



Information Privacy Behaviors during the COVID-19 Pandemic: Focusing on the Restaurant Context

Eunji Lee¹ · Jin-young Kim¹ · Junchul Kim² · Chulmo Koo¹

Accepted: 31 July 2022 / Published online: 19 August 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

The acquisition of personal information has been generally accepted in the pandemic situation as an effective measure to prevent infection, while at the same time raising concerns regarding the infringement of personal privacy. The current study aimed to propose and empirically test a research model for restaurant customers on the disclosure of personal information in a pandemic situation. Privacy calculus theory and institutional theory were applied to theoretically explain the drivers/inhibitors and behavioral responses that affect disclosure of personal information. We verified that the most influential factor on intention to disclose was “perceived benefit”, followed by “government pressure” as another strong predictor. We present theoretical and practical implications for restaurant managers and policy agencies.

Keywords Information Disclosure · Privacy Calculus Theory · Institutional Theory · COVID-19 · Threat Appraisal

1 Introduction

In response to COVID-19, various policy strategies were adopted to control community infections (Lu et al., 2020). In doing so, technology has played a significant role in managing and controlling the pandemic situation (Piccialli et al., 2022). Specifically, one of the measures introduced by many countries to control infectious diseases is “contact tracing.” Contact tracing means the “the process of identifying, assessing, and managing people who have been exposed to a contagious disease to prevent onward transmission.” (World Health Organization, 2014). The visitor QR (quick response) code system adopted in multi-use facilities is an

example of using information and communications technology for personal information collection and tracking, which has become an integral part of quarantine and monitoring strategies (Lee, 2020; Park, 2021). For example, in South Korea, visitor logs at restaurants became mandatory, and individuals’ contact information (i.e., addresses and phone number), and visit time were collected (Kim & Mah, 2020). On the other hand, in the U.S., local governments institutionalized the collection of personal information about customers at multi-use facilities (Houck, 2020). The acquisition and use of personal information are regarded as an inevitable and effective measure to prevent the spread of infection in a pandemic, but at the same time, the need for privacy protection is often overlooked (Bhatt et al., 2022). As a result, user privacy violation incidents increased exponentially during the health crisis (Brough & Martin, 2021).

In fact, privacy concerns are among the most critical issues related to personal information disclosure (PID) (Fox & James, 2021; Gasser et al., 2020; Huang et al., 2020). This topic has been recognized and examined widely since the beginning of the Information Age in the mid-1980s, resulting in active discussion about privacy, accuracy, property, and accessibility (PAPA) related to information use (Bélanger & Crossler, 2011) with a solid theoretical foundation for information privacy (Li, 2012; Bélanger & Crossler, 2011) stated that information privacy could be defined in one way as “a moral right or a legal right” and in another

✉ Chulmo Koo
helmetgu@khu.ac.kr

Eunji Lee
edreamerj@khu.ac.kr

Jin-young Kim
jk293@khu.ac.kr

Junchul Kim
junchul.kim@brunel.ac.uk

¹ Smart Tourism Education Platform (STEP), Kyung Hee University, Kyung Hee Dearo 26, Seoul, Republic of Korea

² Brunel Business School, Brunel University London, UB8 3PH London, Uxbridge, UK

way as “one’s ability to control information about oneself” (p.1018). While the concepts of information privacy may vary, it is clear that privacy issues are many and varied in nature. Therefore, information privacy has been studied not only by Information System (IS) researchers but also by researchers in marketing, management, psychology, and many other fields.

Empirical research has widely applied privacy calculus theory (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Tsai et al., 2011) as a mechanism that explains individuals’ decision-making via the subjective assessment of the trade-off between the benefits and risks associated with information disclosure. Studies on information disclosure have focused on the privacy issue raised by self-disclosure behavior in a variety of research contexts, such as e-commerce transactions (Tsai et al., 2011), electronic healthcare (Bansal & Gefen, 2010), and social media platforms or social networking sites (Chin et al., 2020; Jozani et al., 2020; Sun et al., 2015). However, debates about government-led data collection and personal freedom in the pandemic situation can be understood as a new social phenomenon (Park, 2021). Privacy tracking in a public health crisis is distinguished from the traditional IS usage addressed in extant literature, which has highlighted the factors of perceived benefits and privacy concerns in terms of end-user motivation. In contrast, in the COVID-19 pandemic, first, the individual’s appraisal of the situational threat imposed by the pandemic is likely to formulate their safety-related psychological state, which in turn affects their perceptions on the benefits and risks of privacy disclosure. Second, by providing personal information through the tracking system, individuals have the advantage of timely infection-related information when necessary. The perceived benefits of providing personal information are relevant to mutual safety. Thus, the disclosure of personal information in the special circumstances of a pandemic can be understood not only in terms of a relationship between individual benefits and risk but also as a social behavior consistent with society’s pursuit of the public interest (Lin & Martin, 2020).

Although privacy issues have emerged as a new social problem arising from the tracking systems mandated in multi-use facilities, including restaurants, there has been little research that has adopted a comprehensive conceptual framework encompassing external situational threat, intrinsic benefits and risks, and social and government factors for understanding individuals’ information disclosure through contact tracing tools. Prior research on personal information disclosure mainly emphasized the importance of internal motivators in terms of perceived benefits and risks. There has been insufficient research that verifies situational antecedents for risk and benefit assessment, or social and institutional influences on personal information disclosure.

Therefore, the uniqueness of the pandemic situation provides opportunities to refine theories that explain privacy issues. Moreover, this research will help restaurant managers and government authorities understand the restaurant patrons and establish more effective policy regarding information privacy collection.

Accordingly, this study sought to identify factors that affect privacy disclosure from an integrated perspective in the context of restaurants. The relationship between individuals’ perceptions of infectious diseases and their intrinsic factors relating to personal information disclosure were identified to explain behavioral intentions. To theoretically explain the drivers/inhibitors of privacy disclosure and behavioral responses, privacy calculus theory and institutional theory were applied as a conceptual framework in the current research. The privacy calculus model, which suggests that individuals engage in a risk-benefit analysis when sharing information with a vendor, has been adopted in previous studies (Kim et al., 2019; Li et al., 2016). In addition, institutional theory proposes that certain human behaviors are influenced by the environment of the organization as well as by regulatory, cognitive, and normative pressures (DiMaggio & Powell, 1983; Scott, 2004). In our study, external pressure for personal information disclosure at restaurants is imposed by government pressure and subjective norms created among members of society.

Drawing on these theoretical models, the current study aimed to propose and empirically test a research model that explains information privacy behavior for restaurant customers in a pandemic situation. The specific aims of this research were to: (1) identify the influence of perceived severity of and perceived vulnerability to COVID-19 on conflicting intrinsic factors in personal information disclosure (perceived benefit and perceived risk); and (2) examine the effect of intrinsic factors and extrinsic factors (subjective norms and government pressure) on intention to disclose personal information. Our study was conducted with customers who had experienced disclosing personal information in restaurants during the pandemic. As the need for personal information disclosure emerged in multi-use facilities, including restaurants, investigating the awareness of personal information loss in daily life became significant for understanding this new social phenomenon. The results of this study have practical implications for restaurant managers and policy agencies.

2 Research background

2.1 Privacy Calculus Theory

Privacy calculus theory suggests that information privacy-related attitudes and behaviors are determined by individuals' evaluations of the benefits and risks associated with the provision of personal information (Culnan & Armstrong, 1999; Dinev & Hart, 2006) argue that individuals anticipate and evaluate the privacy-related risks and benefits of disclosing personal information when they encounter a situation that requires the provision of potentially sensitive and private information. Extant literature has suggested that individuals are less likely to share personal information when they are concerned about information privacy (Culnan & Armstrong, 1999; Li et al., 2010). As people tend to withhold their private information, other motivators are necessary to encourage them to provide it (Smith et al., 2011). Prior research on privacy found that people were willing to disclose personal information in exchange for some economic or social benefit, subject to the 'privacy calculus,' a subjective assessment of whether their personal information would subsequently be used fairly and they would not suffer negative consequences (Culnan & Armstrong, 1999).

According to privacy calculus theory, perceived risk is uncertainty concerning the potential invasion of privacy as a result of personal information disclosure (Dinev & Hart, 2006). Perceived privacy risks include information sensitivity (Yang & Wang, 2009), privacy concerns (Bansal & Gefen, 2010), and legislative protection (Li et al., 2016). The perceived benefits, the other construct of privacy calculus theory, refer to a wide range of financial and non-financial incentives as consequences of sharing personal information (Smith et al., 2011). Benefits include the disclosure of public goodness (Nabity-Grover et al., 2020) and individual-organization trust (De Wulf et al., 2001; Gefen & Heart, 2006; Wang et al., 2017) found that individuals gave more weight to social rewards than financial rewards with regard to self-disclosure intention.

