Asia Pacific Journal of Information Systems
Vol. 34 No. 2 (June 2024), 541-564

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2024.34.2.541

Analyzing Factors Influencing COVID-19 Contact-Tracing Application Users' Mobile Location Service Settings: A Perspective of Information-Motivation-Behavioral Skills Model and Implementation Intention

Jongki Kim[a], Jianbo Wang[b,*], Wei Zhang[c]

[a] *Professor, Department of Business Administration, School of Business, Pusan National University, Korea*
[b] *Ph.D. Student, Department of Business Administration, Pusan National University, Korea*
[c] *Professor, School of Information, Central University of Finance and Economics, Beijing, China*

ABSTRACT

Contact-tracing applications have significantly contributed to mitigating the spread of coronavirus disease 2019 (COVID-19), yet the extensive use of these location-based applications raises serious privacy concerns. Drawing on the Information-Motivation-Behavioral (IMB) skills model, our study investigated factors that influence users' protective behaviors toward location privacy, elucidating the privacy paradox and the mediating role of implementation intention. Through an online survey conducted in China with 311 participants, we found that privacy concerns and privacy awareness positively affected the use of mobile location service settings, with privacy concerns mediating the relationship between privacy awareness and the intention to protect privacy. Furthermore, our study demonstrated the privacy paradox, revealing the pivotal mediating role of implementation intentions in bridging the gap between users' intentions and their actual behaviors. This study offers new perspectives on the privacy paradox, particularly through the lens of implementation intention, and provides valuable insights for motivating greater use of contact-tracing applications. It offers both theoretical and practical guidance for stakeholders to address privacy concerns during global pandemics like COVID-19, thereby encouraging a more widespread and responsible engagement with technology in public health.

Keywords: COVID-19 Contact-tracing Application, Mobile Location Service Settings, Privacy Paradox, Implementation Intention, Information-motivation-behavioral (IMB) Skills Model

*Corresponding Author. E-mail: luckyblair@pusan.ac.kr

Ⅰ. Introduction

The coronavirus disease 2019 (COVID-19) pandemic has caused millions of illnesses and deaths worldwide. This rapidly spreading and long-lasting disease has profoundly affected and even permanently changed our daily lives in various ways. Additionally, the COVID-19 pandemic has triggered significant economic repercussions, almost destabilizing the global economy and leading to heightened unemployment rates and financial strain worldwide, necessitating innovative approaches to recovery (Feyisa, 2020). In response, governments and health authorities have devised strategies to fight the pandemic and restore normal daily life to people. Among these strategies, contact-tracing applications have played a crucial role. With the help of technologies such as Global Positioning System (GPS) and Bluetooth, these applications track the movements of infected individuals, aiding in the timely identification and notification of diagnosed patients from the perspectives of both health authorities and individuals (Fahey and Hino, 2020). Evidence suggests that the wide adoption and use of contact-tracing applications can effectively reduce the spread of the virus, leading to more efficient control of the pandemic at lower costs (Rowe, 2020).

However, for contact-tracing applications to work properly, more sensitive private information must be collected and processed (Rowe, 2020). Although data collected through contact-tracing applications are used to minimize virus transmission, such data may be leaked or even hacked for unintended purposes (Walrave et al., 2020). These potential threats to personal information security have heightened public concerns about privacy and security. Despite individuals expressing serious concerns about their personal privacy in various studies (e.g., Kim and Wang, 2020; Xu et al., 2011); only a small proportion takes active measures for self-protection. This paradoxical relationship between privacy attitudes and privacy behaviors is commonly known as the privacy paradox phenomenon.

The privacy paradox has been extensively explored in the information privacy literature. For instance, in the context of e-commerce, individuals may express concerns about online privacy but willingly provide private information in exchange for rewards, visible or invisible (e.g., Acquisti and Grossklags, 2005; Bandara et al., 2020). Similarly, in the context of social media, people often share and disclose personal information despite expressing serious concerns about privacy (e.g., Roberts, 2012; Taddicken, 2014).

Given the significance of privacy concerns during the COVID-19 pandemic, it is imperative to explore the privacy paradox in the context of contact-tracing applications. To contain the further spread of the virus, many countries have relied on digital technologies, with contact-tracing applications being the most popular approach (Trestian et al., 2022). However, the functionality of these applications function inherently entails privacy risks. When individuals perceive that their personal information is not well-protected, they may become unwilling to adopt contact-tracing applications (Xu et al., 2011). Therefore, to gain a deeper understanding of the situation and promote the use of such applications, there is an urgent need for further research, especially empirical approaches, to examine the effects of privacy concerns in the context of contact-tracing applications.

While existing studies on COVID-19 contact-tracing applications have primarily focused on adoption rates and benefits (e.g., Singh et al., 2020; Trestian et al., 2022), there is limited literature addressing potential negative consequences (e.g., Kim and Kwan,

2021; Nguyen et al., 2023). Despite the evident significance of comprehending the effectiveness and efficiency of contact-tracing applications, there is a lack of empirical approaches from multifaceted perspectives in the existing literature. Moreover, several studies have highlighted the discrepancy between intentions and behaviors, known as the intention-behavior gap (e.g., Acikgoz and Sumer, 2019; Gollwitzer and Sheeran, 2006). This suggests that intention may not be the most accurate predictor of behavior. In an effort to bridge this gap and provide a comprehensive explanation of privacy-protective behavior among contact-tracing application users, we incorporated implementation intention into our study. Accumulated evidence in the socio-psychological literature underscores the effectiveness of implementation intention in closing the intention-behavior gap (Kim and Wang, 2020).

Therefore, our study aims to demonstrate the privacy paradox in the context of COVID-19 contact-tracing applications. Specifically, we sought to examine the balance between using contact-tracing applications to protect personal health and using location service settings to preserve personal privacy. Drawing on the Information-Motivation-Behavioral (IMB) skills model, we investigated the factors influencing the use of mobile location service settings and demonstrated the privacy paradox within this research context. In addition, we highlighted the mediating effects of implementation intention on the relationship between intention and behavior. We expect to enhance the comprehension of privacy-related issues in the use of contact-tracing applications, thereby assisting in formulating targeted policies and strategies to better manage global crises such as the COVID-19 pandemic.

Ⅱ. Literature Review

2.1. COVID-19 Contact-Tracing Applications and Privacy Paradox

Mobile-based applications have played a significant role in mitigating the spread of COVID-19, offering a wide range of functions, including contact-tracing, quarantine, and symptom monitoring applications (Singh et al., 2020). Contact-tracing, particularly, has emerged as the most popular application adopted by different countries to control the COVID-19 pandemic, enabling users to received alerts about potential exposure to COVID-19 positive contacts (Trestian et al., 2022). The pivotal role of information in pandemic management has spurred significant academic attention on contact-tracing applications worldwide. Early studies focused on comparing different contact-tracing applications in terms of their technologies, functions, and characteristics, highlighting the diverse nature of these applications. Within the technology framework, there are two prominent types of contact-tracing applications: centralized and decentralized, supported by techniques such as GPS, Bluetooth, and Quick Response (QR) code scanning (Osmanlliu et al., 2021).

