Information Systems Frontiers (2024) 26:1435–1451
https://doi.org/10.1007/s10796-023-10420-7

Is Contact Tracing for Pandemic Relief or Privacy Menace?: a Lens of Dual-Calculus Decision

Eunji Lee[1] · Chul Woo Yoo[2] · Jahyun Goo[2] · Kichan Nam[3] · Chulmo Koo[1]

Accepted: 25 June 2023 / Published online: 17 July 2023

Abstract
South Korea endured early outbreaks and flattened the coronavirus curve without paralyzing economic systems. The critical factor that leads to the policy's success is contact tracing using personal information. However, at the same time, the extensive use of personal information has raised social problems related to privacy loss. Even in devastating pandemics, balancing personal privacy and public safety remains a crucial issue. Thus, this study attempted to gain a deeper understanding of privacy disclosure for restaurant customers. We applied privacy calculus theory and risk-risk trade-off concepts to explain the relationship between two conflicting risks. i.e., privacy risk and health risk. We found that "risk substitutions" provide implications for how customers' privacy perceptions change with the level of health risk and the importance of perceived benefit. Finally, we verified that institutional privacy protection directly influences disclosure intention. This study has implications for theory and practice.

Keywords Privacy calculus · Risk-risk trade-off · Institutional privacy protection · Information privacy disclosure · Restaurants customer · COVID-19 pandemic

1 Introduction

Given the severity of COVID-19, the government has introduced measures to prevent and control the spread of diseases. Among many countries, South Korea has emerged as an example to emulate in pandemic situations (Kim & Denyer, 2020). In particular, significant factors that led to the success of South Korea's quarantine policy include government-driven communication, national infectious disease plans, and stringent contact tracing (You, 2020). One of the effective measures is regarded as "contact tracing." In efforts to conduct contact tracing during the pandemic, South Korea has accessed individual personal information to track the route of infected people and their distribution in the region (Jung et al., 2020). Specifically, the government mandated personal information disclosure such as personal contact information (phone number, address) and visit records (name, visit time) for admission to multi-use facilities (e.g., restaurants, tourism facilities) and used it for contact tracing. However, this effective measure has opened up a healthy debate on how to balance the benefits of privacy and public health.

Considering pandemic is an unprecedented circumstance that poses enormous health risks potentially affecting people worldwide, the Korean governments have put public health and safety issues before the individual privacy concerns (Han et al., 2020). All the pandemic protocols across all governments and private companies, as a result, have promoted and acknowledged the use of personal information as a critical measure for mitigating the spread of the virus while easing lockdown measures (Gasser et al., 2020). For

✉ Chulmo Koo
helmetgu@khu.ac.kr

Eunji Lee
edreamerj@khu.ac.kr

Chul Woo Yoo
yooc@fau.edu

Jahyun Goo
jgoo@fau.edu

Kichan Nam
knam@aus.edu

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

[2] Florida Atlantic University, Boca Raton, FL, USA

[3] School of Business Administration, Department of Marketing and Information Systems, American University of Sharjah, Sharjah, United Arab Emirates

these reasons, policymakers enforce "implicit" consent to the use of information privacy (Ahn et al., 2020), leaving out privacy infringement issues overlooked (Bhatt et al., 2022). With concerns regarding the "dossier effect"[1] (Goldberg et al., 1997), however, privacy advocates and some media outlets have started pointing out a possibility of mismanaging vast amounts of data with the risk of leakage, stressing that privacy breaches may have emerged as social problems. For example, problems have arisen in pursuing potent public purposes in the pandemic due to unexpected possible privacy losses, such as online trolling of infected people, unintended uses of collected data for marketing purposes, and excessive government surveillance and control (Brough & Martin, 2021; Ribeiro-Navarrete et al., 2021).

As such, the current situation of complying with the pandemic protocol of personal information collection in an effort of mitigating the community health risks poses unique challenges that requires us to balance these two conflicting risks (i.e., privacy and health risks). Literature in individual psychology suggest that facing such conflicting expectations is considered aversive, since recruiting cognitive control to resolve conflict is effortful (c.f., Freeston et al., 1994). Therefore, it is important to identify ways people simultaneously address these two infectious diseases-driven, conflicting risks. Moreover, although there has been numerous privacy research on generic online environments, privacy disclosure in pandemic situations has the following contextual differences compared to previous studies. First, privacy disclosure in using services (e.g., restaurants, tourism facilities, etc.) can be seen as an act in response to the threat of viruses. It means that in a pandemic situation, an individual simultaneously recognizes threats from viruses and concerns of privacy loss. Similarly, Tran and Nguyen (2021) demonstrated that health risk and privacy risk have conflicting influences on contact tracing applications use. Second, privacy disclosure in restaurants is implemented under institutional pressure. Thus, it is noteworthy that "privacy disclosure" is directly related to the "requirement to use a restaurant." On the other hand, prior research at the individual level on information privacy disclosure in a pandemic situation mainly focused on the voluntary installation or use of contact tracing applications (e.g., Dzandu, 2023; Fernandes & Pereira, 2021; Fox et al., 2022; Hassandoust et al., 2021). Further, prior studies have looked into the independent effects of conflicting factors such as privacy calculus and institutional or environmental factors on behavioral responses. Those differences demonstrate a clear research gap in the extant literature and call for a new approach to examine the phenomena.

Thus, in this study, we address the following issue of individual decision-making under regulatory pressure in this conflict of the privacy protection and the physical health: Which comes first, individual privacy rights or collective protection from virus infection? In particular, we focus on the context of personal information disclosure in the restaurant because this is the most common case where individuals make a decision every day. To answer our research question, we conceptualized the dual-calculus of privacy disclosure by applying the privacy calculus theory and the concept of risk-risk tradeoff. Further, considering that privacy disclosure at restaurants is being implemented at the level of quarantine policy from the institutional perspective, we tried to confirm the influence of institutional privacy protection.

This study investigates individuals' awareness and behavior regarding information privacy under the threat of infectious diseases, providing meaningful insights that can be applicable in future pandemic situations. Specifically, this study makes several contributions. First, the study shows how risk-risk trade-off occurs when people deal with the conflicting consequences of health risks and privacy risks with respect to information disclosure in the pandemic situation. Second, this study extends the privacy calculus frame by incorporating the fully mediating role of perceived benefit between health risks and information disclosure in the pandemic contexts. Third, this study suggests the impacts of regulations on individual decision making by investigating the moderating effects of institutional privacy protection between privacy calculus factors and privacy disclosure.

2 Literature Review

2.1 Privacy Calculus in COVID-19 Pandemic Situations

Laufer and Wolfe (1977) developed the privacy calculus theory, and then Culnan and Armstrong (1999) applied this concept in the information system field, so called information privacy. In the privacy calculus framework, costs often involve the loss of an individual's privacy, and benefits refer to context-specific gains that an individual expects in return for personal information provided by the individual. From the commodity view, privacy can be interpreted as an economic value, and individuals entail a subjective cost-benefit analysis when asked to disclose information (Smith et al., 2011). Based on this tradeoff calculus analysis, disclosure occurs when the benefit is expected to be greater than the privacy risk (Dinev & Hart, 2006). This approach aligns with social exchange theory (Homans, 1961), which explains that people engage in exchange situations only if they expect the net result to be positive.

[1] Since the late 1990s, concerns have been raised regarding the "dossier effect" that collecting a large number of innocuous data points could easily be de-anonymized and create a combined dataset with a startling amount of personal.