The degree of benefits and risks perceived by individuals in a particular situation may differ depending on past experience (Dienlin & Metzger, 2016), or the purpose and the context of social transactions (Liu et al., 2014). The privacy calculus can also be influenced by an individual's subjective value, and it serves as a personal or internal motivation in the decision-making process (Li, 2012). Privacy calculus theory has been applied in a variety of research contexts, such as location-based social network services (Sun et al., 2015), mobile applications (Morosan & DeFranco, 2015; Wang et al., 2016), electronic health records (EHRs) (Dinev et al., 2016), mobile location-based advertising (Gutierrez et al., 2019) and IoT services (Kim et al., 2019). Within this

literature, scholars have largely agreed that privacy is situational and significantly contextual.

These studies suggest that in the pandemic situation in which personal information is used by national health agencies to conduct contact tracing to prevent infection in local communities, individuals' privacy perceptions may be different than in other contexts (e.g., use of e-commerce and SNS). Given the unprecedented circumstances presented by the COVID-19 pandemic, the disclosure of personal information is a crucial component in containing the spread of infection (Gasser et al., 2020). In this context, the privacy calculus theory postulates that individuals compare the benefit of receiving information about being in contact with infected individuals with the risk of a loss of control over their personal information or misuse by government or private organizations. With the pandemic threat, there has been widespread acceptance of tracking technology, and a relatively low public perception of concern about providing personal information has been found (Lewandowsky et al., 2021). However, Jung et al., (2020) emphasized that despite the advantage of reducing the spread of infection by locating infected persons, there could be serious privacy problems if personal identification occurs. The perceived benefits for public health and the credibility of authorities' privacy protection policies have a positive effect on the disclosure of personal information (Hassandoust et al., 2021). Privacy calculus factors (benefit and risk) can explain the mechanism of behavior for privacy disclosure in the current restaurant contexts, a new social phenomenon, and are expected to present meaningful results.

2.2 Institutional Theory

While the term 'institution' has been defined differently, it generally refers to a basic framework constituting a set of norms, rules, and beliefs (North, 1990). Institutional environments may endogenously influence organizations through the archetypes they develop for actors, the logic they legitimate, and the governance system and rules of social activities they support. In other words, organizational decisions are not only driven by individuals' rational goals but also by social and cultural factors and concerns about legitimacy (Scott et al., 2000). With respect to institutional theory, Scott (1995) classified a country's institutional environment into three dimensions: regulatory, cognitive, and normative. The regulatory dimension refers to the rules and laws accountable for the stability of society. The cognitive dimension contains the cognitive structures and mechanisms in a society that are taken for granted. Lastly, the normative dimension covers the social and cultural values and norms in society (Yiu & Makino, 2002).

In further developing the model, DiMaggio & Powell (1983) identified three mechanisms through which institutional members engage in similar decisions and behaviors: (1) coercive isomorphism, (2) mimetic isomorphism, and (3) normative isomorphism. Coercive isomorphism emerges as a result of formal and informal pressure exerted by governments and institutions. Regulatory bodies impose legal and administrative sanctions to introduce specific behaviors or standards (Kostova, 1997; Scott, 1995), and individuals are coercively encouraged to comply with social standards (García-Sánchez et al., 2016). Mimetic isomorphism can be understood as an effort to respond to uncertainty and produce good results by imitating the decision-making and actions of a role model or a leader within an organization (Shi et al., 2008). Finally, normative isomorphism refers to the process of rationalizing and theorizing new operating standards until members take them for granted (Strang & Meyer, 1993). Specific cases within an organization may change the principles that are applicable to the entire organization, i.e., behavioral patterns can be rationalized, and homogeneity among all members can be achieved (Suchman, 1995).

Empirical studies of institutional theory have examined the influence of pressure within organizations on operation methods and people's intention to accept specific technologies. Coercive pressure, normative pressure, and mimetic pressure have been measured and research has verified that these pressures influence the diffusion rate of operating methods within organizations (Burns & Wholey, 1993; Lee & Pennings, 2002). Furthermore, IS researchers have verified that institutional forces affect the use or adoption of new technology in organizations (Gibbs & Kraemer, 2004; Soares et al., 2020), such as enterprise resource planning (ERP) system (Liang et al., 2007), electronic procurement systems (EPSs) (Soares-Aguiar & Palma-dos-Reis, 2008), and EHRs (Sherer et al., 2015).

The disclosure of personal information in the context of a pandemic is considered to be more than an individual's calculus of privacy risk-benefit; it is also motivated by external factors, such as normative pressure on social actors or coercive pressure from government (Lin & Martin, 2020). Individuals within an organization tend to harmonize with their surroundings to resolve uncertainty and constraints, and social homogeneity itself can act as a crucial external motive factor in the decision-making process (Sherer et al., 2015). While institutional pressure includes three types of pressures, Scott (2005) suggests that special attention should be paid to "regulatory" and "normative" pressures, focusing on the targets under which they are applied. Wang et al., (2018) also classified institutional pressures affecting environmental management practices into regulatory pressures and normative pressures. Considering each pressure

is context-specific (Berrone et al., 2013), the pressures in this study can be largely divided into social and governmental. Therefore, in this study, institutional pressure was composed of subjective norms for society members and coercive pressure from government regulations.

In summary, by applying the privacy calculus theory and institutional theory discussed above, this study presents a conceptual model as shown in Fig. 1. The subjects of this study were customers who had experience in disclosing personal information in restaurants, and we sought to identify the importance of the factors that led to personal information disclosure behavior. The current study also defined the relationship between individual threat appraisal and privacy calculus factors as 'situational privacy calculus', and tried to explain the mechanisms for threat appraisal, drivers/inhibitors, and behavior.

3 Hypothesis Development and Research Model

3.1 Research Model

Figure 2 demonstrates the research model, which consists of eight main hypotheses derived from the literature discussed in the previous section. The model explains the structural relationships between threat appraisal of COVID-19, the drivers and inhibitors of PID, and intention to disclose. The following variables were included in the research model to ensure an accurate evaluation of intention to disclose PI (Personal Information): years of smartphone use; and the number of personal information disclosures. Prior studies have verified that individuals with frequent experiences of privacy disclosure are less sensitive about their personal information (Lang et al., 2018). In a similar vein, given that privacy-related issues have become a significant issue owing to the development of ICT and the high frequency of privacy-providing experiences using mobile devices in the pandemic situation (Cha et al., 2021), we also considered that the duration of smartphone usage would affect personal information disclosure intentions.

3.2 Perceived Severity and Vulnerability toward Privacy Calculus Factors

Threat appraisal refers to the individual's cognitive assessment of the relevant external threats (Maddux & Rogers, 1983). This concept has been articulated further based on perceived severity, which refers to the degree of seriousness of the consequences from the negative event imposing the threat, and perceived vulnerability, which means the magnitude of susceptibility felt by the individual to the

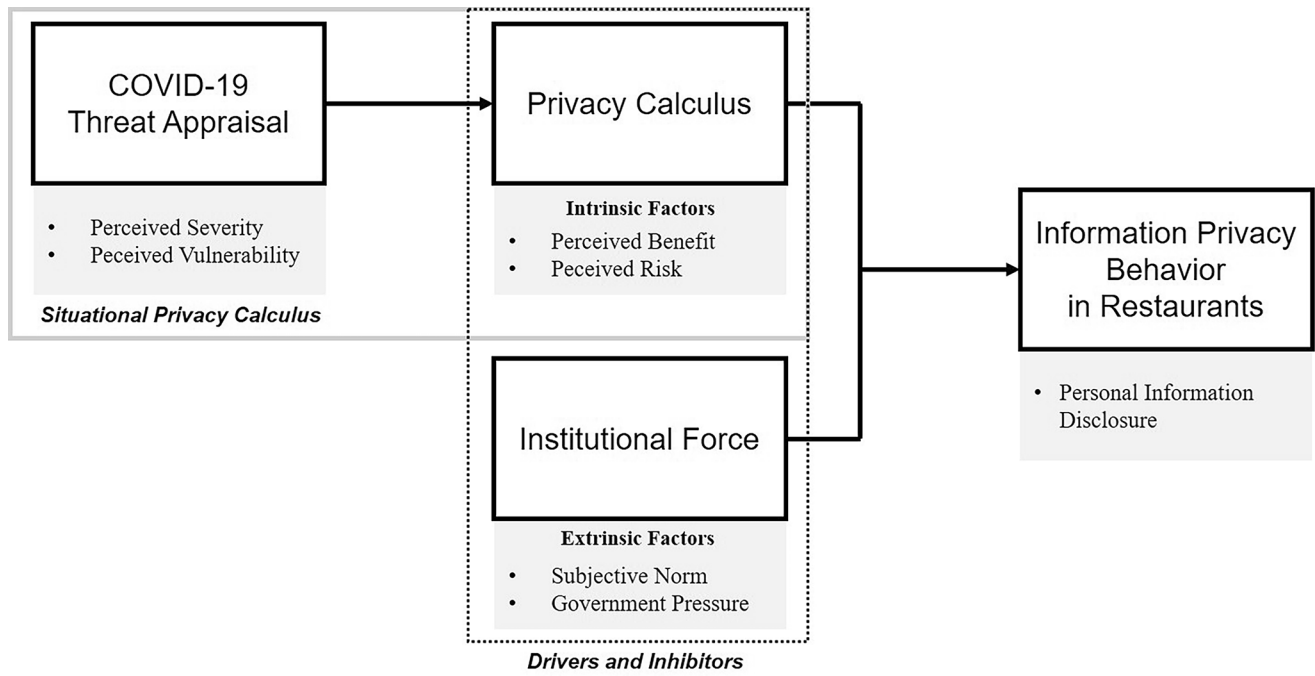


Fig. 1 Conceptual model

threat (Rogers, 1975). The protection motivation framework (Wurtele & Maddux, 1987) postulates that a high

threat appraisal leads to elevated self-protection against the impending threat (Wang et al., 2019).