Then, further studies emphasized the potential benefits of mobile contact-tracing applications in managing pandemic challenges. For instance, Kondylakis et al. (2020) compared the features of different contact-tracing applications and demonstrated their value in pandemic management, not only for citizens but also for health professionals and decision-makers. Collado-Borrell et al. (2020) examined a wide range of COVID-19-related applications and analysed the characteristics and capabilities of these applications, contributing to the understanding of their crucial role in the management

of the pandemic. Similarly, Juneau et al. (2023) indicated that contact-tracing applications could significantly improve control measures and potentially halt the spread of the COVID-19 pandemic.

Early adopters of contact-tracing applications, such as China and South Korea, have experienced relative success in controlling the spread of the virus (Lee and Lee, 2020; Liang, 2020). However, privacy concerns have emerged as a significant challenge in the deployment of contact-tracing applications, especially in Asia where the first contact-tracing applications were introduced (Vitak and Zimmer, 2020). While these applications rely on collecting a diverse range of sensitive information, including identification, location, and health information, concerns regarding personal privacy violations persist (Nguyen et al., 2023).

Studies have highlighted rapidly increasing privacy concerns in different countries, despite the effectiveness of contact-tracing applications. For example, DiMoia (2020) found that public health policies have raised growing concerns about privacy in South Korea. Despite receiving international acclaim, the country is facing increasing concerns regarding privacy violations. Kim and Kwan (2021) found that individuals show a higher level of concern for methods that require more sensitive information in South Korea and the United States. Ang and Shar (2021) analysed 70 contact-tracing applications worldwide, revealing that a significant portion lacked adequate protection for sensitive personal information. Likewise, Kim and Wang (2022) investigated the deployment of COVID-19 contact-tracing applications in South Korea and China, noting that users in both countries expressing privacy concerns regarding these applications. Unfortunately, privacy concerns have the potential to curb the adoption and use of certain technologies and applications (Fox and Connolly, 2018)

Furthermore, the phenomenon known as the privacy paradox reveals that individuals, despite expressing privacy concerns, often exhibit behaviors that compromise their own privacy, particularly evident in e-commerce and social media contexts (Barth and De Jong, 2017; Gerber et al., 2018). It is imperative to address such paradoxical behaviors, especially regarding the use of contact-tracing applications during the global pandemic. This involves sharing sensitive personal information, thereby exposing individuals to potential privacy threats and risks (Jahari et al., 2022). In this study, we delve into the privacy paradox regarding the use of COVID-19 contact-tracing applications and mobile location settings, aiming to contribute to a deeper understanding of privacy-related issues in pandemic management.

2.2. IMB Skills Model and Implementation Intention

The IMB skills model, first proposed by Fisher and Fisher, was developed to explain the influence of health behaviors at the individual level (Rubens et al., 2015). The model posits that when individuals have information about how to improve or prevent a health issue and they are motivated to take action, they are more likely to use the skills needed to influence their health (Fish and Fisher, 2000). Primarily applied in behavioral health and social psychology literature, the IMB skills model has also been suggested as a theoretical foundation for exploring security and privacy behaviors in the information system literature. According to the IMB skills model, performing a behavior hinges on the extent to which someone is well-informed about the behavior, motivated to perform it (e.g., having positive personal beliefs and attitudes toward the behavior or outcome),

and equipped with the requisite skills to execute the behavior across various situations (Fisher et al., 2003). In other words, individuals who are well-informed, motivated to act, and possess the necessary behavioral skills are more likely to enact the behavior (Crossler and Belanger, 2019).

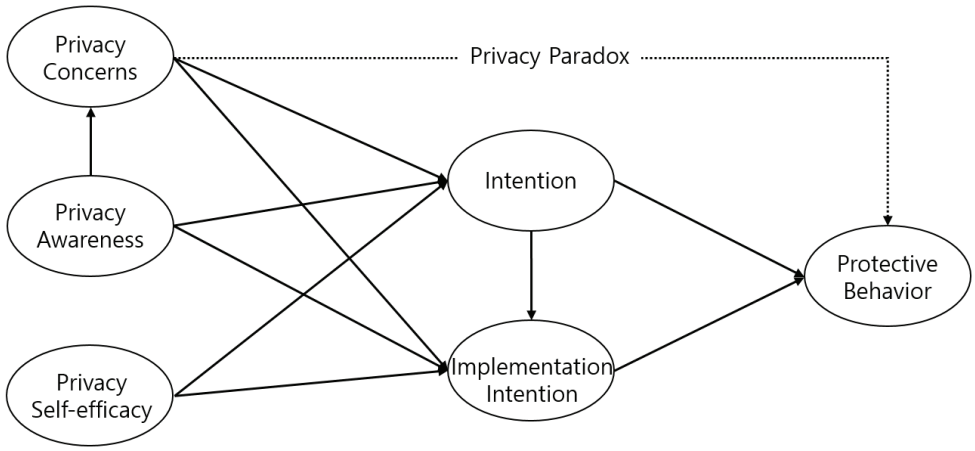
However, numerous studies have demonstrated the existence of a gap between intention and behavior; that is, individuals often express their intention to act on certain behaviors but do not always behave accordingly. To bridge this intention-behavior gap, we introduced a potent tool from the field of socio-psychology known as implementation intention. For decades, models such as the theory of reasoned action (TRA) and the theory of planned behavior (TPB) have been applied to explain and predict human behavior across various fields. However, as previously noted, the gap between intention and behavior has posed a challenge. Evidence suggests that these popular models are actually better at explaining behavioral intentions rather than actual behaviors (e.g., Acikgoz and Sumer, 2019; Gollwitzer and Sheeran, 2006). In other words, intention is not always the most effective predictor of actual behavior. This leads us to the notion of implementation intention, which has emerged as a powerful tool for bridging the gap between intention and actual behavior in the socio-psychological literature (Bieleke et al., 2018).

According to Bagozzi et al. (2003), intention comprises two components: goals and implementation. The notion employed in models such as the TRA and TPB refers to goal intention, commonly referred to as intention. As per Gollwitzer (1993), goal intention is defined as an individual's intention to achieve a certain action, but it does not guarantee the completion of the action, whereas implementation intention entails an individual's intention to perform a specific action when encountering certain situations. In essence, goal intention focuses on what an individual intends to do, while implementation intention involves detailed plans such as when, where, and how to perform the action (Van Gelderen et al., 2018). Implementation intention has been identified as a significant variable for bridging the gap between intention and behavior, as it aids individuals in translating their intentions into specific actions (Sheeran, 2002). Therefore, we integrate the IMB skill model and implementation intentions into the research model.