Acquisti et al. (2015) argued that privacy calculus depends on the context because individuals are willing to provide personal information in return for certain benefits while taking extreme measures to protect it at different times and situations. In other words, it can be understood that under what circumstances privacy exchange takes place and what benefits are given to individuals are the primary motivators for disclosure. Thus, information privacy research applying the privacy calculus mechanism has been attempted in various research contexts such as E-commerce (Fernandes & Pereira, 2021), social networking sites (Trepte et al., 2020), and mobile applications (Zhu et al., 2021). These previous studies have highlighted the importance of non-financial benefits like convenience, lower search cost, and better service gained from disclosing personal information in adopting new technologies or services in an online environment from a consumer perspective. On the other hand, most studies in the hospitality and tourism sectors have focused on the perception and behavior of information privacy disclosure when using applications for hotel or restaurant services (Kang & Namkung, 2019; Morosan & DeFranco, 2015). Specifically, Kang and Namkung (2019) examined consumers' behaviors toward personalized services offered by mobile applications in the food service industry. They verified that significant influence relationship only in the relationship between the perceived benefit and value to disclosure. In this way, the need to specify the characteristics and situations of the study object is raised in that the interpretation and results in empirical research were inconsistent.

On the other hand, as privacy violation issues emerged in the COVID-19 situation, studies applying privacy calculus theory have provided valuable insights. For example, as shown in Table 1, empirical studies commonly focus on verifying the independent effects of risk and benefit for voluntary use or installation of contact tracing applications (CTA). In addition, the benefit of using CTA takes a perspective on the diagnosis of individual health (Fox et al., 2022), the acquisition of health-related information (Carlsson Hauff & Nilsson, 2021), and the public interest of society (Abramova et al., 2022; Hassandoust et al., 2021). In other words, it suggests that the benefits of providing privacy under the pandemic are related to safety against infectious diseases that unlike pre-pandemic studies.

Although these studies are meaningful in understanding how information privacy works in an extraordinary situation and how people behave under health threats, they do not clearly show how two different risks, i.e., privacy risk and health risk, work in tandem in the calculus framework. Therefore, this study attempts to examine main effects, interaction effects and mediation effects of privacy risk and health risk on perceived benefit and personal information disclosure intention.

2.2 Risk-Risk Tradeoff: Health Risk Vs. Privacy Risk

The concept of risk is one of the most prevalent frames in understanding the human decision making. Bauer (1960) originally conceptualized that risk comprises a two-dimensional structure: uncertainty and consequences. Following these two principal dimensions of perceived risk, in the consumer behavior literature, a number of studies have been conducted to identify sub-factors of risk. Typically, Jacoby and Kaplan (1972) have classified types of perceived risk including financial, performance, social, psychological, and physical risk. The subcategories of risk are clearly distinguished, but in certain situations, various risks can occur simultaneously. Thus, consumer engage in risk "tradeoff" behavior, which is the process of assessing overall risk in certain situations where they perceive several independent risks (Roselius, 1971).

In a similar vein, the concept of risk-risk tradeoff was proposed to develop a methodology for measuring the values that individuals place on morbidity risk reductions and measuring the benefits of reducing the risks of contracting diseases (Viscusi et al., 1991). Further, Graham et al. (1995) academically defined these concepts that "the change in the portfolio of risks occurs when a countervailing risk is generated (knowingly or inadvertently) by an intervention to reduce the target risk." in the health and environmental policies context. A general issue within this concept is that efforts to combat a "target risk" can unintentionally foster an increase in "countervailing risks." (Hansen & Tickner, 2008). Countervailing risks are commonly known by "side effects (e.g., medicine)." "collateral damage (e.g., military tactics)," or "unintended consequences (e.g., public policy)." Graham et al. (1995) were also classified into four categories of risk-risk tradeoff as follows; (1) *Risk transfer*: when the same risky outcome is shifted from one group to another; (2) *Risk offset*: when the same adverse outcome is created in the target population; (3) *Risk substitution*: when one type of adverse outcome is replaced by another adverse outcome in the same target population; (4) *Risk transformation*: when the countervailing risk is different in both outcome and affected population.

On the other hand, this concept primarily has been applied for decision-making at the organizational level, and a few studies adopted this concept at the individual level in the context of medical or health tradeoff decisions (Shimshack & Ward, 2010) and drug advertising effectiveness (Aikin et al., 2019). Further, Tran and Nguyen (2021) applied the risk-risk tradeoff model to examine the COVID-19 contact-tracing app use's decision from the perspective of health risk minimizations. These previous studies suggest the importance of guidance on which risks are more influential to individuals and which risks should be managed first for decision-making. Decision-making is a focal interest in

Table 1 Empirical studies in the pandemic situations

IV	DV	Findings	Reference
(1) Contact tracing benefits (2) Risk beliefs	Intention to install contact tracing app (CTA)	Individuals' intention to install a CTA is influenced by their risk beliefs, perceived individual/ societal benefits to public health, privacy concerns, privacy protection initiatives (legal and technical protection), and technology features (anonymity and use of less sensitive data).	Hassandoust et al. (2021)
(1) Aspects of benefit -Perceived pro-social usefulness -Perceived utilitarian Usefulness -Perceived hedonic usefulness (2) Aspects of risk -Privacy concern	Willingness to use contact tracing app	The results indicate significant privacy concerns with using contact-tracing apps. Also, perceived hedonic and pro-social positive positively affected willingness to use CTA.	Carlsson Hauff and Nilsson (2021)
(1) Aspects of benefit -Health benefit -Reciprocal benefit (2) Social influence (3) Perceived privacy	Future Usage intention Willingness to disclose information app	Integrating privacy calculus theory with social contract theory to include reciprocity and social influence, findings suggest that perceived privacy, two kinds of benefits, and social influence all positively influence individuals' intentions to download or continue the use of contact tracing applications.	Fox et al. (2022)
(1) Perceived health risk (2) Perceived privacy risk (3) Perceived value	App usage	Based on the privacy calculus theory and the risk-risk tradeoff concept, the research suggested that the risk-risk tradeoff model and verified perceived health risk and perceived privacy risk has conflicting influence on perceived value and app usage.	Tran and Nguyen (2021)
(1) Individual benefits (2) Individual privacy risks (3) Social benefit (4) Social risks	Acceptance of CTA (before/after the launch of the apps)	Based on the privacy calculus model, this study theorized that users hold social considerations (i.e., social benefits and risks) as well as individual privacy calculus that affecting their acceptance decisions.	Abramova et al. (2022)

individual level research; because individual involve making difficult trade-offs and constantly make decision about the selection (Luce et al., 2001).

Considering our research context, this framework provides a useful lens. In the study, privacy risk can be regarded as countervailing risk because it is unintentionally made in reducing the health risk in the Pandemic context. We expect risk substitution happens here. It can be further assumed that when, as target risk, the health risk is strong, this substitution can be easier. In other words, it can be perceived that the necessary steps that are designed to reduce the health risk brings more benefits although this does not require any additional actions. As a result, the influence of privacy risk reduces, perceived benefit increases and it can lead to strong disclosure intention. Integrating this lens gives additional insight into the extant privacy calculus frame.