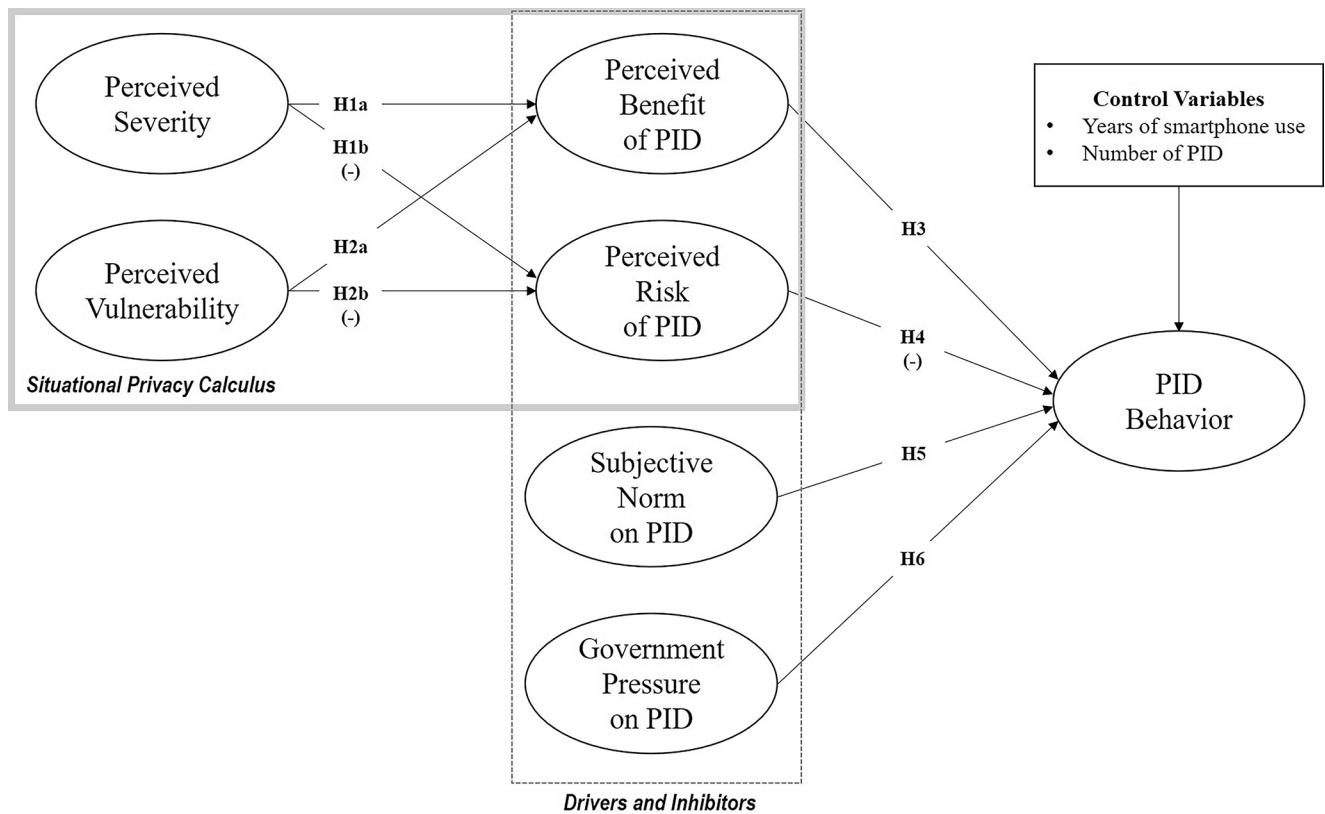


Fig. 2 Research Model. Note: PID = Personal Information Disclosure

Applying this framework in the context of the COVID-19 pandemic, Bashirian et al., (2020) reported that healthcare workers' threat appraisal (perceived severity and perceived vulnerability) affected their protection motivation with regard to COVID-19 preventive behavior. Similarly, Ezati Rad et al., (2021) reported that COVID-19 protection motivation was significantly and positively correlated with perceived severity and perceived vulnerability. This heightened health motivation is expected to affect the likelihood of engaging in the recommended behaviors for health protection. To lend support, Itani & Hollebeek (2021) showed that travelers' threat appraisal (perceived severity and perceived susceptibility) positively affected their social distancing behavior, which in turn influenced their intention to use virtual reality-based (vs. in-person) attractions. In the same vein, people who have a high perception of COVID-19 threats consider continuously using social distancing practices (Sreelakshmi & Prathap, 2020). In other words, these previous studies suggest that a perceived high threat to health by an individual induces protective motivation, and ultimately affects the individual's decision-making process (Brewer et al., 2004; Maiman & Becker, 1974).

The collection and utilization of personal information by the government or health authorities can be effective in preventing the spread of infection (Ienca & Vayena, 2020). Personal information is used to track and identify people exposed to COVID-19, and, in such a pandemic situation, the provision of personal information can be viewed as a protective action against threats to individual safety. Further, when the perceived threat is more severely appraised, it is more likely that individuals will take protective actions, as they perceive the benefits of such behavior more positively. Risks associated with information disclosure have also been recognized. Lewandowsky et al., (2021) probed the public's attitude towards potentially privacy-encroaching options, such as tracking technology and immunity passports to combat the pandemic. They explained that perceived harm from COVID-19 offsets the risks to individual privacy from a privacy calculus perspective. According to this argument, the larger the perceived threat, the smaller the perceived risk of personal information disclosure. Tran & Nguyen (2021) also explained the use of contact tracing applications as a precautionary behavior against the virus, verifying that health risks positively influenced the perceived value. Therefore, it is likely that the threat appraisal is positively related to the perceived benefit of personal information disclosure in a pandemic situation. Based on prior research, we propose the following hypotheses.

H1a. In a pandemic situation, perceived severity has a positive effect on the perceived benefit of PID.

H1b. In a pandemic situation, perceived severity has a negative effect on the perceived risk of PID.

H2a. In a pandemic situation, perceived vulnerability has a positive effect on the perceived benefit of PID.

H2b. In a pandemic situation, perceived vulnerability has a negative effect on the perceived risk of PID.

3.3 Perceived Risk and Benefit toward Personal Information

Drawing on the privacy calculus perspective, this study defines perceived benefit as the degree of positive safety-related consequences of personal information disclosure, and the perceived risk as the predicted degree of privacy loss from personal information disclosure. With respect to perceived risks and perceived benefits, which explain individuals' conflicting views on information provision (Dinev & Hart, 2006), people perform a costs (risks)-benefits analysis of information disclosure based on the specific circumstances of IS adoption.

For example, in the context of mobile applications usage, Wang et al., (2016) proposed that privacy is relinquished to some extent for the anticipated benefits of using the applications. Therefore, it is possible to postulate that benefits from the app, such as convenience, personalization, entertainment, or other rewards, are likely to lead to its adoption. With respect to information provision in the pandemic situation, Sharma et al., (2020) have reported that favorable expected outcomes influence attitudes toward COVID-19 digital contact tracing applications, while privacy concerns have a negative impact. Hassandoust et al., (2021) also verified that risk, privacy concerns, and benefits to public health affected the intention to install a contact tracing mobile application. When individuals' perception of a benefit exceeded the privacy risk loss, they were willing to surrender personal information even if their personal information was sensitive (Li et al., 2016). Based on these previous findings, the current research established the following hypotheses concerning the disclosure of personal information in a pandemic situation:

H3. In a pandemic situation, the perceived benefit of PID has a positive effect on PID behavior.

H4. In a pandemic situation, the perceived risk of PID has a negative effect on PID behavior.

3.4 Subjective Norms and Government Pressure for Personal Information Disclosure

The disclosure of personal information in a pandemic context can be understood not only as a trade-off relationship between the individual's privacy benefit and risk, but also in terms of the normative pressure on social actors or coercive pressure from government (Lin & Martin, 2020). Accordingly, in our study, institutional pressure on personal

information disclosure was divided into subjective norms and government pressure within the country's institutional environment.

The institutional force model has been applied to explain the role of external forces (such as social norms or regulatory pressure) on the adoption of information systems and technologies, such as supply chain management system or enterprise applications (Kokkonen et al., 2013; Liang et al., 2007; Tsai et al., 2013). For example, Gibbs & Kraemer (2004) verified that environmental factors (external pressure, government promotion, and legislation barriers) are directly associated with the scope of e-commerce use. In a similar vein, Sherer et al., (2015) reported the impact of the institutional influence of government policies and industry norms on the adoption of EHRs.