Ⅲ. Research Model and Hypotheses

Drawing on the IMB skills model and implementation intention theory, we proposed a research model (see <Figure 1>) to elucidate the factors that influence COVID-19 contact-tracing application users' mobile location service settings and to confirm the existence of the privacy paradox in our research context as well. Furthermore, we aimed to shed light on the mediating role of implementation intention in the relationship between intention and behavior, and to verify the mediating effects of privacy concerns on the relationship between privacy awareness and two types of intentions: intention and implementation intention.

Adjusted to the current research context of personal health and privacy, we included six constructs in the research model, that is, privacy concerns, privacy awareness, privacy self-efficacy, intention, implementation intention, and the dependent variable protective behavior. As the theoretical basis of our study, IMB skills model was initially developed to provide insights to health-related behaviors such as HIV prevention behaviors. Since then, the model has been widely used in health psychology research.



<Figure 1> Research Model

As clearly summarized in the name, the model has three core components: I as in information, M as in motivation, and B as in behavioral skills. We integrated these three constructs as three independent variables into our research model.

Based on the IMB skills model, motivation refers to an individual's attitude toward the desired behavior, which is a crucial determinant of engaging the corresponding behavior (Farooq et al., 2019). Provided that the current study focused on the context of health and privacy, motivation can be interpreted as an individual's attitude toward the privacy-related issues regarding the use of COVID-19 contact-tracing applications. Polls and extant studies have consistently shown that individuals express their severe concerns about their personal privacy regarding the use of location-based mobile services such as contact-tracing applications (e.g., Jung and Park, 2018; Zhou, 2011). In this study, therefore, we used privacy concerns to assess individuals' attitudes toward the use of these applications. Similarly, Kim and Wang (2020) found that privacy concerns, as an individual's attitude regarding the use of social media, were positively related to intention and implementation intention to protect personal privacy. In addition, their findings also indicated that users did show high privacy concerns, but they failed to take protective measures, which demonstrated the privacy paradox by identifying the paradoxical relationship between privacy concerns and protective behaviors. Likewise, Baker-Eveleth et al. (2022) also found that privacy concerns positively affect social media users' protection behaviors. Therefore, we hypothesized that:

H1: Privacy concerns are positively related to the intention to use location service settings to protect privacy.

H2: Privacy concerns are positively related to the implementation intention to use location service settings to protect privacy.

H3: Privacy concerns are not positively related to the protective behavior of using location service settings.

Information in the IMB skills model originally referred to individuals' knowledge of the behavior of interest and their understanding of the necessary ways to achieve the corresponding behavioral change

(Crossler and Belanger, 2019). After being applied in different fields and various realms, of course, information has been defined in all kinds of ways and perspectives. What we found in most studies is that information has been commonly defined as knowledge or awareness of desired behaviors (Fisher et al., 2003). To fit the information privacy literature, that is to say, information can be viewed as individuals' awareness towards privacy-related behaviors. In the context of mobile information security and privacy, for instance, information relates to user awareness of the risks associated with the use of mobile devices and applications (Crossler and Belanger, 2017). When users are aware of potential threats and risks, they are motivated to perform privacy-preserving actions (Sheehan and Hoy, 2000). Adapted to our study, we referred to information as privacy awareness to estimate individuals' awareness of protective behaviors. In other words, if users are aware of the negative consequences of contact-tracing applications, they tend to use location settings to protect personal privacy. Thus, we hypothesized that:

H4: Privacy awareness is positively related to intention.

H5: Privacy awareness is positively related to implementation intention.

H6: Privacy awareness is positively related to privacy concerns.

Most prior studies on behavioral skills have focused on self-efficacy (Chang et al., 2014). For instance, Fisher et al. (2006) used self-efficacy as a proxy measure for behavioral skills to achieve a desired behavior. Studies in the information security literature have also shown that self-efficacy significantly influences individuals' security behaviors (e.g., Johnston and Warkentin, 2010; Liang and Xue, 2010). To stay consistent with previous studies based on IMB skills model, we operationalized the behavioral skills as privacy self-efficacy as well. In the case of our research context, we defined privacy self-efficacy as users' beliefs that they know how to use mobile location service settings to protect their own privacy (Crossler and Belanger, 2019). In addition, according to Chen and Chen (2015), self-efficacy in privacy management could encourage users to engage in actions to limit disclosure and protect personal privacy. Similarly, Dienlin and Metzger (2016) also confirmed that individuals with greater privacy self-efficacy engaged in more privacy enhancing behaviors online. Therefore, we made the following hypotheses:

H7: Privacy self-efficacy is positively related to intention.

H8: Privacy self-efficacy is positively related to implementation intention.

Contact-tracing applications have been a big help in mitigating the spread of COVID-19 globally, but use of such applications has amplified public concerns about personal privacy (Jahari et al., 2022). However, these expressed privacy concerns do not seem to translate into corresponding privacy-preserving behaviors (Hoffmann et al., 2016). As discussed earlier, such a paradoxical phenomenon (i.e., the privacy paradox) has been demonstrated in different contexts such as e-commerce and social media. Most of these approaches argue that there is a gap between privacy attitudes and privacy behaviors (Norberg et al., 2007). Simply put, individuals who are concerned about their information privacy claim that they will engage in privacy-preserving behaviors, but rarely take action. Based on the findings of Kim and Wang (2020), privacy concerns positively affect individuals'

intentions to perform protective behaviors, but such intentions fail to translate into actual behaviors. They also found that implementation intention could significantly mediate the paradoxical relationship between intention and behavior.

As previously mentioned, it is crucial to differentiate between intention and implementation intention. Intention refers to the conscious decision or commitment to engage in a particular behavior, representing an individual's motivation or willingness to act (Ajzen, 1991). Conversely, implementation intention involves formulating specific plans or strategies for executing a behavior in a particular context, specifying the "when," "where," and "how" aspects of the intended action (Gollwitzer, 1999). This distinction highlights the vital role of implementation intention in translating intention into action by providing concrete cues or triggers for behavior enactment. Gollwitzer (1999) emphasized the strong effects of implementation intention in facilitating goal pursuit, underscoring the significance of simple plans in promoting behavior change. Similarly, Sheeran et al. (2005) highlighted the interplay between goal intention and implementation intention, elucidating how these constructs collectively influence behavior. Accumulated findings affirmed the robustness of implementation intention as a mechanism for bridging the intention-behavior gap across diverse behavioral contexts. For instance, Sheeran and Orbell (2000) provided empirical evidence of the efficacy of implementation intention in promoting health-related behaviors. Sheeran et al. (2005) illustrated the pivotal role of implementation intention in fostering health-related behavioral change. Adriaanse et al. (2010) underscored the importance of implementation intention in combating unhealthy habits.