Thus, we applied this mechanism and tried to verify the risk-risk tradeoff statistically. As mentioned above, the target risk refers to the health risk of COVID-19 and countervailing risk generated when personal information is collected as a privacy risk. In other words, health and privacy risks can be understood as conflicting concepts, and this study focused on verifying the tradeoff relationships. Privacy issues are directly related to customer consumption or visits in the tourism and hospitality sectors. Therefore, our

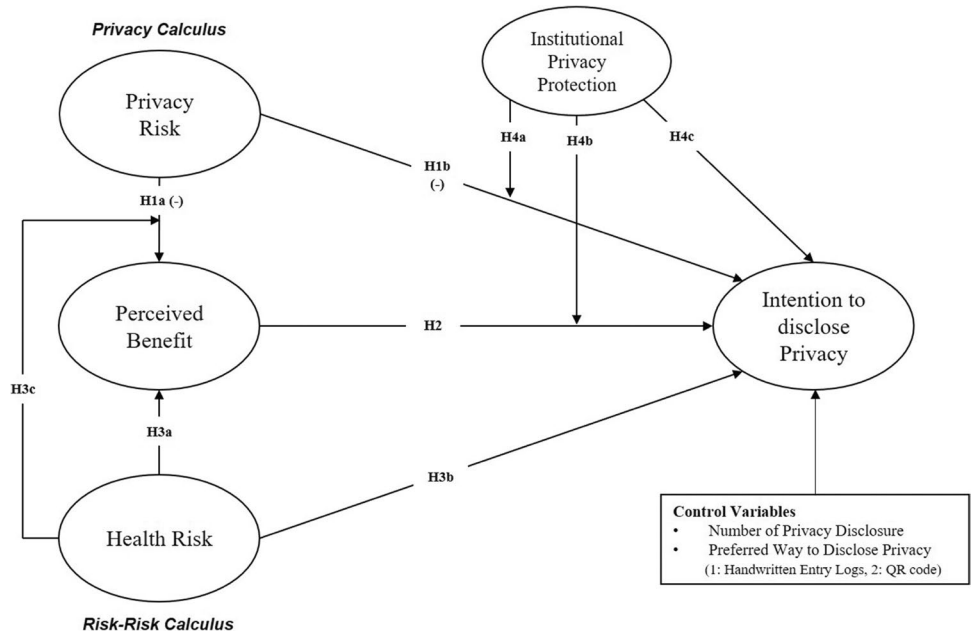

Fig. 1 Research model

approach is considered that it will provide meaningful insights through the understanding of the mental process of customers trying to disclose information privacy in restaurants.

2.3 COVID-19 and Institutional Privacy Protection

Pandemic has put immediate policy pressure on society to adapt and produced new health solutions (Weible et al., 2020). During such extraordinary times, the spread of virus has accelerated the adoption of various emerging technologies (Parker et al., 2020). Further, the urgency of the novel infectious diseases has led the government to readjust its priorities, and the most common evidence is that several governments implemented the collection of sensitive personal information for purpose of protecting public health against COVID-19 (Li et al., 2022). Accordingly, arguments on the role of government and the evaluation of quarantine policies between countries during the pandemic have continued (Margherita et al., 2021). On the other hand, in the context of South Korea, quarantine strategies using visit logs in the restaurant have been recognized as effective strategies worldwide. That is, this pandemic has allowed "privacy protection" and "compliance" in the hospitality sector to re-examining. Thus, this study deals with "collection of personal information in restaurants", which was exceptionally applied to prevent the spread of COVID-19.

3 Research Model and Hypothesis Development

Based on the conceptual model, our research model is illustrated in Fig. 1.

3.1 Hypothesis Development

3.1.1 Privacy Calculus

Privacy risk is defined as the degree to which an individual believes there is a high potential for loss associated with the release of personal information (Malhotra et al., 2004). In this study, privacy risk refers to the potential loss due to losing control of their personal information without the permission of restaurant customers (Park & Tussyadiah, 2017). In general, consumers are more willing to consent to their personal information release, when they are informed about the vendor's information practice and consider the business as fair to them (Culnan & Armstrong, 1999). This logic is aligned with the utility maximization theory from the economic science (U(x) = Benefit – Cost) (Rust et al., 2002) and the social exchange theory of social psychology (Homans, 1961). Following this mechanism, the relationship between risk and benefits verified have negative correlations (Awad & Krishnan, 2006; de Groot et al., 2020). Regarding the relationship between two privacy calculus factors, Nasser and Nasser (2020) examined that privacy risk concerns have negative impact toward benefit to disclose personal information when they use E-government platforms. Thus, we hypothesize:

H1a: Privacy risk negatively influences perceived benefit.

The other construct, perceived benefits, has been interpreted from various perspectives depending on the context of the study, such as "financial rewards," "personalization," and "social adjustment benefit" (Smith et al., 2011). In

this study, perceived benefit refers to any possible benefit that individual can obtain through disclosing the personal information at the restaurant. Individuals who disclose the information can receive notifications later whether they were exposed to possible COVID-19 infects in the restaurant or the near area. And it tuns out they were infected, in information can be used to help other people too, vice versa.

On the other hand, privacy violations emerged during the pandemic, and studies related to adopting contact tracing applications (CTA) have been conducted. For example, Individual behavior to install CTA acts as a driver of perceived individual/societal benefits toward public health, despite the significant negative effect on risk beliefs (Hassandoust et al., 2021). Also, the individual benefits and individual privacy risk directly make opposite impacts on acceptance of CTA (Abramova et al., 2022). Thus, we hypothesize:

H1b: Privacy risk negatively influences intention to disclose privacy.
H2: Perceived benefit positively influence intention to disclose privacy.

3.1.2 Health Risk

Health risk is generally defined as potential unfavorable consequences that may occur from health hazards caused by internal and external factors (Leppin & Aro, 2009). In particular, in this study, health risk refers an individual's perception about the potential health loss due to COVID-19. Health risk has represented a central structure in many theories to understand individual protective motivations and behavior (Maiman & Becker, 1974; Rogers, 1975). Further, with epidemics situations, several empirical studies from health psychology have examined the positive relationship between risk perception and precautionary responses. Specifically, perception of likelihood (i.e., cognitive belief) and severity of infection worry (i.e., affective beliefs) leads to protective actions such as hygiene behaviors (Magnan et al., 2021). Notably, mobile-based banking transactions are considered to be affected by social distancing mechanisms, and perceived health threats significantly affect the adoption of mobile payment services (Sreelakshmi & Prathap, 2020). On the other hand, in this study, privacy disclosure can be regarded as a protective action against COVID-19 in that the purpose of "privacy utilization" is "prevention of public and individual infection." In a similar vein, Tran and Nguyen (2021) also interpreted the use of contact tracing applications as a precautious behavior against the virus, confirming that health risks positively influence the perceived value and use of CTA. Thus, we hypothesize:

H3a: Health risk positively influence perceived benefit.
H3b: Health risk positively influence intention to disclose privacy.

3.1.3 Risk-Risk Calculus

Risk-risk tradeoff occur when regulators focus on reducing one particular risk in one area, which may result in other areas that are not originally considered (Graham et al., 1995). We focused on risk-substitution, which means that one type of adverse outcome in the same target population is replaced by another adverse outcome. The COVID-19 virus has caused many deaths and high infection rates worldwide, and social and institutional measures have been taken for public safety. In other words, health-threatening situations can be seen as a significant target risk, suggesting that government measures to compensate for this can create a new countervailing risk (i.e., information privacy) (Yeong-Tsyr Wang et al., 2021). Following the logic of this concept, we consider that negative influence of privacy risk on perceived benefit can be weaker in the group of individuals with high health risk perception compared to the group of individuals with low health risk. In other words, because the direct relationship between privacy risk and perceived benefit was hypothesized positive previously, the moderating relationship is assumed positive here. Therefore, we hypothesize the following.

H3c: Health risk weakens the relationship between privacy risk and perceived benefit.