The theory of planned behavior (Ajzen, 1991) also asserts that subjective norms influence behavioral intentions. With regard to information technology adoption, researchers have validated subjective norms as an antecedent to behavioral intentions (Bock et al., 2005; Kaushik et al., 2015; Ozkan & Kanat, 2011). In the context of information privacy issues, subjective norms as a socially related factor in disclosure behavior are positively related to behavioral intention to use a website (Kaushik et al., 2018). Therefore, it is logical to conclude that the stronger the group standards, the more justifiable certain behaviors are among the social community members. Based on the above literature, this research hypothesized that subjective norms and government pressure relating to PID are significantly related to intention to disclose PI. Thus, the following two hypotheses were suggested:

H5. In a pandemic situation, subjective norms relating to PID have a positive effect on PID Behavior.

H6. In a pandemic situation, government pressure relating to PID has a positive effect on PID Behavior.

4 Research Method and Analysis

4.1 Survey measures

To avoid measurement inaccuracies, previously validated multi-measurement items were used in the questionnaire (Churchill Jr., 1979) after adapting them to the context of the current study. Initially, the survey questions included 27 items for seven constructs: perceived severity, perceived vulnerability, perceived risk of PID, perceived benefit of PID, subjective norms relevant to PID, government pressure relating to PID, and PID behavior in the pandemic situation. Perceived severity was assessed using four items derived from Prasetyo et al., (2020). Perceived vulnerability was assessed using 4 items derived from Prasetyo et al., (2020)

and De Zwart et al., (2009). To assess the perceived risk of PID in the pandemic situation, four items were adapted from research conducted by Morosan & DeFranco (2015) and Xu et al., (2011). For the perceived benefit of PID, four items were developed based on prior research (Dinev et al., 2013, 2016) in the context of the pandemic situation. To measure the subjective norms relating to PID, three items were drawn from Sledgianowski & Kulviwat (2009). To assess government pressure relating to PID in the pandemic situation, four items were drawn from Ahmadi et al., (2017) and Krell et al., (2016). Lastly, four items were adapted from prior research (Bansal & Gefen, 2010) to measure PID behavior.

4.2 Data collection

The unit of analysis for this study was individuals in South Korea, the United States (US), and the United Kingdom (UK) who had experienced the disclosure of personal information via QR codes and hand-written entry logs in restaurants. Considering the pandemic situation, this study conducted a survey on residents in South Korea (a representative Eastern country), the United Kingdom and the United States (Western countries), which are actively using ICT to prevent COVID-19 infection (Whitelaw et al., 2020). Data collection through an online survey for respondents in South Korea was performed from December 23 to December 31, 2020, and in the US and the UK, it was performed from January 4 to January 5, 2021. Seven-point Likert-type scales were used for high reliability and discriminant validity (Cicchetti et al., 1985). The participants were asked to indicate the extent to which they agreed or disagreed with each of the 27 items (1 = strongly disagree and 7 = strongly agree). In addition, the survey contained two items associated with past experience of PID in the pandemic situation (i.e., number of experiences disclosing PI, and the preferred way to disclose personal information), and eight questions related to socio-demographics (i.e., age, gender, occupation, marital status, education, monthly income, country of residence, and number of years using smartphones). The measurement was originally designed in English and then translated into Korean by two professionals who are proficient in English and Korean. The Korean version was then back-translated into English, and some discrepancies were remedied between the English and Korean expressions. Two scholars whose native language is Korean evaluated the content validity of the survey questions. As a pilot test, the questionnaire was administered to four students majoring in hospitality management. A pretest was administered to 57 participants with the assistance of a marketing company. This procedure found no material discrepancies.

Table 1 Demographics. (n = 475)

Variable	Content	Frequency (%)
Gender	Male	238 (50.1%)
	Female	237 (49.9%)
Country of Residence	South Korea	311 (65.5%)
	U.S.	89 (18.7%)
	U.K.	75 (15.8%)
Age	19 or younger	4 (0.8%)
	20 ~ 29	112 (23.6%)
	30 ~ 39	126 (26.5%)
	40 ~ 49	101 (21.3%)
	50 ~ 59	81 (17.1%)
	60 or order	45 (9.5%)
	No response	6 (1.3%)
Marital Status	Single	202 (42.5%)
	Married	273 (57.5%)
Education	Secondary School	73 (15.4%)
	Trade/Vocational/College School	79 (16.6%)
	Bachelor's degree	234 (49.3%)
	Master's degree or higher	89 (18.7%)
Monthly Income	\$1,999 or below	124 (26.1%)
	\$2,000 - \$2,999	133 (28.0%)
	\$3,000 - \$3,999	81 (17.1%)
	\$4,000 - \$4,999	57 (12.0%)
	\$5,000 or above	80 (16.8%)
Years using a Smartphone	Less than 3 years	43 (9.1%)
	3 years - within 5 years	37 (7.8%)
	5 years - within 10 years	166 (34.9%)
	More than 10 years	229 (48.2%)
Number of PI disclosures	1 ~ 2	115 (24.2%)
	3 ~ 5	100 (21.1%)
	6 ~ 9	61 (12.8%)
	10 times or more	199 (41.9%)
Preferred method of disclosing PI	Handwritten entry logs	174 (36.6%)
	QR code	300 (63.2%)
	No response	1 (0.2%)

An online survey was considered to be a particularly appropriate data collection method in the pandemic situation. Access to potential respondents in South Korea was obtained through a reputable marketing research firm (Macromill Embrain, www.embrain.com), and a quota sampling approach was implemented. Access to potential participants in the US and the UK was obtained in a similar manner through a marketing research firm (Prolific, <https://www.prolific.com>) using a convenience sampling method. In a screening question purposely designed for the survey, all subjects were asked to indicate whether they had experienced disclosing personal information in a restaurant in the pandemic situation (i.e., “How many times have you experienced personal information disclosure in a restaurant in the pandemic situation?”).

4.3 Data analysis

4.3.1 Sample Characteristics

A total of 475 usable surveys were completed: 311 from South Korea, 89 from the US, and 75 from the UK. Female respondents accounted for 49.9% of the overall sample. Approximately 26.5% of the respondents were between 30 and 39 years of age, 23.6% were between 20 and 29, and 21.3% were between 40 and 49. About 49.3% of the respondents held a bachelor's degree, 18.7% had master's degrees, 16.6% held a trade/vocational/college degree, and 15.4% had secondary school qualifications or below. About 48.2% of the respondents had more than 10 years of experience using smartphones, 34.9% had 5 to 10 years of experience, 9.1% had less than 3 years of experience, and 7.8% had 3 to 5 years of experience in using a smartphone. Regarding personal information disclosure experiences in the pandemic situation, 41.9% had more than 10 disclosure experiences, 24.2% had one or two disclosure experiences, 21.1% had three to five disclosure experiences, and 12.8% had six to nine disclosure experiences. Approximately 63.2% of the respondents were found to prefer QR codes, and 36.6% of the respondents preferred handwritten entry logs when using restaurants in the pandemic situation. The respondents' detailed demographics are reported in Table 1.

4.3.2 Measurement Model

This study employed partial least squares–structural equation modeling (PLS-SEM) analysis to examine the proposed measurement and structural model and test the proposed hypotheses. The PLS-SEM technique was used instead of CB-SEM procedures because of the research objective, which addressed the new context of the pandemic situation (Hair Jr et al., 2021). PLS-SEM uses the residual variance of the latent variables, and its main object is predicting key target variables (Fornell & Bookstein, 1982). Considering the current study was primarily prediction-oriented, we chose to use PLS-SEM analysis.

Because respondents were asked to rate all survey questions at once, common method variance was a potential issue. Therefore, Harman's single-factor test as a post hoc statistical test was performed to confirm whether common method bias was present in the resultant data set (Harman, 1967). We subjected all 27 measurement items to an exploratory factor analysis (EFA), and unrotated factor solutions were examined. In this process, when a single factor appears or when one factor accounts for more than 50% of the variance of the variables, there is an issue of common method bias (Podsakoff et al., 2003). The EFA results delineated seven variables (Eigenvalue > 1) and each dimension