Therefore, in this study, we believe that despite serious concerns about information privacy, COVID-19 contact-tracing application users rarely act to protect their personal information by taking control of the location service settings, which calls for implementation intention to help translate intention into behavior. In line with the discussion above, we hypothesized that:

H9: Intention is positively related to protective behavior.

H10: Intention is positively related to implementation intention.

H11: Implementation intention is positively related to protective behavior.

Ⅳ. Research Methodology

4.1. Construct Operationalization and Measurement

To investigate the factors that influence the use of location service settings and examine if the privacy paradox exists in such a context, we developed a research model based on the IMB skills model and implementation intention, which included privacy concerns, privacy awareness, privacy self-efficacy, intention, implementation intention, and protective behavior. As for the dependent construct of our study, protective behavior, addressing the use of mobile location service settings, was measured by 4 items adopted from Kim and Wang (2020). The four-item intention scale and the four-item implementation intention scale were also derived from the work of Kim and Wang (2020). The intention, which is short for the goal intention, assessed COVID-19 contact-tracing application users' willingness to use mobile location service settings to protect their own

privacy. While the implementation intention measured users' specific plans regarding the use of mobile location service settings as protective means of personal privacy. Four items of privacy awareness were adapted from Ermakova et al. (2014) to estimate the extent of users' knowledge or awareness regarding the protective behavior. Four items of privacy self-efficacy were obtained from Hoffmann and Lutz (2021) to measure users' behavioral skills to use mobile location service settings to protect their personal privacy. Privacy concerns were measured by four items derived from Kim and Wang (2022), which assessed users' concerns about the potential of privacy loss due to the use of location-based services. All measuring items used in the study were adapted from prior studies and we made a few adjustments to fit our research context. We also made slight modifications to instructions and the phrasing of survey questions based on feedback from fellow workers. Each item was measured in a 7-point Likert scale ranging from 1 (perfect disagreement) to 7 (perfect agreement). We listed all measuring items used for the final survey in the <Appendix>.

4.2. Sample and Procedure

In this study, we aimed to identify the factors that determine the use of mobile location service settings and examine if the privacy paradox exists in our research context. Targeted COVID-19 contact-tracing application users, we found it appropriate to conduct a survey in China that has a surprisingly high penetration rate of COVID-19 contact-tracing application use owing to the mandatory policy of Chinese government. Having adapted measurement items from extant research, we designed an online survey questionnaire and created its QR code. We conducted our online survey by distributing the QR code through popular messengers and social media platforms. In this way, respondents could participate in the survey by simply scanning the QR code linked to the online questionnaire. Once completed the survey, every respondent would be financially rewarded with Chinese RMB 1 Yuan (approximately US $0.14) immediately. Our online survey questionnaire consisted of two major sections. The first section began with descriptions and instructions, followed by 24 main survey questions. There were 8 questions in the second section including additional questions assessing users' opinions regarding the topic and common demographic questions.

To validate the measuring instruments used in the study, we first carried out a pilot test on 73 Chinese COVID-19 contact-tracing application users. The pilot test was available online for three days in September 2022 and we found no items to eliminate. Then, we conducted the final survey during the following week and kept it run online for about 8 days. In total, we retrieved 311 valid responses for the final analysis. We summarized the demographic characteristics of participants in <Table 1>. As shown in the table, 200 female and 111 male respondents participated in the online survey. Interestingly, almost 80% of respondents expressed concerns over personal information privacy regarding the use of mobile location services. However, when asked to check the present options of location services on their cell phones, more than 70% of the users left the location services on even though they were not currently using them. This supports our confirmation of the privacy paradox in our research context.

Ⅴ. Analysis and Results

<Table 1> Descriptive Statistics of Respondents

Demographic Variable		Frequency	Percent
Gender	Male	111	35.69%
	Female	200	64.31%
Age	< 20s	130	41.80%
	20s～40s	174	55.95%
	> 40s	7	2.25%
Are you worried that using mobile location services will endanger your privacy?	Never thought about it	38	12.22%
	Not at all worried	22	7.07%
	Somewhat worried	223	71.70%
	Very worried	28	9.00%
Are you aware of the potential privacy threats and risks that mobile location services may bring to you?	Never thought about it	39	12.54%
	Not at all aware	30	9.65%
	Somewhat aware	229	73.63%
	Very aware	13	4.18%
Are you aware of how to protect your information privacy? (e.g., to change the location settings)	Never thought about it	46	14.79%
	Not at all aware	46	14.79%
	Somewhat aware	195	62.70%
	Very aware	24	7.72%
Do you think it is useful to protect your privacy by controlling mobile location settings?	Never thought about it	41	13.18%
	Not at all useful	26	8.36%
	Somewhat useful	205	65.92%
	Very useful	39	12.54%
How do you usually use mobile location services?	Never heard of the location services before	8	2.57%
	Never modified the default setting	45	14.47%
	Never turned on the location services	9	2.89%
	Turn on the location services when needed	134	43.09%
	Never turned off the location services	59	18.97%
	Turn off the location services when necessary	56	18.01%
Please check your mobile location service settings right now.	It's on at the moment.	231	74.28%
	It's off at the moment.	80	25.72%
Total		311	100.00%

First, we used SmartPLS 3.0 for confirmatory factor analysis of the measurement model. The analysis revealed that Cronbach's alpha (α) and composite reliability (CR) values of each variable were above 0.7, and the average variance extracted (AVE) values were greater than 0.5, which confirmed the reliability and the convergent validity of the variables in our study (Nunnally and Bernstein, 1994; Thompson et

al., 1995). Furthermore, the square root of the AVE value being higher than the correlation between that construct and any other variable supports the discriminant validity of the variables (Awad and Krishnan, 2006). The reliability and validity test results are listed in <Table 2> and <Table 3>.