3.1.4 Institutional Privacy Protection

The current study operationally defines *institutional information protection* as the degree of belief in the government's efforts to provide accurate and reliable information as part of individual information protection practices. On the other hand, organizational information practices lead to consumer privacy concerns about information privacy and can cause various privacy-violation issues (Solove, 2007). Thus, from an administrator's point of view, privacy protection efforts have been required to reduce consumers' privacy risk perception. Privacy protection is composed of technical practices and solutions, such as compliance with users' authorization, presenting a statement of the privacy policy, and ensuring user awareness of information collections (Culnan & Bies, 2003). The perception of privacy protection has been considered a factor in reducing privacy concerns in online environments (Hong et al., 2019). In other words, institutional factors crucially influence the individual's attitude and decision to disclose information (Chen et al., 2017). Further, institutional privacy assurances (i.e., privacy policy and industry self-regulation) lead to reduce risk-control assessment (i.e., privacy control and privacy risk) (Xu et al.,

2011). In pandemic situations, the government takes the lead in various quarantine policies, including collecting personal information about restaurant customers. In this process, the trust of institutional policy gives legitimacy to its compliance (Hartley & Jarvis, 2020; Li et al., 2022), which can also lead to privacy disclosure behavior. In other words, it suggests that efforts at the institutional level can act as a factor that moderates the relationship between the perception of customer information privacy and behavior response. We therefore hypothesize:

H4a: Institutional privacy protection weakens the relationship between privacy risk and intention to disclose privacy.
H4b: Institutional privacy protection strengthens the relationship between perceived benefit and intention to disclose privacy.
H4c: Institutional privacy protection positively influences intention to disclose privacy.

4 Methodology

4.1 Data Collection and Sample

The population of this study is customers those who had experienced providing personal information via QR codes and hand-written entry logs at the restaurant. Data collection through an online survey was performed from December 23 to December 31, 2020. Access to potential respondents in South Korea was obtained through a marketing research firm, and a quota sampling approach was implemented considering age dependency ration of South Korea.

Initially, data were collected from 317 respondents. However, responses from participants who did not meet the eligibility criteria based on screening questions about restaurant visits during the period of personal information collection at multiple facilities were removed. As a result, a total of 311 samples were included in the final analysis. Regarding respondent information, the survey contained two items associated with past experience of personal information disclosure (i.e., number of disclosing personal information, the preferred way to disclose personal information), and six socio-demographics questions. The detailed demographic information of the respondents is shown Table 2.

4.2 Measurements

To ensure content validity, constructs of this study were adapted from previous studies with minor wording amendments in the context of COVID-19 situations. Privacy risk was assessed with four items derived from Morosan and DeFranco (2015) and Xu et al. (2011). Also, health risk was assessed using 4 items derived from De Zwart et al. (2009) and Prasetyo et al. (2020). To measure the perceived benefit, we adapted four items from previous research (Dinev et al., 2016; Fahey & Hino, 2020), and modified them to fit the context of our study. Four items were adapted from Hassandoust et al. (2021), and Hong et al. (2019) to measure institutional privacy protection. Last, to assess intention to disclose privacy, four items were drawn from Bulgurcu et al. (2010). All items were measured on a seven-point Likert-type scale. Appendix Table 5 presents operational definitions, and each survey item adequately modified according to the present research context.

We included two control variables: number of privacy disclosure and preferred way to disclose privacy. Previous literatures have shown that previous experience on privacy disclosure reduce people's privacy risk and enhance willingness to disclosure individual information privacy (Bansal et al., 2016; Li et al., 2020; Meinert et al., 2006). Once habits are formed, related behaviors can be triggered automatically by specific situational cues (Aarts et al., 1997). In this context, we assume that a higher frequency of personal information disclosure can induce habitual decision-making, potentially leading to subsequent behaviors that require less deliberation. Moreover, the convenience and accessibility of information provision methods can influence people's behaviors, particularly in situations involving sensitive information (Metzger, 2006). For these reasons, we intend to control these situational factors associated with personal information disclosure.

5 Results and Analysis

The current study is more prediction-oriented because it aims to explore the dual-calculus relationship between conflicting variables for privacy disclosure in the South Korea context. Thus, PLS-SEM method is a suitable to address our research questions.

5.1 Measurement Model

Given that this study measured in a pandemic situation, EFA and CFA were performed for thorough assessment of the measurement model. Table 3 show reliability and validity of the constructs. The composite reliability of all constructs ranges from 0.925 to 0.974. In additions, Dillon-Goldstein's rho value range from 0.925 to 0.974. For measurement validity, we assessed the convergent and discriminant validity. All factor loadings were satisfactory, and the average variance extracted (AVE) from

Table 2 Demographics information ($n = 311$)

Variable	Content	Frequency (%)
Gender	Male	156 (50.2%)
	Female	155(49.8%)
Age	19 or younger	–
	20 ~ 29	71 (22.8%)
	30 ~ 39	71 (22.8%)
	40 ~ 49	64 (20.6%)
	50 ~ 59	63 (20.3%)
	60 or order	42 (13.5%)
	No response	–
Marital statues	Single	126 (40.5%)
	Married	185 (59.5%)
Education	Secondary School	52 (16.7%)
	Trade/Vocational/College School	37 (11.9%)
	Bachelor's degree	188 (60.5%)
	Master's degree or higher	34 (10.9%)
Monthly income	$1999 or below	62 (19.9%)
	$2000 - $2999	99 (31.8%)
	$3000 - $3999	65 (20.9%)
	$4000 - $4999	39 (12.5%)
	More than $5000	46 (14.8%)
Years on the use of Smartphone	Less than 3 years	40 (12.9%)
	3 years - within 5 years	23 (7.4%)
	5 years - within 10 years	89 (28.6%)
	More than 10 years	159 (51.1%)
Number of disclosing PI	1 ~ 2	16 (5.1%)
	3~	48 (18.6%)
	6 ~ 9	56 (18%)
	More than 10 times	181 (58.2%)
Preferred method of disclosing PI	Handwritten entry logs	78 (25.1%)
	QR code	233 (74.9%)
	No response	–

all constructs ranges from 0.758 to 0.903 (AVE > 0.50), supporting convergent validity. Discriminant validity is assessed on the basis of the heterotrait–monotrait ratio of correlations (HTMT) to establish more rigorous discriminant validity. All HTMT values of the latent variables were below the critical value of 0.85 (from 0.091 to 0.762).

Further, we conducted Harman's single-factor to examine whether common method bias was present in the data set. We performed an exploratory factor analysis (EFA), and unrotated factor solutions were examined. The EFA results delineated four dimensions (Eigenvalue >1) and each dimension explained 10.661% to 37.045% of the covariation among the measures. As none of the factors accounted for more than 50% of the covariation, it was concluded that there is little concern regarding common method bias.