Table 2 Measurement Item Properties

Construct	Items	Loading	alpha	CR	rho_A	AVE
SEV	I believe COVID-19 is a serious disease.	0.91	0.833	0.884	0.878	0.659
	I believe COVID-19 can lead to death.	0.849				
	I believe COVID-19 is more severe than any other disease.	0.662				
	I believe COVID-19 can affect mental health.	0.805				
VUL	I think I am likely to contract COVID-19.	0.896	0.859	0.905	0.875	0.705
	I think my family are likely to contract COVID-19.	0.893				
	My past experiences make me believe that I am likely to get sick when my friends/colleagues are sick.	0.746				
	I think there is a chance that my neighborhood will be infected by COVID-19.	0.814				
RISK	It would be risky to disclose my personal information to the service provider in restaurants in the pandemic situation.	0.888	0.917	0.941	0.928	0.801
	There would be high potential for privacy loss in disclosing my personal information to the service provider in restaurants in the pandemic situation.	0.919				
	Personal information could be improperly used by this service provider in the pandemic situation.	0.851				
	Providing the service provider with my personal information in a restaurant would involve many unexpected problems in the pandemic situation.	0.92				
BEN	By disclosing my personal information in restaurants, I can be contacted if I need to be tested.	0.848	0.927	0.949	0.929	0.822
	By disclosing my personal information, I can reduce the risk of spreading the virus unknowingly via a positive COVID-19 case from the restaurants that I visited.	0.92				
	Disclosing my personal information will help health officials fight against COVID-19 cases.	0.936				
	Disclosing my personal information in restaurants will generate a positive contribution for public health in our society.	0.921				
NOR	People who are important to me think that I should disclose my personal information in restaurants in the pandemic situation.	0.96	0.966	0.978	0.967	0.937
	People whose opinions I value would prefer me to disclose my personal information in restaurants in the pandemic situation.	0.977				
	People whom I look up to expect me to disclose my personal information in restaurants in the pandemic situation.	0.967				
PRE	The government requires me to disclose my personal information in restaurants.	0.91	0.851	0.898	0.918	0.69
	Disclosing personal information in restaurants is necessary for legal compliance.	0.905				
	Regulatory requirements impose penalties for not disclosing personal information(e.g. imposition of fines).	0.828				
	I feel pressure from the government to disclose personal information.	0.653				
BEH	I have provided my personal information in restaurants.	0.892	0.916	0.941	0.918	0.799
	I keep providing my personal information in restaurants.	0.883				
	I am willing to provide my personal information in restaurants.	0.885				
	I am likely to provide my personal information in restaurants.	0.914				

Note: SEV = Perceived Severity, VUL = Perceived Vulnerability, BEN = Perceived Benefit of PID, RISK = Perceived Risk of PID, NOR = Subjective Norm on PID, PRE = Government Pressure on PID, BEH = PID Behavior

explained 4.425–32.001% of the covariation among the measures. As none of the factors accounted for more than 50% of the covariation, it was concluded that the measures in this study did not have a serious common method bias problem.

The analysis first assessed the measurement model through the validity and reliability of the constructs. Convergent validity was evaluated the strength and significance of the loadings, the average variance extracted (AVE), and the reliability estimates (Bagozzi & Heatherton, 1994). As Table 2 shows, all loadings were satisfactory, and all AVEs were greater than 0.50, exceeding the suggested threshold

(Fornell & Larcker, 1981). Taken together, the results provide strong evidence for convergent validity. Next, construct reliability was assessed via internal consistency and indicator reliability. Internal consistency was evaluated with Dillon-Goldstein's rho, which does not assume parallelity of the manifest variables as Cronbach's alpha does. All factors achieved satisfactory reliability (Cronbach's alpha > 0.70), and Dillon-Goldstein's rho value ranged from 0.875 to 0.967 (Table 2). Finally, discriminant validity was established on the basis of the heterotrait–monotrait ratio of correlations (HTMT), a procedure superior to the commonly considered criterion (Fornell & Larcker, 1981), and by the assessment

Table 3 Heterotrait-Monotrait Ratio of Correlations (HTMT)

	Mean	S.D.	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1) SEV	5.707	1.039							
(2) VUL	4.919	1.128	0.504						
(3) RISK	4.398	1.346	0.097	0.058					
(4) BEN	5.538	1.099	0.361	0.281	0.325				
(5) NOR	4.527	1.521	0.242	0.151	0.249	0.408			
(6) PRE	4.553	1.413	0.201	0.208	0.171	0.363	0.663		
(7) BEH	5.151	1.490	0.208	0.239	0.287	0.597	0.575	0.655	

Note: SEV = Perceived Severity, VUL = Perceived Vulnerability, BEN = Perceived Benefit of PID, RISK = Perceived Risk of PID, NOR = Subjective Norm on PID, PRE = Government Pressure on PID, BEH = PID Behavior

of cross-loadings (Henseler et al., 2015). The results showed that all HTMT values of the latent variables were below the critical and conservative value of 0.85 (Table 3). The results demonstrated that, overall, the scales were valid and reliable measures of their respective constructs.

4.3.3 Testing of the Hypothesized Structural Model

The multicollinearity of each independent variable was diagnosed using the variance inflation factor (VIF). Because all values for VIF fell between 1.004 and 1.848, multicollinearity was not an issue in this research. The corrected R^2 values refer to the explanatory power of predictor variables onto the respective constructs. To estimate the accuracy of the structural framework, the R^2 of variance explained for the perceived risk of PID (0.004), perceived benefit of PID (0.13), and intention to disclose personal information (0.548) were calculated as predictive powers. In addition to the R^2 analysis, Stone-Geisser's Q^2 value (Stone, 1974) was calculated to assess the predictive relevance of the model in this study. Q^2 evaluates the predictive validity of a model by skipping some indicator values using calculated parameters. The difference between the skipped data points and the predicted ones is the basis for the Q^2 calculation (Chin et al., 2008). Q^2 shows how well the empirically collected data can be reconstructed with the help of the model and PLS parameters produced in the initial analysis. A Q^2 greater than 0 means that the model has predictive relevance, while a Q^2 of less than 0 is interpreted as lacking predictive relevance. The Q^2 for the perceived risk of PID, perceived benefit of PID, and intention to disclose personal information were 0.006, 0.106, and 0.432, respectively, indicating acceptable predictive relevance. To determine whether there were demographic influences on the research model, this study tested years of smartphone use, and the number of PI disclosures as control variables, using 5,000 bootstrapping resamples in PLS-SEM.

Figure 3 shows the results of the structural relationships hypothesized in this research, as well as the control variables. Among the control variables considered in this study, the number of PI disclosures had a strong positive effect on

the intention to disclose. This result can be understood in a similar context to the previous literature, in that with more experiences of disclosing personal information, repetition of such actions became more likely (Lang et al., 2018). On the other hand, the duration (years) of smartphone use was not related to the intention to disclose. These results indicate that the analytical data supported the proposed hypotheses, with the exception of H1b and H2b. As shown in Fig. 3, six main hypotheses were supported.

Specifically, perceived severity was found to significantly influence perceived benefit of PID (H1a: $\beta = 0.295$, t value = 5.684, $p < 0.001$). Additionally, perceived severity was not significantly affected by perceived risk of PID (H1b: $\beta = -0.087$, t value = 1.552). Meanwhile, perceived vulnerability significantly influenced perceived benefit of PID (H2a: $\beta = 0.131$, t = 2.604, $p < 0.01$), and did not influence perceived risk of PID (H2b: $\beta = 0.086$, t value = 1.412). Intention to disclose PI was affected by perceived benefit of PID (H3: $\beta = 0.34$, t value = 8.235, $p < 0.001$), perceived risk of PID (H4: $\beta = -0.105$, t value = 3.21, $p < 0.01$), subjective norms on PID (H5: $\beta = 0.159$, t value = 3.099, $p < 0.01$), and government pressure on PID (H6: $\beta = 0.332$, t value = 5.76, $p < 0.001$). That is, the strongest influence on information disclosure was the perceived benefit of PID, followed by government pressure and subjective norms. Furthermore, we verified that the perceived risk of disclosure was a major inhibitor on personal information disclosure in the pandemic situation.

5 Discussion and implications

5.1 Discussion

Despite the ongoing personal information disclosure issue in the pandemic situation, in-depth research on individual adoption behavior is insufficient, especially in the restaurant context. Several key findings from the analysis are worth noting. First, it was confirmed that threat appraisal (perceived severity and perceived vulnerability) affects the perceived benefit of PID. In other words, the greater the

