and Social Sciences*, 8(15), 68–81.
- Okazaki, S., Navarro-Bailón, M. Á., & Molina-Castillo, F. J. (2012). Privacy concerns in quick response code mobile promotion: The role of social anxiety and situational involvement. *International Journal of Electronic Commerce*, 16(4), 91–120. <https://doi.org/10.2753/JEC1086-4415160404>
- Ooi, K. B., Hew, J. J., & Lin, B. (2018). Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach. *Behaviour & Information Technology*, 37(6), 575–595. <https://doi.org/10.1080/0144929X.2018.1465997>
- Ozturk, A. B. (2016). Customer acceptance of cashless payment systems in the hospitality industry. *International Journal of Contemporary Hospitality Management*, 28(4), 801–817. <https://doi.org/10.1108/IJCHM-02-2015-0073>
- 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>
- Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research*, 15(1), 37–59.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41. <https://doi.org/10.1509/jppm.19.1.27.16941>
- Pradhan, M., Oh, J., & Lee, H. (2018). Understanding travelers' behaviour for sustainable smart tourism: A technology readiness perspective. *Sustainability*, 10(11), 4259. <https://doi.org/10.3390/su10114259>
- Rana, N. P., & Dwivedi, Y. K. (2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). *Government Information Quarterly*, 32(2), 172–181. <https://doi.org/10.1016/j.giq.2015.02.002>
- Sample Size Calculator. (2019). Retrieved October 1, 2019, from <http://www.surveysystem.com/sscalc.htm>
- Sedarati, P., & Baktash, A. (2017). Adoption of smart glasses in smart tourism destination: A system thinking approach. Travel and Tourism Research Association: Advancing Tourism Research Globally 2017 ttra International Conference.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. <https://doi.org/10.2307/249477>
- Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(3), 503–529. <https://doi.org/10.2307/25148854>
- Tabachnick, B. G., & Fidell, L. S. (2014). *Using multivariate statistics* (New international ed.). Pearson.

- Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223. <https://doi.org/10.1007/s10660-009-9036-2>
- Van de Wijnngaert, L., & Bouwman, H. (2009). Would you share? Predicting the potential use of a new technology. *Telematics and Informatics*, 26(1), 85–102. <https://doi.org/10.1016/j.tele.2008.01.002>
- Wang, D., Xiang, Z., & Fesenmaier, D. R. (2014). Adapting to the mobile world: A model of smartphone use. *Annals of Tourism Research*, 48, 11–26. <https://doi.org/10.1016/j.annals.2014.04.008>
- Wang, E. S. T., & Lin, R. L. (2017). Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. *Behaviour and Information Technology*, 36(1), 2–10.
- Wang, J., Xie, C., Huang, Q., & Morrison, A. M. (2020). Smart tourism destination experiences: The mediating impact of arousal levels. *Tourism Management Perspectives*, 35, 100707. <https://doi.org/10.1016/j.tmp.2020.100707>
- Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. <https://doi.org/10.1016/j.dss.2010.11.017>
- Yang, J., He, J., & Gu, Y. (2012). The implicit measurement of destination image: The application of Implicit Association Tests. *Tourism Management*, 33(1), 50–52.
- Zhou, T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research*, 13(2), 135.
- Zhou, T. (2016). Understanding location-based services continuance: An IS success model perspective. *International Journal of Mobile Communications*, 14(6), 553–567. <https://doi.org/10.1504/IJMC.2016.079300>
- Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, 37, 283–289. <https://doi.org/10.1016/j.chb.2014.05.008>