5.2 Structural Model

We diagnosed variance inflation factor (VIF) to detect multicollinearity of each independent variables. Multicollinearity issue was not founded because all value of VIF show between 1.003 and 1.337. Also, to check the predictive power, the R^2 of variance explained for perceived benefit (14.8%), and intention to disclose privacy (58.9%) were calculated. The f^2 values (effect size) in this study were calculated to range from 0.006 (indicating minor impact) to 0.694 (indicating major impact) based on Cohen (1992). Additionally, we conducted PLS predict analysis to verify the predictive performance. Predictive validity suggests that a specific set of measures for a particular construct can predict a given outcome variable (Shmueli et al., 2016). Following the approach proposed by Chin (2010) and Evermann and Tate (2012), which is a modified version of the jackknife

Table 3 Measurement model

Constructs Factors	Health Risk	Privacy Risk	Perceived Benefit	Institutional Privacy Protection	Intention to Disclose Privacy	Measures Constructs	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted	Mean	Standard Deviation
HRISK1	0.918	0.034	0.134	0.037	0.127	Health Risk	0.912	0.946	0.944	0.809	5.044	1.086
HRISK2	0.920	0.040	0.144	0.026	0.086							
HRISK3	0.825	0.054	0.066	0.053	0.031							
HRISK4	0.869	0.055	0.151	0.064	0.143							
PRISK1	0.055	0.894	−0.054	−0.017	−0.055	Privacy Risk	0.934	0.94	0.953	0.835	4.553	1.146
PRISK2	0.035	0.916	−0.025	−0.004	−0.052							
PRISK3	0.053	0.903	−0.033	−0.038	−0.090							
PRISK4	0.035	0.923	−0.007	−0.045	−0.085							
BEN1	0.149	0.053	0.775	0.080	0.353	Perceived Benefit	0.928	0.93	0.949	0.823	5.457	0.945
BEN2	0.155	−0.065	0.812	0.166	0.331							
BEN3	0.171	−0.014	0.852	0.154	0.336							
BEN4	0.141	−0.114	0.810	0.186	0.327							
PRO1	−0.012	0.096	0.158	0.785	−0.073	Institutional Privacy Protection	0.894	0.948	0.925	0.758	4.626	1.093
PRO2	0.074	−0.093	0.188	0.841	0.179							
PRO3	0.052	−0.075	0.066	0.881	0.268							
PRO4	0.081	−0.058	0.069	0.885	0.210							
INT1	0.164	−0.073	0.342	0.164	0.837	Intention to Disclose Privacy	0.964	0.964	0.974	0.903	5.5619	1.018
INT2	0.118	−0.111	0.387	0.171	0.835							
INT3	0.100	−0.094	0.346	0.153	0.865							
INT4	0.102	−0.115	0.363	0.181	0.850							

*Seven-point Likert-type scale; Principal Components Analysis with Varimax Rotation (KMO measures of sampling exceed of 0.5, and Batlett's test of sphericity: $p < 0.001$)

Fig. 2 Structural model results

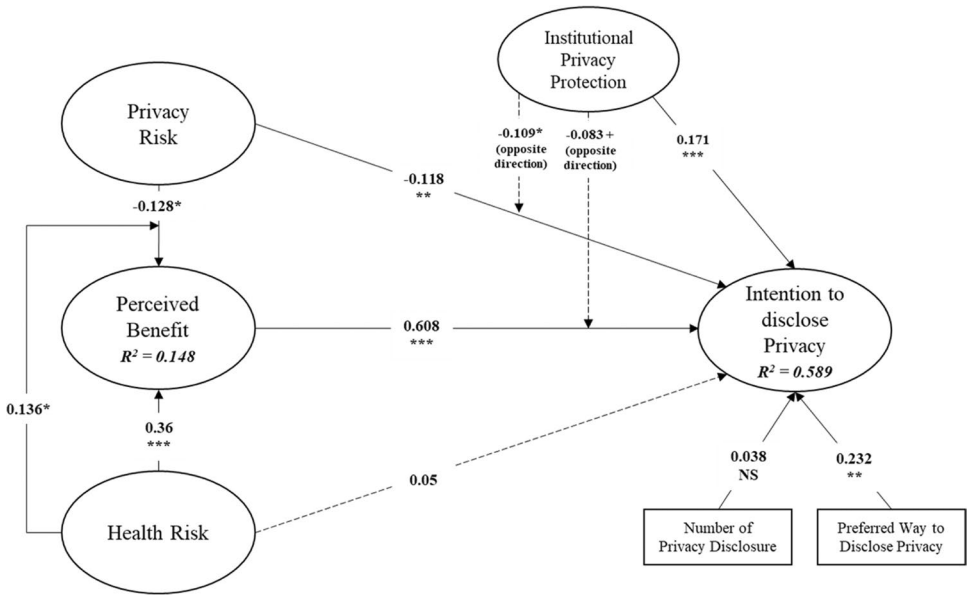

Table 4 Results of hypothesis testing

Main direct effect					
Hypothesis	Path	β	T-statistic	*P* value	Result
H1a	Privacy risk → Perceived benefit (−)	−0.128	2.155	0.031*	Supported
H1b	Privacy risk → Intention to disclose Privacy (−)	−0.118	2.818	0.005**	Supported
H2	Perceived benefit → Intention to disclose Privacy	0.608	14.894	0.000***	Supported
H3a	Health risk → Perceived benefit	0.360	6.809	0.000***	Supported
H3b	Health risk → Intention to disclose Privacy	0.050	1.190	0.234	Not Supported
H4c	Institutional privacy protection → Intention to disclose Privacy	0.171	3.969	0.000***	Supported
Moderating effect[a]					
Hypothesis	Path	β	T-statistic	*P* value	Result
H3c	Health risk × Privacy risk → Perceived benefit	0.136	1.961	0.050*	Supported
H4a	Institutional privacy protection × Privacy risk → Intention to disclose Privacy	−0.109	2.000	0.046*	Not Supported (opposite direction)
H4b	Institutional privacy protection × Perceived benefit → Intention to disclose Privacy	−0.083	1.873	0.061	Not Supported
Mediating effect					
Mediator	Path	β	T-statistic (*p* value)	VAF[b]	Result
Perceived benefit	Health risk → Perceived benefit → Intention to disclose privacy	0.219	6.32***	0.814	Full mediations
	Privacy risk → Perceived benefit → Intention to disclose privacy	−0.078	2.123*	0.397	Partial mediations

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$; [a] product-indicator approach; [b] *VAF* Variance Accounted For

approach, we calculated Q^2 based on blindfolding. The resulting Q^2 values were 0.121 for perceived benefit and 0.528 for intention to disclose privacy, demonstrating the predictive relevance of the model ($Q^2 > 0$).

Next, we conducted bootstrapping method with 5000 subsamples to test our research hypothesis. Figure 2 and Table 4 indicate the results with path coefficients on our research model. Specifically, the result suggest that privacy risk negatively affects perceived benefit (β = −0.128; t = 2.155; $p < 0.05$), supporting H1a. Also, privacy risk has a significant negative impact on intention to disclose privacy (β = −0.118; t = 2.818; $p < 0.01$), which supports H1b. Regarding health risk, it positively strong affects perceived benefit (β = 0.36; t = 6.809; $p < 0.001$; supporting H3a), whereas it has not significant effect on intention to disclose privacy (β = 0.05; t = 1.19; not supporting H3b). Further, intention to disclose privacy was positively affected by perceived benefit (β = 0.608; t = 14.894; $p < 0.001$;

supporting H2), and institutional privacy protection (β = 0.171; t = 3.969; $p < 0.001$; supporting H4c).

Regarding the moderators, our interaction terms are "quasi" moderators, since the two moderators (i.e., health risk and institutional privacy protection) are hypothesized to direct impact on dependent variables (i.e., perceived benefit and intention to disclose privacy). The interaction term was calculated through the product-indicator approach that multiplies indicators of the independent variables by the indicators of the moderator variable in reflective model. The testing results showed that health risk positively moderates the relationship between privacy risk and perceived benefit (β = 0.136; t = 1.961; $p < 0.05$; supporting H3c). However, contrary to our expectations, institutional privacy protection negatively moderates the relationship between privacy risk and intention to disclose privacy (opposite directions; β = −0.109; t = 2.00; $p < 0.05$). Further, institutional privacy protection has not significant moderating effects between privacy risk and intention to disclose privacy. Thus, H4a and H4b are not supported. Lastly, as control variables, number of privacy disclosure has not significant effects on intention to disclose privacy (β = 0.038; t = 1.055), whereas preferred way to disclose privacy significantly influenced intention to disclosure (β = 0.232; t = 2.597; $p < 0.01$).