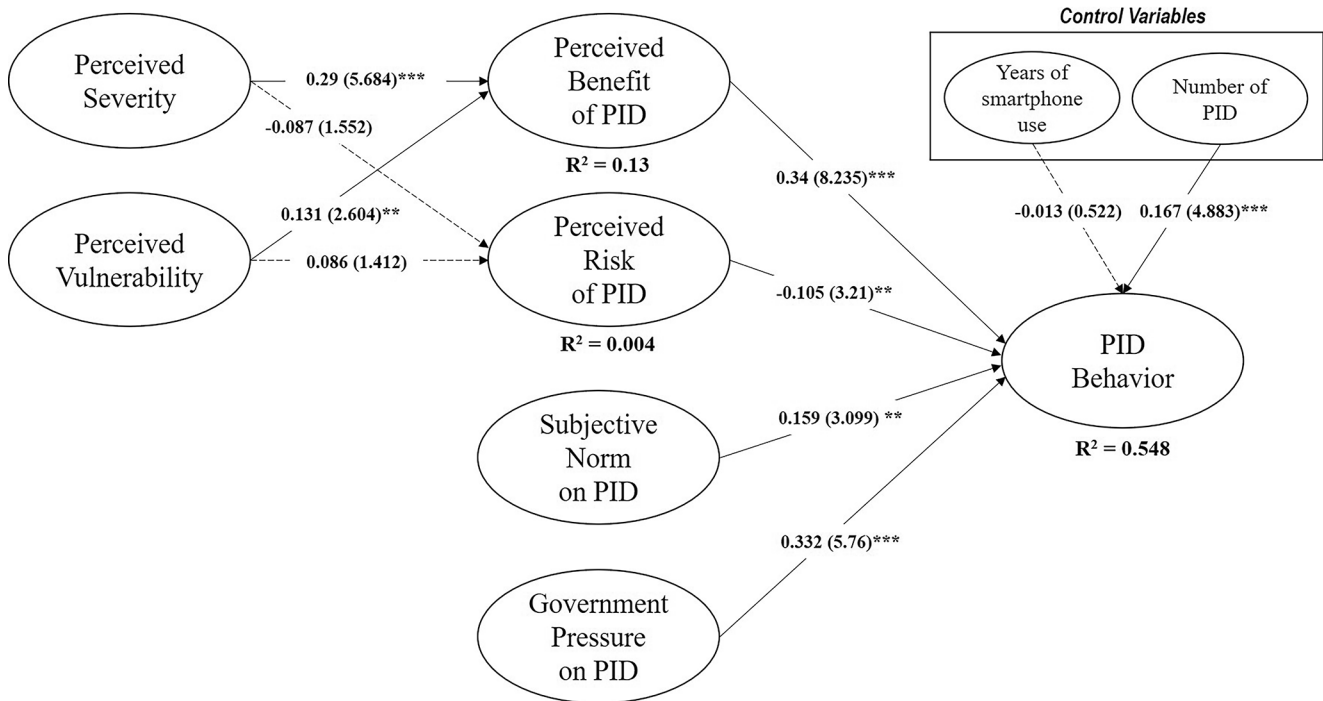


Fig. 3 Result of the structural model. Note: PID = Personal Information Disclosure
*p < 0.05, **p < 0.01, ***p < 0.001

awareness of virus threats in epidemics, the higher the perception of privacy benefits related to personal safety protection. Also, this study verified the influence of four factors of PID on behavior intention. We verified that perceived benefit was the most influential factor on intention to disclose. It was demonstrated that the perception of the benefit related to individual safety was the most influential factor in the pandemic situation. In the context of COVID-19, individuals can contribute to quarantine policies by allowing the activation of contact tracing. In this process, individuals are willing to voluntarily share their personal information and movement history in return for the significant assurance that they are protected by obtaining information on local infections. In this regard, Hassandoust et al., (2021) showed that the perceived benefit of contact tracing had a stronger influence on the intention to install contact tracing apps than privacy risk beliefs did. Moreover, we verified that subjective norms and government pressure, considered extrinsic factors, are also significant factors influencing PID behavior. Since contact tracing is closely related to public interests in pandemic situations, it can be a crucial issue for individuals to feel a sense of legitimacy and necessity when disclosing personal information (Hartley & Jarvis, 2020).

5.2 A post-hoc analysis: The moderating effect of cultural difference

Given that COVID-19 and privacy issues are common worldwide, we consider it meaningful to understand differences in privacy-related motivators/inhibitors and behaviors for different cultural backgrounds (individualist versus collectivist culture). Accordingly, a post-hoc analysis was performed. A multi-group analysis was conducted to examine the influence of cultural differences on the disclosure of personal information between two groups – an individualist culture (as in the US and the UK) versus a collectivist culture (South Korea) determined by referring to the measures of individualism-collectivism in Hofstede’s dimensions. According to Hofstede Insights (2021), the individualism values for South Korea, the UK, and the US were 18, 89, and 91, respectively. As shown in Table 4, the paths from perceived risk and intention to PID behavior were significantly stronger in the US and UK groups than in the South Korean group (difference = 0.15, p < 0.05); however, for the other paths, differences between the South Korean group and the US and UK groups were not significant.

IS researchers have verified that there are differences in information privacy concerns based on cultural differences (Bellman et al., 2004). Specifically, Dinev et al., (2006) investigated cross-cultural differences in beliefs related to e-commerce use in Italy and the US. They found a strong

Table 4 PLS Multigroup Analysis for Two Groups

Paths	Group 1: South Korea		Group 2: U.S. and U.K.		Group1 vs. Group2		
	Paths Coefficients	T-value	Paths Coefficients	T-value	Difference Coefficients	P-value	Test of Moderating effects
BEN→BEH	0.396	6.291***	0.319	4.902***	0.077	0.404	Not Supported
RISK→ BEH	-0.042	0.95	-0.193	3.375***	0.15	0.036*	Supported (G1 < G2)
NORM→ BEH	0.174	2.775**	0.147	1.773	0.028	0.781	Not Supported
PRES→ BEH	0.211	3.095**	0.374	4.545***	0.163	0.136	Not Supported

Note: SEV = Perceived Severity, VUL = Perceived Vulnerability, BEN = Perceived Benefit of PID, RISK = Perceived Risk of PID, NORM = Subjective Norm on PID, PRES = Government Pressure on PID, BEH = PID Behavior, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

moderating effect between perceived risks and e-commerce use in individualist cultural groups (US). The results of post-hoc analysis also show that individualist countries tend to be more sensitive to privacy risks.

5.3 Implications for research and practice

This study contributes to individuals' privacy-related literature in several ways. First, this study applied the protection motivation theory (Wurtele & Maddux, 1987) to better understand customer privacy calculus in pandemic situations. Specifically, by verifying the relationship between protection motivation factors (i.e., perceived severity and perceived vulnerability) and perceived benefit, we established that restaurant customers perform a "situational privacy calculus" when they disclose their privacy. Second, this study tried to embody and redefine perceived benefits to clarify privacy disclosure behavior. This study sought to understand individuals' health-related benefits of contact tracing and further verified that it is a strong motivator of privacy disclosure behavior. This study differs from information privacy studies focused on individual financial and non-financial benefits before COVID-19, and enables a better understanding of the central variables of privacy calculus under health-threatening situations. Third, this study adopted institutional theory to verify the institutional impact on privacy disclosure. While many previous studies have distinguished between internal and external dimensions, the current study took a more comprehensive approach to understanding the situation. In particular, applying two theories to confirm the verification of intrinsic and extrinsic factors is considered of academic value as an approach to the theoretical integration of structural frameworks.

Since the pandemic's start, governments, health authorities, and stakeholders involved in the fight against the virus have relied on data analytics and digital technologies to address the threat (Xiang, 2021). The use of personal information has been evaluated as a necessary measure to prevent the spread of the pandemic, but various efforts are

required to minimize social problems related to privacy protection. Importantly, this study suggests meaningful implications for restaurant operations in similar circumstances and conditions worldwide. Although consumers are also very concerned about the safety and hygiene environment of multi-use facilities, they overwhelmingly desire to visit restaurants even during pandemic circumstances (Alt, 2021). Therefore, it seems necessary to continue discussions with government and health authorities about how restaurant businesses can manage the pandemic situation with respect to privacy protection as well as the physical safety of restaurant customers, based on the results of this study. More specifically, there is a need to devise ways to address two types of concerns (virus threat and privacy risk) perceived by restaurant customers in the current situation.

The following practical suggestions are presented based on the results of this study: First, to promote the benefits of privacy disclosure in the pandemic, the role of government and health authorities is believed to be crucial. Based on our results, it should be recognized that in extreme threat situations, the individual can perform situational privacy calculus that prioritizes individual health. Accordingly, the government should specifically present the purpose of "preventing the spread of infectious diseases" in health-threat situations and promote the health-related benefits of disclosing privacy. For example, efforts such as presenting phrases emphasizing the threat of infectious diseases on the QR system, continuously updating health-related information processed by disclosing personal information on government websites, and promoting public access are required.

Second, measures should be sought to induce disclosure of personal information by emphasizing the legitimacy of the government's policy measures and the prevailing social norms. Considering that the subjective criterion for PID is a strong motivation, the government should devise ways to make restaurant customers aware of their social and moral obligation to disclose personal information. Specifically, such approaches should clearly present the influence of PID behavior on society beyond individual interests and

emphasize that it is socially justified at a normative level. Furthermore, considering that government pressure is also a crucial factor driving behavior, thorough and strict legal action by the government against the inappropriate disclosure of personal information is also required.

In addition, the relationship between privacy risk and PID behavior was significant in the pooled sample (i.e., South Korea, the US and the UK), but the post-hoc analysis showed that the result was driven by the US and UK group, i.e., in the multi-group analysis, the negative relationship was significant only for the US and UK group. Thus, in the case of individualist culture countries, in particular, there is a need for restaurant managers to make efforts to reduce concerns about privacy loss in the process of collecting personal information. For example, thorough training for restaurant employees is required to prevent exposure of personal information by other customers or restaurant employees during the collection process. Although individuals habitually disclose personal information, and their perception of privacy is changing, new social problems are rapidly increasing due to the loss of privacy. In this situation, the perception that customers' private information is being collected and managed for an appropriate purpose will increase their willingness to visit the restaurant despite disclosing their privacy.