Next, we tested the structural model using structural equation modeling in SmartPLS 3.0. First, we tested the collinearity statistics, and with every variance inflation factor value less than 5, we confirmed that there were no multicollinearity problems in the study (<Table 4>). Then, we tested R square statistics to demonstrate the explanatory power of the structural model. As shown in <Figure 2>, the dependent variable, protective behavior, could explain 70.5% of the variance (R^2 = 0.705). According to Hair et al. (2016), R-squared values of 0.75, 0.50, or 0.25 can be described as substantial, moderate, or weak, respectively. In our case, we can conclude that R square value for protective behavior, the dependent

<Table 2> Reliability and Convergent Validity Testing Results

Variable	Item	Loading	t-value	α	rho_A	CR	AVE
Privacy Concerns	Item1	0.901	46.228	0.934	0.936	0.953	0.835
	Item2	0.944	74.536				
	Item3	0.920	60.190				
	Item4	0.890	53.859				
Privacy Awareness	Item1	0.894	53.831	0.920	0.921	0.943	0.807
	Item2	0.911	77.235				
	Item3	0.890	55.386				
	Item4	0.898	55.316				
Privacy Self-efficacy	Item1	0.865	40.184	0.860	0.874	0.904	0.702
	Item2	0.831	30.727				
	Item3	0.827	37.619				
	Item4	0.827	33.135				
Intention	Item1	0.871	45.388	0.888	0.888	0.922	0.748
	Item2	0.869	36.062				
	Item3	0.864	41.042				
	Item4	0.854	32.408				
Implementation Intention	Item1	0.924	54.172	0.957	0.958	0.969	0.886
	Item2	0.962	169.179				
	Item3	0.918	55.223				
	Item4	0.960	140.430				
Protective Behavior	Item1	0.893	54.052	0.936	0.936	0.954	0.840
	Item2	0.934	99.383				
	Item3	0.918	62.652				
	Item4	0.920	73.463				

Note: α = Cronbach's α, CR = composite reliability, AVE = average variance extracted

<Table 3> Discriminant Validity Testing Results

	1	2	3	4	5	6
1. Implementation Intention	**0.941**					
2. Intention	0.506	**0.865**				
3. Privacy Awareness	0.644	0.325	**0.898**			
4. Privacy Concerns	0.276	0.595	0.253	**0.914**		
5. Privacy Self-efficacy	0.433	0.323	0.529	0.377	**0.838**	
6. Protective Behavior	0.798	0.630	0.583	0.368	0.420	**0.916**

Note: Leading diagonal shows the square root of AVE of each construct

<Table 4> Multicollinearity Testing Results (Inner Variance Inflation Factor Values)

	1	2	3	4	5	6
1. Implementation Intention	—	—	—	—	—	1.346
2. Intention	1.632	—	—	—	—	1.926
3. Privacy Awareness	1.438	1.389	—	1.000	—	—
4. Privacy Concerns	1.649	1.173	—	—	—	1.550
5. Privacy Self-efficacy	1.519	1.518	—	—	—	—
6. Protective Behavior	—	—	—	—	—	—

variable in the study, was almost substantial. Furthermore, we tested effect size (f^2) and predictive relevance (Q^2). According to Cohen (1988), when the f-square value is greater than 0.02, 0.15, and 0.35, the effect sizes are small, medium, and large, respectively (<Table 5>). Additionally, Q-squared values above zero indicate that the structural model has predictive relevance (<Table 6>). In other words, the structural model of our study has predictive relevance, and both implementation intention and intention positively affect protective behavior. Privacy concerns had no influence on protective behaviors, demonstrating the privacy paradox in our research context.

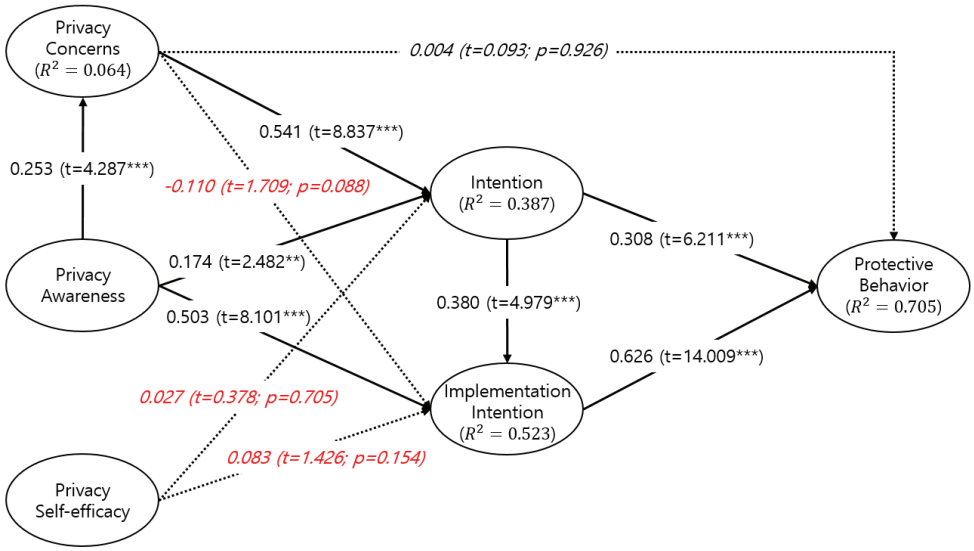
Finally, we tested the hypotheses and presented the results in terms of path coefficient values, p-values, and R-squared values (see <Figure 2>). The p-values of 0.000 (H1), 0.000 (H5), and 0.000 (H6) are statistically significant at a significance level of 0.01, and the p-value of 0.013 (H4) is statistically significant at a significance level of 0.05. The more concerned users are about their privacy being violated, the more likely they are to protect it, such as using location service settings. The more aware they were of privacy risks and protections, the more likely they were to act. Interestingly, privacy concerns mediate the relationship between privacy awareness and intention. That is, awareness alone is probably not powerful enough to make people protect their privacy, but when such awareness causes serious concerns, they become more concerned and are more likely to act on it. However, as shown in <Figure 2>, at a significance level of 0.05, the p-values of 0.926 (H3), 0.705 (H7), and 0.154 (H8) are statistically non-significant. As hypothesized, there is no significant relationship between privacy concerns and

<Table 5> Effect Size (f^2)

	1	2	3	4	5	6
1. Implementation Intention	—	—	—	—	—	1.045
2. Intention	0.186	—	—	—	—	0.153
3. Privacy Awareness	0.371	0.036	—	0.068	—	—
4. Privacy Concerns	0.015	0.406	—	—	—	0.000
5. Privacy Self-efficacy	0.010	0.001	—	—	—	—
6. Protective Behavior	—	—	—	—	—	—

<Table 6> Construct Crossvalidated Redundancy (Q^2)

	SSO	SSE	Q^2 (=1-SSE/SSO)
1. Implementation Intention	1244.000	675.047	0.457
2. Intention	1244.000	891.091	0.284
3. Privacy Awareness	1244.000	1244.000	—
4. Privacy Concerns	1244.000	1181.828	0.050
5. Privacy Self-efficacy	1244.000	1244.000	—
6. Protective Behavior	1244.000	516.082	0.585



Note: ** p < 0.05, *** p < 0.01; non-significant paths are indicated by dashed lines

<Figure 2> Hypothesis Testing Results

protective behavior, which supports the hypothesis that the privacy paradox exists in our research context. Similarly, privacy concerns had no significant influence on implementation intentions, which also demonstrates the privacy paradox. Moreover, we found that privacy self-efficacy had no significant effect

on the two intentions, which is understandable because of the frequent data breaches and leaks recently occurring on a global scale. People may have lost faith in their ability to protect their privacy, or may simply be unaware of how to take control of their information, both of which necessitate solutions. Next, the p-values of 0.000 (H9), 0.000 (H10), and 0.000 (H11) were also statistically significant at the 0.01 level, which supported the idea that implementation intention mediated the relationship between intention and behavior. As Sheeran (2002) suggests, implementation intention can help translate intention into actions, thus bridging the intention-behavior gap.