To confirm the role of perceived benefit, we performed the meditating analysis through PLS bootstrapping method using 5000 subsamples. Health risk has positive indirect effects on the intention to disclose privacy through perceived benefit (β = 0.219; t = 6.32; $p < 0.001$). Also, privacy risk has negative indirect effects on the intention to disclose privacy through perceived benefit (β = −0.078; t = 2.123; $p < 0.05$). However, Hair Jr et al. (2014) stated that if the indirect effect is significant, the size of the indirect effect has to be evaluated by "Variance Accounted For" (VAF; indirect effect/total effect) to confirm the exact role of mediator. Following this, we additionally calculated the VAF value of perceived benefit. If the VAF is more than 20%, and less than 80% it interprets partial mediation, and if the VAF is larger than 80%, it means full mediation. We confirmed that the perceived benefit is partial mediator on relationships between privacy risk and intention to disclose privacy (VAF = 0.397), and full mediator on health risk response to intention to disclose privacy (VAF = 0.814).

6 Discussion and Conclusion

The main findings of this study are as follows. First, the results of this study demonstrated the dual-calculus decision-making for restaurant customers. Specifically, Fig. 3 describes the relationship between privacy risk, perceived benefit, and health risk. Our finding shows that when there is a high level of health risk, the relationship between customers' privacy risks and perceived benefits significantly not changes. These results can be understood as health risk (i.e., target risk) offsetting privacy risk (i.e., countervailing risk), resulting in "*risk substitution*." Although prior privacy studies have mainly focused on the independent effects of privacy calculus factors, this study demonstrates how two different conflicting risks (health risk vs. privacy risk) result in perceived benefit of privacy disclosure in tandem. Considering that the influence of COVID-19 is still going on in the tourism industry in the post-pandemic era, this is a novel and meaningful finding in the tourism literature.

Second, it was verified that perceived benefits fully mediate the relationship between health risk and privacy

Fig. 3 Interaction plot (health risk)

disclosure intention. This result indicates that restaurant customers do not simply disclose their personal information when they feel severe health risk (not supporting (H3b: Health risk → Intention to disclose privacy) but disclose privacy if it is considered beneficial. This result aligns with the findings of previous research focused on contextual benefits (Kim et al., 2019; Ma et al., 2021), particularly health-related benefits in COVID-19 pandemics (Abramova et al., 2022; Fox et al., 2022; Hassandoust et al., 2021). Intriguingly, regarding a rejected main hypothesis (H3b: Health risk → Intention to disclose privacy) in our research, we need to refer to Chan and Saqib (2021)'study, which is noteworthy. They validated the counterintuitive hypothesis that greater social conservatism arose due to disease concerns, leading to greater privacy concerns in Democratic states. This counterintuitive hypothesis is based on people's conservative tendencies, opposing violations of moral standards when disease concerns are severe (Horberg et al., 2009). In other words, the relationship between health risk and privacy disclosure suggests that it may appear differently depending on individual beliefs or cultural and political characteristics (e.g., social conservatism).

Finally, institutional privacy protection affects an individual's privacy disclosure intention, but the moderating effect between privacy calculus factors and the intention was not supported. In particular, institutional privacy protection was found to strengthen the relationship between privacy risk and privacy disclosure intention (opposite direction). As shown in Fig. 4, the group with a low perception of institutional privacy protection was relatively less aware of privacy risk, indicating that the relationship between privacy risk and privacy disclosure intention was insignificant. Further, the group with a high perception of institutional privacy protection has a relatively high intention to disclose privacy. In addition, it can be seen that the relationship between privacy risk and disclosure intention weakens within the group with high awareness of institutional privacy protection. In this study, institutional privacy protection is operationally defined as "the degree of belief in the government's efforts to provide accurate and reliable information as part of individual information protection practices." Thus, this means that the individuals' perception of government-level endeavors can work as a signal to individuals that the collected private data needs thorough protection. That is, it might rather increase the awareness about the privacy risk as a red flag and inversely strengthen the relationship between privacy risk and disclosure behaviors negatively. Furthermore, in our research context, the government uses individual privacy for the policy itself; thus, customers can recognize high awareness of privacy risks and privacy protection at the same time.

6.1 Implications

The findings of our research are deemed to hold significant value as they explore individuals' willingness to disclose personal privacy in the context of an infectious disease threat. Unlike previous epidemics, COVID-19 has been a pivotal event that has brought about global changes in people's daily lives and work routines. As such, the results of this study are expected to provide meaningful insights in future pandemic situations. The specific implications of this research are as follows.

This study offers a deeper understanding of customers' privacy disclosure in pandemic situations. First, using the privacy calculus theory and the concept of risk-risk tradeoff, this study verified "dual-calculus decision making." Privacy

Fig. 4 Interaction plots (institutional privacy protection)

disclosure behavior in pandemic situations has been regarded as context-dependent (Abramova et al., 2022); thus, we consider the health risk as another tradeoff variable with privacy calculus. Specifically, our research confirmed risk substitutions, providing implications for how customers' privacy perceptions change with the level of health risk, along with the importance of perceived benefit. In other words, this study is of academic significance in that it examines the relationship between privacy-related variables by adding situational variables not presented in the existing privacy literature.

Second, After COVID-19 pandemics, many studies focused on the resilience or performance of the restaurant or hotel industry (Brizek et al., 2021; Kim et al., 2021; Song et al., 2021). This stream of literature offers valuable insights into the understanding effect of infected disease and policy changes. However, this study tried to take an approach to understanding the psychological drivers and inhibitors of customers' privacy disclosure, which is part of the government policy. Privacy studies have been well-targeted in the various disciplines of economics, psychology, marketing, social and political science, and management information systems (Smith et al., 2011). However, privacy research is rare within the hospitality sector, and almost all of them focus on using new technology adoptions such as smartphone applications. In the sense that our research is regarding "privacy exchange occurring in restaurants," Our study, which differs from existing research, will serve as an important starting point for discussions in the hospitality industry in future outbreaks of another pandemic. In essence, this research makes an academic contribution by addressing the perception of privacy disclosure in situations where privacy disclosure is institutionalized, unlike previous studies that focused on different topics.

In practice, our findings also offer insights into the government (or health authority) and restaurant managers on how the visit log for contact tacking should be promoted and managed. First, by verifying the importance of perceived benefits in current research, the government should make efforts to communicate health that focuses on safety-related benefits for customers. The purpose of privacy collection (i.e., to prevent the spread of infectious diseases) and the benefits individuals can gain from privacy disclosure should be presented to recognize its legitimacy as part of the privacy collection prevention policy. Specifically, it is necessary to promote websites or platforms that inform individuals of health-related information and real-time infection tracking information.

Also, the government must continue to identify customers' perceptions of two risks and promote national goals and individual interests through risk management to reduce the two risks. We found that that when health risk is high, people do not do privacy calculus (i.e., dual-calculus). In other words, the government should apply the policy message on target risk differently based on changes in the risk level for infectious diseases.

Further, despite the coexistence of the two risks, restaurant managers need services to understand the risks of customers visiting the restaurant. For example, considering that privacy disclosure occurs in offline environments, handwriting should block access to other customers or employees. In addition, education for employees who collect personal information should also raise awareness about the management of personal information lists. In a pandemic situation, restaurant customers are willing and habitually disclose their privacy, but behind it is a persistent social problem. By delivering a message on privacy protection for the state and its employees, customers visit restaurants and tourism facilities despite the pandemic, which is thought to contribute to the revitalization of the hospitality industry.