5.4 Limitations and future research

Although the results of this research provide pertinent contributions, this research has several limitations that suggest future study directions. First, the respondents' evaluation of threat appraisal was investigated at a specific point in time. Future research could consider a comparative study with longitudinal measurements to better understand threat situations. In addition, this study, and research applying the privacy calculus model in general, have focused on the initial transaction level, which did not consider the customers' long-term intentions. On the other hand, social exchange theory suggests how perceived costs and benefit calculus are applied in the perspective exchange relationship. Considering this approach, further research is needed to explore these exchange relationships through longitudinal experiments rather than verifying only independent relationships at particular points in time. In addition, future research should expand beyond the cultural dimensions of individualism/collectivism used in this study and examine other individual traits (e.g., the big five personality traits) as moderating variables. It could provide a valuable extension to examining individuals' behavior with regard to personal information disclosure in the context of a pandemic.

6 Conclusion

With the global spread of COVID-19, contact tracing through personal information is being used or explored in a growing number of countries, despite concerns about individual privacy and state surveillance. Although many studies have been conducted, there remains a need for more in-depth research on personal information disclosure in the context of a pandemic. To bridge this gap, this research identified the factors that encourage people to disclose their personal information in restaurants from the perspective of contextual privacy calculation and institutional effects. Specifically, this study examined the threat appraisal of COVID-19, drivers and inhibitors of personal information disclosure, and information privacy behaviors by applying privacy calculus theory (Culnan & Armstrong, 1999) and institutional theory (DiMaggio & Powell, 1983). This research developed and tested a theoretical framework for the relationships between threat appraisal, the drivers and inhibitors of PID, and behaviors relating to disclosing personal information. As a result, it was confirmed that restaurant customers performed situational privacy calculus, and the intrinsic/extrinsic factors affected privacy disclosure behavior. In addition, we verified that there are differences in factors that affect privacy behavior according to cultural differences through post-hoc analysis. Specifically, in the case of individualist culture (as in the US and the UK), even in a pandemic situation, it was found that there was a strong negative relationship between privacy risk and privacy disclosure behavior. As previously discussed, understanding these cultural differences provides essential insights to each government or health authority in a position to regulate customers' information privacy to guide policy direction. In summary, this current study provides a contribution by adding a new “what (collecting personal information for virus contact tracing)” to an existing theory in order to describe “how (threat appraisal, drivers and inhibitor of personal information disclosure)” the relationship unfolds and “when (in the pandemic situation).”, or “for whom (country of residence; cultural difference)” the relationships are likely to be manifested (Whetten, 1989).

Acknowledgements This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A3A2098438).

Declarations No potential conflict of interest was reported by the author(s).

References

Ahmadi, H., Nilashi, M., Shahmoradi, L., & Ibrahim, O. (2017). Hospital Information System adoption: Expert perspectives on an

- adoption framework for Malaysian public hospitals. *Computers in Human Behavior*, 67, 161–189
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211
- Alt, R. (2021). Digital transformation in the restaurant industry: Current developments and implications. *Journal of Smart Tourism*, 1(1), 69–74
- Bagozzi, R. P., & Heatherton, T. F. (1994). A general approach to representing multifaceted personality constructs: Application to state self-esteem. *Structural Equation Modeling: A Multidisciplinary Journal*, 1(1), 35–67
- Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150
- Bashirian, S., Jenabi, E., Khazaei, S., Barati, M., Karimi-Shahanjarini, A., Zareian, S., Rezapour-Shahkolai, F., & Moeini, B. (2020). Factors associated with preventive behaviours of COVID-19 among hospital staff in Iran in 2020: an application of the Protection Motivation Theory. *Journal of Hospital Infection*, 105(3), 430–433
- 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
- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5), 313–324
- Berrone, P., Fosfuri, A., Gelabert, L., & Gomez-Mejia, L. R. (2013). Necessity as the mother of ‘green’ inventions: Institutional pressures and environmental innovations. *Strategic Management Journal*, 34(8), 891–909
- Bhatt, P., Vemprala, N., Valecha, R., Hariharan, G., & Rao, H. R. (2022). User Privacy, Surveillance and Public Health during COVID-19—An Examination of Twitterverse. *Information Systems Frontiers*, 1–16
- Bock, G. W., Zmud, R. W., Kim, Y. G., & Lee, J. N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. *MIS Quarterly*, 29(1), 87–111
- Brewer, N. T., Weinstein, N. D., Cuite, C. L., & Herrington, J. E. (2004). Risk perceptions and their relation to risk behavior. *Annals of Behavioral Medicine*, 27(2), 125–130
- Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing*, 40(1), 108–110
- Burns, L. R., & Wholey, D. R. (1993). Adoption and abandonment of matrix management programs: Effects of organizational characteristics and interorganizational networks. *Academy of Management Journal*, 36(1), 106–138
- Cha, H. S., Wi, J. H., Park, C., & Kim, T. (2021). Sustainability Calculus in Adopting Smart Speakers—Personalized Services and Privacy Risks. *Sustainability*, 13(2), 602
- Chin, A. G., Harris, M. A., & Brookshire, R. (2020). An empirical investigation of intent to adopt mobile payment systems using a trust-based extended valence framework. *Information Systems Frontiers*, 24, 329–347
- Chin, W. W., Peterson, R. A., & Brown, S. P. (2008). Structural equation modeling in marketing: Some practical reminders. *Journal of Marketing Theory and Practice*, 16(4), 287–298
- Churchill, G. A. Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 16(1), 64–73
- Cicchetti, D. V., Shoinralter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement*, 9(1), 31–36
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115
- De Wulf, K., Odekerken-Schröder, G., & Iacobucci, D. (2001). Investments in consumer relationships: A cross-country and cross-industry exploration. *Journal of Marketing*, 65(4), 33–50
- De Zwart, O., Veldhuijzen, I. K., Elam, G., Aro, A. R., Abraham, T., Bishop, G. D., Voeten, H. A., Richardus, J. H., & Brug, J. (2009). Perceived threat, risk perception, and efficacy beliefs related to SARS and other (emerging) infectious diseases: results of an international survey. *International journal of Behavioral Medicine*, 16(1), 30–40
- Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160
- Dinev, T., Albano, V., Xu, H., D’Atri, A., & Hart, P. (2016). Individuals’ attitudes towards electronic health records: A privacy calculus perspective. *Advances in Healthcare Informatics and Analytics* (pp. 19–50). Springer
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389–402
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316
- Ezati Rad, R., Mohseni, S., Takhti, K., Hassani Azad, H., Shahabi, M., Aghamolaei, N., T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study. *Bmc Public Health*, 21(1), 1–11
- Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 19(4), 440–452
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50
- Fox, G., & James, T. L. (2021). Toward an understanding of the antecedents to health information privacy concern: a mixed methods study. *Information Systems Frontiers*, 23(6), 1537–1562
- García-Sánchez, I. M., Cuadrado-Ballesteros, B., & Frias-Aceituno, J. V. (2016). Impact of the institutional macro context on the voluntary disclosure of CSR information. *Long Range Planning*, 49(1), 15–35
- Gasser, U., Ienca, M., Scheibner, J., Sleight, J., & Vayena, E. (2020). Digital tools against COVID-19: Framing the ethical challenges and how to address them. *arXiv preprint arXiv:2004.10236*
- Gefen, D., & Heart, T. H. (2006). On the need to include national culture as a central issue in e-commerce trust beliefs. *Journal of Global Information Management (JGIM)*, 14(4), 1–30
- Gibbs, J. L., & Kraemer, K. L. (2004). A cross-country investigation of the determinants of scope of e-commerce use: an institutional approach. *Electronic Markets*, 14(2), 124–137
- Gutierrez, A., O’Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, 95, 295–306