Ⅵ. Findings and Conclusions

6.1. Summary and Discussion

Utilizing the IMB skills model and implementation intention theory as theoretical foundations, we demonstrated the privacy paradox regarding the use of mobile location service settings within the realm of COVID-19 contact-tracing applications. Our findings confirmed the existence of the privacy paradox and affirmed the existing evidence on the conflicting relationship between privacy concerns and actual privacy-protective behaviors in this relatively unexplored research domain. While contact-tracing applications have played a significant role in combatting the COVID-19 pandemic by curbing the spread of the virus, they have also confronted inevitable challenges and concerns (Shahroz et al., 2021). To begin with, the increasing use of contact-tracing applications increased the access, analysis, transfer, and storage of private information, which has led to increasing privacy concerns. According to Valentino-DeVries et al. (2018), location-based data collected from applications are usually analyzed and then sold to advertisers and retailers, further exacerbating privacy-related anxieties. In light of these potential threats and risks, individuals consistently express their concerns over privacy (Hoffmann et al., 2016). In addition, evidence suggests that heightened privacy concerns decrease individuals' willingness to embrace contact-tracing applications, thus hindering these applications from realizing their full potential (Chan and Saqib, 2021).

Paradoxically, despite expressing great concerns about personal privacy, individuals do not behave correspondingly and frequently engage in risky behaviors to compromise their privacy, such as indiscreetly disclosing private information, giving rise to the privacy paradox phenomena (Barth et al., 2019; Jahari et al., 2022). As a powerful COVID-19 exit strategy, the effectiveness of contact-tracing application mostly relies on the level of uptake by the general population, but it is still unclear how to motivate more people to use these applications (Walrave et al., 2020). Hence, it is imperative to deeply understand the intricate interplay between privacy concerns and privacy-protective behaviors.

Our study offered a novel and insightful perspective on individuals' paradoxical behaviors through the lens of implementation intention. By formulating implementation intention, users can translate their privacy concerns into intention and subsequently into tangible actions to protect their privacy. Characterized by detailed plans specifying what, when, and how actions will be undertaken, implementation intention facilitates the realization of individuals' intentions to preserve personal privacy.

6.2. Implications and Limitations

This study contributes to the literature in the following ways. To date, a great number of studies have addressed the privacy paradox in varying research contexts (e.g., Hoffmann et al., 2016). However, most studies focus on intentions rather than behaviors (Barth et al., 2019). To start with, this study presented a new approach and perspective to fill the research gap in the literature on the paradoxical relationship between privacy attitude and privacy behavior. Specifically, we examined the privacy paradox regarding the use of mobile location service settings in the circumstances of COVID-19 contact-tracing applications by identifying users' privacy concerns and behaviors. The results confirmed the existence of the privacy paradox in our research context, trendy but under-explored. Then, we expanded IMB skills model into a new literature background and research context combining both personal health and information privacy issues. So far, the IMB skills model has mostly been applied in either health or privacy studies respectively. Furthermore, we extended IMB skills model by integrating implementation intention into bridging the intention-behavior gap. Since numbers of prior studies have revealed that there exists a gap between intention and behavior, which means what those widely used models such as TRA and TPM explain is the intention instead of behavior (e.g., Acikgoz and Sumer, 2019). In the study, results indicated that implementation intention significantly mediated the relationship between intention and behavior, which supported the existing evidence considering implementation intention as a powerful tool to bridge the intention-behavior gap. Then, we also found that privacy concerns played a mediating role in the relationship between privacy awareness and intention. According to Hoffmann et al. (2016), users' awareness towards privacy can be seen as a potential solution to the privacy paradox. Our finding of privacy concerns' positive mediating effects on the path from privacy awareness to intention can provide useful insights into the explanation for privacy paradox. Last but not least, the findings of our study offered a new perspective to understand and explain the paradoxical relationship between privacy concerns and privacy protective behavior, thus offering possible solutions to the privacy paradox in our context or even other alternative contexts in the future.

This study also has several practical implications. Contact-tracing applications have been playing a significant role in the COVID-19 pandemic. However, Oxford researchers proposed that it needed at least 60% of active users for these applications to curb the virus (Fraser, 2020). Therefore, understanding how to motivate more use of applications is a key task for governments and health authorities. Experiments revealed that serious concerns about privacy lowered the willingness to use COVID-19 contact-tracing applications even when the pandemic is at peak (Chan and Saqib, 2021). Given the trade-off between health and privacy, there is an urgent need for comprehensive strategies to balance this dichotomy. To begin with, we found that the majority of COVID-19 contact-tracing application users, to some extent, were concerned about their privacy being violated due to the use of these applications. Governments and relevant authorities should take such privacy issues as seriously as possible and take action upon that. For instance, it is likely for them to enforce specific laws and policies on privacy issues related to contact-tracing applications, and it is also important to allow users to know about details such what kind of personal information is getting collected, how it is getting used, and it is used by whom and for how long time (Alshawi et al., 2022). On the one hand, it is the obligation of application providers

to be honest and transparent to their users and clarify how they are to protect users' privacy (Walrave et al., 2020). Similarly, Ferretti et al. (2020) suggested that governments, health authorities, and application providers follow ethical principles and make efforts to gain or regain trust of the public, thus promoting application adoption. On the other hand, it is each user's basic right to know about what these applications are doing with their personal information (Vitak and Zimmer, 2020). In addition, we discovered that application users perceived that even though they took action such as using location service settings, they still could not protect their own privacy, which implied users' negativity and desperation regarding their privacy issues. This demands privacy-related practitioners to offer easy and clear instructions to guide users to preserve their own privacy, find innovative solutions to assist users to balance privacy and health, and provide powerful and trustworthy privacy guarantees to rebuilding users' faith. Then, we noticed that the positive role of privacy awareness playing in motivating the use of location service settings. This calls for immediate response from application providers and designers to let their users clearly understand the potential privacy risks and how they can do to cope with the challenging situation. Finally, having identified the existence of privacy paradox in our research context, we provided theoretical support for practitioners to find possible solutions to the privacy paradox from the perspective of implementation intention.