6.2 Limitations and Future Research Directions

Our research also has several limitations. First, our study is limited to a single-country sample (i.e., South Korea). Thus, comparative studies considering nationality and cultural differences would extend valuable insights. Second, as the pandemic continues, the need for longitudinal studies is raised because the perception of health risks is changing. Precisely, to verify dual-calculus decision-making more rigorously, the approach to tracking the same sample at different points in time is required. Third, to reduce potential experience bias, it is necessary to consider control variables or moderating variables such as infection experience and vaccination on COVID-19. Last, as suggested in our findings, we suggest that further research into the role of government will be needed. For example, how trust in the government or social norms for privacy disclosure differ will also provide meaningful implications for quarantine policies and restaurant management and operation.

Appendix

Table 5 Operational definitions and survey items

Constructs	Operational definitions	Items
Health risk (HRISK)	The degree of probability that a health loss due to COVID-19 infections.	I think I am likely to contact COVID–19.
		I think my family are likely to contact COVID-19.
		My past experiences make me believe that I am likely to get sick when my friends/ colleagues are sick.
		I think there is a chance that my neighborhood will be infected by COVID-19
Privacy risk (PRISK)	The degree of privacy loss predicted by disclosure of personal information when visiting restaurants in the pandemic situation.	It would be risky to disclose my personal information to the service provider in restaurants in the pandemic situation.
		There would be high potential for privacy loss in disclosing my personal information to the service provider in restaurants in the pandemic situation.
		Personal information could be improperly used by this service provider in the pandemic situation.
		Providing the service provider with my personal information in a restaurant would involve many unexpected problems in the pandemic situation.
Perceived benefit (BEN)	The degree of belief in the safety-related favorable consequences of disclosing personal information when visiting restaurants in the pandemic situation.	By disclosing my personal information in restaurants, I can be contacted if I need to be tested.
		By disclosing my personal information, I can reduce risk of spreading the virus unknowingly in a positive COVID-19 case related to the restaurants that I visited.
		Disclosing my personal information will help health officials in the case of a positive COVID-19 case linked to the business.
		Disclosing my personal information in restaurants will generate positive results for the public health in our society.
Institutional privacy protection (PRO)	The degree of belief in the government's efforts to provide accurate and reliable information as part of individual information protection practices.	I think public health authorities ask for my authorization before collecting my personal information in the pandemic situation. (e.g., Procedure for consent to terms and conditions before personal information collection)
		I think public health authorities adhere to privacy protection law and requirements in the pandemic situation.
		Public health authorities include a privacy policy statement on their website or application in the pandemic situation.
		Public health authorities include the exact purpose of collecting my personal information on their website or application in the pandemic situation.
Intention to disclose privacy (INT)	The degree of intention to comply with privacy disclosure in the pandemic situation.	I intend to comply with the requirements for providing of personal information to response to COVID-19 in the future.
		I intend to disclose personal information according to the requirements for providing of personal information to response to COVID-19 in the future.
		I intend to follow the requirements for providing of personal information to response to COVID-19 in the future.
		I intend to carry out my responsibilities of the requirements for providing of personal information to response to COVID-19 in the future.

Data Availability The data that support the findings of this study are analyzed from the authors' survey, and the data for all analyses is available upon request.

Declarations

Conflicting Interests The Author(s) declare(s) that there is no conflict of interest.

References

Aarts, H., Paulussen, T., & Schaalma, H. (1997). Physical exercise habit: On the conceptualization and formation of habitual health behaviours. *Health Education Research, 12*(3), 363–374.

Abramova, O., Wagner, A., Olt, C. M., & Buxmann, P. (2022). One for all, all for one: Social considerations in user acceptance of contact tracing apps using longitudinal evidence from Germany and Switzerland. *International Journal of Information Management, 64*, 102473.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Ahn, N. Y., Park, J. E., Lee, D. H., & Hong, P. C. (2020). Balancing personal privacy and public safety during COVID-19: The case of South Korea. *Ieee Access, 8*, 171325–171333.

Aikin, K. J., Betts, K. R., Ziemer, K. S., & Keisler, A. (2019). Consumer tradeoff of advertising claim versus efficacy information in direct-to-consumer prescription drug ads. *Research in Social & Administrative Pharmacy, 15*(12), 1484–1488.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21.

Bauer, R. A. (1960). Consumer behavior as risk taking. In R. L. Hancock (Ed.), *Dynamic Marketing for a Changing World*. American Marketing Association.

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.

Brizek, M. G., Frash, R. E., McLeod, B. M., & Patience, M. O. (2021). Independent restaurant operator perspectives in the wake of the COVID-19 pandemic. *International Journal of Hospitality Management, 93*, 102766.

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.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Carlsson Hauff, J., & Nilsson, J. (2021). Individual costs and societal benefits: The privacy calculus of contact-tracing apps. *Journal of Consumer Marketing*.

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Comput Human Behav, 119*, 106718.

Chen, L., Zarifis, A., & Kroenung, J. (2017). The role of trust in personal information disclosure on health-related websites. *Proceedings of the European Conference on Information Systems (ECIS), 1*, 777–786.

Chin, W. W. (2010). *Bootstrap cross-validation indices for PLS path model assessment. Handbook of partial least squares*. Springer Handbooks of Computational Statistics.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155–159.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

de Groot, J. I. M., Schweiger, E., & Schubert, I. (2020). Social influence, risk and benefit perceptions, and the acceptability of risky energy technologies: An explanatory model of nuclear power versus shale gas. *Risk Analysis, 40*(6), 1226–1243.

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.

Dinev, T., & Hart, P. (2006). An extended privacy Calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy Calculus perspective. In A. Gupta, V. Patel, & R. Greenes (Eds.), *Advances in healthcare informatics and analytics. Annals of information systems, 19*. Springer.

Dzandu, M. D. (2023). Antecedent, behaviour, and consequence (abc) of deploying the contact tracing app in response to COVID-19: Evidence from Europe. *Technological Forecasting and Social Change, 187*, 122217.

Evermann, J., & Tate, M. (2012). Comparing the predictive ability of PLS and covariance analysis. Proceedings of the 33rd international conference on information systems (Orlando, FL).

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management, 55*, 102181.

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics, 65*, 101717.

Fox, G., van der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2022). Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology, 73*(7), 944–967.

Freeston, M. H., Rhéaume, J., Letarte, H., Dugas, M. J., & Ladouceur, R. (1994). Why do people worry? *Personality and Individual Differences, 17*(6), 791–802.

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health, 2*(8), e425–e434.

Goldberg, I., Wagner, D., & Brewer, E. (1997). Privacy-enhancing technologies for the internet. Proceedings IEEE COMPCON 97. Digest of Papers, 103–109.

Graham, J. D., Wiener, J. B., & Sunstein, C. R. (1995). *Risk vs. risk: Tradeoffs in protecting health and the environment*. Harvard university press.

Hair, J. F., Jr., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26*(2), 106–121.

Han, Q., Lin, Q., Jin, S., & You, L. (2020). Coronavirus 2019-nCoV: A brief perspective from the front line. *Journal of Infection, 80*(4), 373–377.

Hansen, S. F., & Tickner, J. A. (2008). Putting risk-risk tradeoffs in perspective: A response to Graham and Wiener. *Journal of Risk Research, 11*(4), 475–483.