- Hair, J. F. Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications
- Hartley, K., & Jarvis, D. S. (2020). Policymaking in a low-trust state: legitimacy, state capacity, and responses to COVID-19 in Hong Kong. *Policy and Society*, 39(3), 403–423
- Harman, D. (1967). A single factor test of common method variance. *Journal of Psychology*, 35(1967), 359–378
- Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, 28(3), 463–471
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135
- Houck, B. (2020). Michigan Clarifies Rules for Restaurants Collecting Customer Contact Information. Retrieved July 15, 2022 from <https://detroit.eater.com/21549042/michigan-rules-for-restaurants-collecting-customer-contact-information>
- Huang, Y., Sun, M., & Sui, Y. (2020). How digital contact tracing slowed Covid-19 in East Asia. *Harvard Business Review*, 15(04)
- Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine*, 26(4), 463–464
- Itani, O. S., & Hollebeek, L. D. (2021). Light at the end of the tunnel: Visitors' virtual reality (versus in-person) attraction site tour-related behavioral intentions during and post-COVID-19. *Tourism Management*, 84, 104290
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107, 106260
- Jung, G., Lee, H., Kim, A., & Lee, U. (2020). Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea. *Frontiers in Public Health*, 8, 305
- Kaushik, A. K., Agrawal, A. K., & Rahman, Z. (2015). Tourist behaviour towards self-service hotel technology adoption: Trust and subjective norm as key antecedents. *Tourism Management Perspectives*, 16, 278–289
- Kaushik, K., Jain, N. K., & Singh, A. K. (2018). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications*, 32, 57–68
- Kim, D., & Mah, S. (2020, June 2). South Korea mandates QR codes to log customers after nightclub coronavirus outbreak. Retrieved July 15, 2022 from <https://www.reuters.com/article/us-health-coronavirus-southkorea-qr-code-idUSKBN23907E>
- Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281
- Kokkonen, E. W., Davis, S. A., Lin, H. C., Dabade, T. S., Feldman, S. R., & Fleischer, A. B. Jr. (2013). Use of electronic medical records differs by specialty and office settings. *Journal of the American Medical Informatics Association*, 20(e1), e33–e38
- Kostova, T. (1997). Country institutional profiles: Concept and measurement. *Academy of Management Proceedings*, 1, 180–184
- Krell, K., Matook, S., & Rohde, F. (2016). The impact of legitimacy-based motives on IS adoption success: An institutional theory perspective. *Information & Management*, 53(6), 683–697
- Lang, M., Wiesche, M., & Krcmar, H. (2018). Perceived Control and Privacy in a Professional Cloud Environment. In Proceedings of the 51st Hawaii International Conference on System Sciences, 3668–3677
- Lee, H. (2020). *These Elite Contact Tracers Show the World How to Beat Covid-19*. Retrieved July 7, 2020, from <https://www.bloomberg.com/news/articles/2020-07-25/these-elite-contact-tracers-show-the-world-how-to-beat-covid-19>
- Lee, K., & Pennings, J. M. (2002). Mimicry and the market: Adoption of a new organizational form. *Academy of Management Journal*, 45(1), 144–162
- Lewandowsky, S., Dennis, S., Perfors, A., Kashima, Y., White, J. P., Garrett, P., Little, D. R., & Yesilada, M. (2021). Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. *Plos one*, 16(1), e0245740
- Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62–71
- Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88, 8–17
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471–481
- Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, 31(1), 59–87
- Lin, L., & Martin, T. W. (2020). How coronavirus is eroding privacy. *The Wall Street Journal*, 15(04)
- Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014). Privacy as a trade-off: Introducing the notion of privacy calculus for context-aware mobile applications. *2014 47th Hawaii International Conference on System Sciences*, 1063–1072
- Lu, N., Cheng, K. W., Qamar, N., Huang, K. C., & Johnson, J. A. (2020). Weathering COVID-19 storm: Successful control measures of five Asian countries. *American Journal of Infection Control*, 48(7), 851
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479
- Maiman, L. A., & Becker, M. H. (1974). The health belief model: Origins and correlates in psychological theory. *Health Education Monographs*, 2(4), 336–353
- Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, 47, 120–130
- Nabity-Grover, T., Cheung, C. M., & Thatcher, J. B. (2020). Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media. *International Journal of Information Management*, 55, 102188
- North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge: Cambridge university press
- Ozkan, S., & Kanat, I. E. (2011). e-Government adoption model based on theory of planned behavior: Empirical validation. *Government Information Quarterly*, 28(4), 503–513
- Park, J. (2021). Striking a Balance between Data Privacy and Public Health Safety A South Korean Perspective. Retrieved April 29, 2021, from <https://www.nbr.org/publication/striking-a-balance-between-data-privacy-and-public-health-safety-a-south-korean-perspective/>
- Piccialli, F., Di Cola, V. S., Giampaolo, F., & Cuomo, S. (2021). The role of artificial intelligence in fighting the COVID-19 pandemic. *Information Systems Frontiers*, 23(6), 1467–1497
- 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
- Prasetyo, Y. T., Castillo, A. M., Salonga, L. J., Sia, J. A., & Seneta, J. A. (2020). Factors affecting perceived effectiveness of COVID-19

- prevention measures among Filipinos during enhanced community quarantine in Luzon, Philippines: Integrating Protection Motivation Theory and extended Theory of Planned Behavior. *International Journal of Infectious Diseases*, 99, 312–323
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change I. *The Journal of Psychology*, 91(1), 93–114
- Scott, W. R. (1995). *Institutions and Organizations*. Thousands Oaks, Cal: Sage Publications
- Scott, W. R. (2004). Institutional theory. *Encyclopedia of Social Theory*, 11, 408–414
- Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. *Great Minds in Management: The Process of Theory Development*, 37(2), 460–484
- Scott, W. R., Ruef, M., Mendel, P. J., & Caronna, C. A. (2000). *Institutional change and healthcare organizations: From professional dominance to managed care*. University of Chicago Press
- Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. *IEEE Transactions on Engineering Management*, 1–17
- Sherer, S. A., Meyerhoefer, C. D., Sheinberg, M., & Levick, D. (2015). Integrating commercial ambulatory electronic health records with hospital systems: An evolutionary process. *International Journal of Medical Informatics*, 84(9), 683–693
- Shi, W., Shambare, N., & Wang, J. (2008). The adoption of internet banking: An institutional theory perspective. *Journal of Financial Services Marketing*, 12(4), 272–286
- Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. *Journal of Computer Information Systems*, 49(4), 74–83
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015
- Soares-Aguiar, A., & Palma-dos-Reis, A. (2008). Why do firms adopt e-procurement systems? Using logistic regression to empirically test a conceptual model. *IEEE Transactions on Engineering Management*, 55(1), 120–133
- Soares, A. L. V., Mendes-Filho, L., & Gretzel, U. (2020). Technology adoption in hotels: applying institutional theory to tourism. *Tourism Review*, 76(3), 669–680
- Sreelakshmi, C., & Prathap, S. K. (2020). Continuance adoption of mobile-based payments in Covid-19 context: an integrated framework of health belief model and expectation confirmation model. *International Journal of Pervasive Computing and Communications*, 16(4), 351–369
- Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the royal statistical society: Series B (Methodological)*, 36(2), 111–133
- Strang, D., & Meyer, J. W. (1993). Institutional conditions for diffusion. *Theory and Society*, 22(4), 487–511
- Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571–610
- Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278–292
- Tran, C. D., & Nguyen, T. T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technology in Society*, 67, 101755
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268
- Tsai, M. C., Lai, K. H., & Hsu, W. C. (2013). A study of the institutional forces influencing the adoption intention of RFID by suppliers. *Information & Management*, 50(1), 59–65
- Wang, J., Liu-Lastres, B., Ritchie, B. W., & Mills, D. J. (2019). Travelers' self-protections against health risks: An application of the full Protection Motivation Theory. *Annals of Tourism Research*, 78, 102743
- Wang, L., Yan, J., Lin, J., & Cui, W. (2017). Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking. *International Journal of Information Management*, 37(1), 1428–1440
- Wang, S., Li, J., & Zhao, D. (2018). Institutional pressures and environmental management practices: The moderating effects of environmental commitment and resource availability. *Business Strategy and the Environment*, 27(1), 52–69
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531–542
- Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, 14(4), 490–495
- Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, 2(8), e435–e440
- World Health Organization (2014). Contact Tracing During an Outbreak of Ebola Virus Disease. Retrieved July 15 from <https://www.who.int/csr/resources/publications/ebola/contact-tracing-during-outbreak-of-ebola.pdf?ua%20=%201>
- Wurtele, S. K., & Maddux, J. E. (1987). Relative contributions of protection motivation theory components in predicting exercise intentions and behavior. *Health Psychology*, 6(5), 453
- Xiang, Z. (2021). Journal of Smart Tourism: A New Platform to Support and Define an Emerging Field. *Journal of Smart Tourism*, 1(1), 1–2
- 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
- Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 40(1), 38–51
- Yiu, D., & Makino, S. (2002). The choice between joint venture and wholly owned subsidiary: An institutional perspective. *Organization Science*, 13(6), 667–683

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Eunji Lee is a PhD candidate of Smart Tourism Education Platform (STEP), College of Hotel and Tourism Management at Kyung Hee University, South Korea. She received a master's in Convention and Exhibition Management from Kyung Hee University. Her current research interest focuses on tourism marketing, service strategy, and smart tourism.

Jin-young Kim is an Associate Professor in the College of Hotel & Tourism Management at Kyung Hee University, Republic of Korea. She received her Ph.D. from Cornell University and her Master's degree from Cardiff University in the United Kingdom. Her research interests include smart tourism, corporate finance and consumer behaviour in the hospitality industry. Her work has been published in *Journal of Travel Research*, *Technological Forecasting and Social Change*, *International Journal of Information Management*, *International Entrepreneurship and Management Journal*, *Cornell Hospitality Quarterly*, and so on.

Junchul Kim is a lecturer of Brunel Business School at Brunel University London, UK. His research interests focus on IS strategy, business intelligence, and smart tourism.

Chulmo Koo is a Professor of Smart Tourism Education Platform (STEP), College of Hotel and Tourism Management at Kyung Hee University, South Korea. He is an Editor-in-Chief of *Journal of Smart Tourism* and has a strong record of smart tourism research and scholarship with significant contributions to the tourism field. He has received prestigious research awards and the Kyung Hee Research Fellowship (2018–2020), Excellent Professor of Kyung Hee (2019) at the school level, and the Best Research Paper Award in the ENTER (2015) conference at the IFITT (International Federation of IT and Travel & Tourism). He is appointed as the top 2 % researcher in 2021, 2022 from Stanford University and Elsevier.