Lately, the global situation regarding COVID-19 may have improved a bit, but it still involves ongoing efforts to manage and mitigate the impact of the COVID-19 pandemic. People around the world have learned a way to live with the virus, and COVID-19 contact-tracing applications are currently becoming underutilized. Thus, we find it important to consider some potential future perspectives and implications concerning the topic as well. For one thing, based on the analysis regarding COVID-19 contact-tracing applications, we can highlight the strengths and cope with the challenges that might arise in the future. Practitioners can explore potential developments in the future contact-tracing applications from various perspectives such as privacy issues, technological advancements, policy adjustments, user interface design, accessibility, and even taking account of the nature of virus. For another thing, governments and health-related authorities could discuss the potential for an integration of contact-tracing applications with a broader public health system, because effective and efficient health information sharing could enhance the overall impact on public health. In addition, we encourage that realizing global collaboration in different levels to manage the possible global pandemic situations more effectively. With new variants constantly emerging, we suggest that policymakers and technology practitioners should work together to ensure that contact-tracing applications can rapidly adjust to new emerging variants, vaccination strategies, and corresponding public health guidelines, which can keep these applications never out of date. Besides, it is necessary to explore alternative application-based technologies and solutions. For now, most contact-tracing work functions application bases and relies on GPS and Bluetooth technology. New contact-tracing methods and bases from multi-faceted perspectives need alternative solutions in the future. Most of all, alerted by global COVID-19 pandemic, we think it is a better idea to fully understand the potential of contact-tracing applications and consider such applications as a major strategy for future pandemic preparedness and responses. In a word, our findings contribute to both literature and practice related to health and privacy, providing innovative

and useful insights and recommendations for relevant practitioners and policymakers such as guidance on technology design, policy and regulation formulation, or community engagement strategies. All efforts to assist us to be well prepared for upcoming fight against global pandemic like COVID-19.

Despite the contributions of our study, several limitations warrant consideration. Firstly, while our research provides valuable insights into mobile location service settings within COVID-19 contact-tracing applications, it is essential to acknowledge that our sample, consisting of Chinese COVID-19 contact-tracing application users, may not fully represent the diverse population of application users. We selected China for its early adoption and high penetration of contact-tracing applications; however, the use of a convenience sampling method and China's mandatory policy regarding application use may limit the generalizability of our findings. Future studies could employ larger and more diverse samples to overcome the limitation. Secondly, the measures used to collect data in our study may have limitations. We did not differentiate between privacy concerns in general application usage and those specific to COVID-19 contact-tracing applications. Given the potential variability of privacy concerns across different contexts or classifications, future research should employ measures specifically tailored to COVID-19-related applications. Furthermore, as technology continues to evolve and new privacy challenges emerge, it is imperative for future research to keep pace with these developments and distinguish privacy concerns across various domains and contexts, thereby enhancing the development of tailored privacy protection measures. In addition, future research should endeavor to propose more innovative ways for measuring complex constructs such as implementation intention and behavior. Lastly, the use of self-reported data in our study may contain potential biases, limiting the generalization of our findings. Future studies should explore alternative methods for data collection to ensure greater accuracy and reduce bias.

6.3. Conclusion

In this study, we targeted COVID-19 contact-tracing application users and observed their use of mobile location service settings. We examined the factors influencing the use of location service settings based on the IMB skills model and implementation intention theory. Furthermore, we demonstrated the privacy paradox in our research context and confirmed the significant mediating role of implementation intention in the relationship between intention and behavior. Our findings revealed that people expressed concerns about their privacy but failed to take action to protect them. Therefore, implementation intention intervention is necessary to bridge the intention-behavior gap. In addition, we found that the awareness of potential risks and protection options could motivate users to take control of location service settings and thus protect their privacy. This conveys the message that users have the right to know exactly what they are dealing with and what their options are. This can draw the attention of information privacy policymakers to the fact that users require more education and information regarding their personal privacy. We found that people lost faith in their ability to control their private information, which is desperate and totally unacceptable. People should always have the right and proper ways to decide what to share, whom to share it with, and how much to share, which calls for real attention and solutions from all relevant agencies.

<References>

[1] Acikgoz, Y., and Sumer, H. C. (2019). Implementation intentions as a predictor of applicant withdrawal. *Military Psychology*, *31*(5), 347-354. https://doi.org/10.1080/08995605.2019.1637208

[2] Acquisti, A., and Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

[3] Adriaanse, M. A., Oettingen, G., Gollwitzer, P. M., Hennes, E. P., de Ridder, D. T. D., and de Wit, J. B. F. (2010). When planning is not enough: Fighting unhealthy snacking habits by mental contrasting with implementation intentions (MCII). *European Journal of Social Psychology, 40*(7), 1277-1293. https://doi.org/10.1002/ejsp.730

[4] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

[5] Alshawi, A., Al-Razgan, M., AlKallas, F. H., Suhaim, R. A. B., Al-Tamimi, R., Alharbi, N., and AlSaif, S. O. (2022). Data privacy during pandemics: A systematic literature review of COVID-19 smartphone applications. *PeerJ Computer Science, 8*, e826. https://doi.org/10.7717/peerj-cs.826

[6] Ang, V., and Shar, L. K. (2021). Covid-19 one year on–security and privacy review of contact tracing mobile apps. *IEEE Pervasive Computing, 20*(4), 61-70. https://doi.org/10.1109/MPRV.2021.3115478

[7] Awad, N. F., and 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*, 13-28.

[8] Bagozzi, R. P., Dholakia, U. M., and Basuroy, S. (2003). How effortful decisions get enacted: The motivating role of decision processes, desires, and anticipated emotions. *Journal of Behavioral Decision Making, 16*(4), 273-295. https://doi.org/10.1002/bdm.446

[9] Baker-Eveleth, L., Stone, R., and Eveleth, D. (2022). Understanding social media users' privacy-protection behaviors. *Information & Computer Security, 30*(3), 324-345. https://doi.org/10.1108/ICS-07-2021-0099

[10] Bandara, R., Fernando, M., and Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services, 52*, 101947. https://doi.org/10.1016/j.jretconser.2019.101947

[11] Barth, S., and De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

[12] Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., and Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41*, 55-69. https://doi.org/10.1016/J.TELE.2019.03.003

[13] Bieleke, M., Legrand, E., Mignon, A., and Gollwitzer, P. M. (2018). More than planned: Implementation intention effects in non-planned situations. *Acta Psychologica*, *184*, 64-74. https://doi.org/10.1016/j.actpsy.2017.06.003

[14] Chan, E. Y., and Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior, 119*, 106718. https://doi.org/10.1016/j.chb.2021.106718

[15] Chang, S. J., Choi, S., Kim, S. A., and Song, M. (2014). Intervention strategies based on information-motivation-behavioral skills model for health behavior change: A systematic review. *Asian Nursing Research, 8*(3), 172-181. https://doi.org/10.1016/j.anr.2014.08.002

[16] Chen, H. T., and Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and

self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13-19. https://doi.org/10.1089/cyber.2014.0456

[17] Cohen, J. (1988). *Statistical Power Analysis for The Behavioral Sciences*. Hillsdale, NJ: Lawrence Erlbaum.