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.

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.

Homans, G. C. (1961). The humanities and the social sciences. *American Behavioral Scientist, 4*(8), 3–6.

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2019). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics, 168*(3), 539–564.

Horberg, E. J., Oveis, C., Keltner, D., & Cohen, A. B. (2009). Disgust and the moralization of purity. *Journal of Personality and Social Psychology, 97*(6), 963–976.

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. In M. Venkatesan (Ed.), *Proceedings of the third annual conference of the Association for Consumer Research* (pp. 382–393). Association for Consumer Research.

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.

Kang, J.-W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps: A privacy calculus perspective. *International Journal of Contemporary Hospitality Management., 31*(2), 734–752.

Kim, M. J., & Denyer, S., 2020. A 'travel log'of the times in South Korea: Mapping the movements of coronavirus carriers. The Washington Post. March 13 Retrieved from: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html

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.

Kim, J., Kim, J., & Wang, Y. (2021). Uncertainty risks and strategic reaction of restaurant firms amid COVID-19: Evidence from China. *International Journal of Hospitality Management, 92*, 102752.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

Leppin, A., & Aro, A. R. (2009). Risk perceptions related to SARS and avian influenza: Theoretical foundations of current empirical research. *International Journal of Behavioral Medicine, 16*(1), 7–29.

Li, K., Cheng, L., & Teng, C. I. (2020). Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Information Processing & Management, 57*(1), 102128.

Li, V. Q., Ma, L., & Wu, X. (2022). COVID-19, policy change, and post-pandemic data governance: A case analysis of contact tracing applications in East Asia. *Policy and Society, 41*(1), 01–14.

Luce, M. F., Bettman, J. R., & Payne, J. W. (2001). Emotional decisions: Tradeoff difficulty and coping in consumer choice. *Monographs of the Journal of Consumer Research, 1*, 1–209.

Ma, X., Qin, Y., Chen, Z., & Cho, H. (2021). Perceived ephemerality, privacy calculus, and the privacy settings of an ephemeral social media site. *Computers in Human Behavior, 124*, 106928.

Magnan, R. E., Gibson, L. P., & Bryan, A. D. (2021). Cognitive and affective risk beliefs and their association with protective health behavior in response to the novel health threat of COVID-19. *Journal of Behavioral Medicine, 44*(3), 285–295.

Maiman, L. A., & Becker, M. H. (1974). The health belief model: Origins and correlates in psychological theory. *Health Education Monographs, 2*(4), 336–353.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Margherita, A., Elia, G., & Klein, M. (2021). Managing the COVID-19 emergency: A coordination framework to enhance response practices and actions. *Technological Forecasting and Social Change, 166*, 120656.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations (JECO), 4*(1), 1–17.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*(3), 155–179.

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120–130.

Nasser, A. A. N., & Nasser, A. A. N. (2020). Impacts of Trust in Government and Privacy Risk Concern on willingness to provide personal information in Saudi Arabia. *International Journal of Management Science and Business Administration, 6*(2), 7–18.

Park, S., & Tussyadiah, I. P. (2017). Multidimensional facets of perceived risk in mobile travel booking. *Journal of Travel Research, 56*(7), 854–867.

Parker, M. J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics, 46*(7), 427–431.

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.

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change, 167*, 120681.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114.

Roselius, T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing, 35*(1), 56–61.

Rust, R. T., Kannan, P., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science, 30*(4), 455–464.

Shimshack, J. P., & Ward, M. B. (2010). Mercury advisories and household health trade-offs. *Journal of Health Economics, 29*(5), 674–685.

Shmueli, G., Ray, S., Estrada, J. M. V., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of business Research, 69*(10), 4552–4564.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review, 44*, 745.

Song, H. J., Yeon, J., & Lee, S. (2021). Impact of the COVID-19 pandemic: Evidence from the US restaurant industry. *International Journal of Hospitality Management, 92*, 102702.

Sreelakshmi, C. 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*, 351–369.

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.

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior, 104*, 106115.

Viscusi, W. K., Magat, W. A., & Huber, J. (1991). Pricing environmental health risks: Survey assessments of risk-risk and risk-dollar trade-offs for chronic bronchitis. *Journal of Environmental Economics and Management, 21*(1), 32–51.

Weible, C. M., Nohrstedt, D., Cairney, P., Carter, D. P., Crow, D. A., Durnová, A. P., Heikkila, T., Ingold, K., McConnell, A., & Stone, D. (2020). COVID-19 and the policy sciences: Initial reactions and perspectives. *Policy Sciences, 53*(2), 225–241.

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), 1.

Yeong-Tsyr Wang, K., Wen-Hui, T., Chuang, T.-Y., & Lee, H.-J. (2021). Rethinking four social issues of the COVID-19 pandemic from social work perspectives. *Asia Pacific Journal of Social Work and Development, 31*(1–2), 45–51.

You, J. (2020). Lessons from South Korea's Covid-19 policy response. *The American Review of Public Administration, 50*(6–7), 801–808.

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics, 61*, 101601.

Eunji Lee is a doctoral candidate in Smart Tourism Education Platform (STEP) at Kyung Hee University in Seoul, South Korea. She received a master's degree in Tourism (Convention Management) from Kyung Hee University in South Korea. Her current research interest focuses on tourism development, tourism marketing, and smart tourism technology. Her papers have been published in *Tourism Management Perspectives, Tourism Review, Information Processing & Management, Information System Frontiers*.

Chul Woo Yoo is an associate professor in the Department of Information Technology and Operations Management in the College of Business at Florida Atlantic University. He holds a PhD degree in MIS from the State University of New York at Buffalo. His research interests include cybersecurity, human factors in e-business, electronic word-of-mouth, information privacy, software piracy, smart tourism, healthcare and IT, and agricultural information system. His works have been published in *Decision Support Systems, Information & Management, Information Development, Information Systems Frontier, JMIR Medical Informatics, Management Information Systems Quarterly, Technological Forecasting & Social Change, and etc*.

Jahyun Goo is a professor in the Department of Information Technology and Operations Management in the College of Business at Florida Atlantic University, where he teaches, researches, and consults on technology management subjects. He has won the researcher of the year award in 2009, 2011, and 2017 at Florida Atlantic University. His papers have been published in *MIS Quarterly, Decision Sciences, Information & Management, Decision Support Systems, Information Systems Journal, and Information Systems Frontier, among others*. Several pieces of his work were recognized as best or outstanding paper awards at prestigious journals and conferences. He has served for major journals as either an associate editor or a coordinating editor. He holds a Ph.D. in MIS from the State University of New York at Buffalo.

Kichan Nam is a professor at American University of Sharjah in UAE. He received his Ph.D in Management Information Systems from the State University of New York at Buffalo and was a professor of MIS at Sogang University in South Korea. His current research interests are smart tourism and smart city, e-business, and IT management. His publications are found in major international journals such as *MIS Quarterly, Information Systems Research, Decision Support Systems, Journal of Management Information Systems, Information and Management, Information Systems Frontiers, Communications of the ACM, etc*.

Chulmo Koo is a Professor at the College of Hotel and Tourism Management and the Editor-in-Chief of the Journal of Smart Tourism at Kyung Hee University in Seoul, South Korea. His papers have been published in *Journal of Tourism Research, Tourism Management, International Journal of Hospitality Management, Journal of Travel & Tourism Marketing, International Journal of Contemporary Hospitality Management, Telematics and Informatics, Computers in Human Behavior, Information & Management, International Journal of Information Management, and so on. His major research areas are smart tourism and eTourism*.