[18] Collado-Borrell, R., Escudero-Vilaplana, V., Villanueva-Bueno, C., Herranz-Alonso, A., and Sanjurjo-Saez, M. (2020). Features and functionalities of smartphone apps related to COVID-19: Systematic search in app stores and content analysis. *Journal of Medical Internet Research, 22*(8), e20334. https://doi.org/10.2196/20334

[19] Crossler, R. E., and Bélanger, F. (2017). The mobile privacy-security knowledge gap model: Understanding behaviors. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4071-4080). Retrieved from http://hdl.handle.net/10919/81983

[20] Crossler, R. E., and Bélanger, F. (2019). Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research, 30*(3), 995-1006. https://doi.org/10.1287/isre.2019.0846

[21] Dienlin, T., and 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. https://doi.org/10.1111/jcc4.12163

[22] DiMoia, J. P. (2020). Contact tracing and COVID-19: The South Korean context for public health enforcement. *East Asian Science, Technology and Society: An International Journal*, *14*(4), 657-665. https://doi.org/10.1215/18752160-8771448

[23] Ermakova, T., Fabian, B., and Zarnekow, R. (2014). Acceptance of health clouds-a privacy calculus perspective. In *Proceedings of the European Conference on Information Systems (ECIS)*. Retrieved from http://aisel.aisnet.org/ecis2014/proceedings/track09/11

[24] Fahey, R. A., and Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 102181. https://doi.org/10.1016/j.ijinfomgt.2020.102181

[25] Farooq, A., Jeske, D., and Isoaho, J. (2019). Predicting students' security behavior using information-motivation-behavioral skills model. In *ICT Systems Security and Privacy Protection. SEC 2019. IFIP Advances in Information and Communication Technology, 562*. Springer, Cham. https://doi.org/10.1007/978-3-030-22312-0_17

[26] Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., ... and Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491), eabb6936. https://doi.org/10.1126/science.abb6936

[27] Feyisa, H. L. (2020). The world economy at COVID-19 quarantine: Contemporary review. *International Journal of Economics, Finance and Management Sciences, 8*(2), 63-74. https://doi.org/0.11648/j.ijefm.20200802.11

[28] Fisher, J. D., and Fisher, W. A. (2000). Theoretical approaches to individual-level change in HIV risk behavior. In *Handbook of HIV Prevention* (pp. 3-55). Springer.

[29] Fisher, J. D., Fisher, W. A., Amico, K. R., and Harman, J. J. (2006). An information-motivation- behavioral skills model of adherence to antiretroviral therapy. *Health Psychology, 25*(4), 462-473. https://doi.org/10.1037/0278-6133.25.4.462

[30] Fisher, W. A., Fisher, J. D., and Harman, J. (2003). The information-motivation-behavioral skills model: A general social psychological approach to understanding and promoting health behavior. *Social Psychological Foundations of Health and Illness, 22*(4), 82-106. https://doi.org/10.1002/9780470753552.ch4

[31] Fox, G., and Connolly, R. (2018). Mobile health

technology adoption across generations: Narrowing the digital divide. *Information Systems Journal, 28*(6), 995-1019. https://doi.org/10.1111/isj.12179

[32] Fraser, C. (2020, April 16). *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown*. Oxford University's Big Data Institute. Retrieved from https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-oreven-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

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

[34] Gollwitzer, P. M. (1993). Goal achievement: The role of intentions. *European Review of Social Psychology*, *4*(1), 141-185. https://doi.org/10.1080/14792779343000059

[35] Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist, 54*(7), 493-503. https://doi.org/10.1037/0003-066X.54.7.493

[36] Gollwitzer, P. M., and Sheeran, P. (2006). Implementation intentions and goal achievement: A meta-analysis of effects and processes. *Advances in Experimental Social Psychology*, *38*, 69-119. https://doi.org/10.1016/S0065-2601(06)38002-1

[37] Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage Publications.

[38] Hoffmann, C. P., and Lutz, C. (2021). Digital divides in political participation: The mediating role of social media self-efficacy and privacy concerns. *Policy & Internet*, *13*(1), 6-29. https://doi.org/10.1002/poi3.225

[39] Hoffmann, C. P., Lutz, C., and Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

[40] Jahari, S. A., Hass, A., Hass, D., and Joseph, M. (2022). Navigating privacy concerns through societal benefits: A case of digital contact tracing applications. *Journal of Consumer Behaviour, 21*(3), 625-638. https://doi.org/10.1002/cb.2029

[41] Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

[42] Juneau, C. E., Briand, A. S., Collazzo, P., Siebert, U., and Pueyo, T. (2023). Effective contact tracing for COVID-19: A systematic review. *Global Epidemiology*, *5*, 100103. https://doi.org/10.1016/j.gloepi.2023.100103

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

[44] Kim, J., and Kwan, M. P. (2021). An examination of people's privacy concerns, perceptions of social benefits, and acceptance of COVID-19 mitigation measures that harness location information: A comparative study of the US and South Korea. *ISPRS International Journal of Geo-Information*, *10*(1), 25. https://doi.org/10.3390/ijgi10010025

[45] Kim, J., and Wang, J. (2020). Examining factors that determine the use of social media privacy settings: Focused on the mediating effect of implementation intention to use privacy settings. *Asia Pacific Journal of Information Systems*, *30*(4), 919-945.

[46] Kim, J., and Wang, J. (2022). Investigating the use of COVID-19 contact tracing applications in South Korea and China: An agency theory perspective. *The Journal of Internet Electronic Commerce Research, 22*(5), 1-24. https://doi.org/10.37272/JIECR.2022.10.22.5.1

[47] Kondylakis, H., Katehakis, D. G., Kouroubali, A., Logothetidis, F., Triantafyllidis, A., Kalamaras, I., ... and Tzovaras, D. (2020). COVID-19 mobile apps:

A systematic review of the literature. *Journal of Medical Internet Research, 22*(12), e23170. https://doi.org/10.2196/23170

[48] Lee, D., and Lee, J. (2020). Testing on the move: South Korea's rapid response to the COVID-19 pandemic. *Transportation Research Interdisciplinary Perspectives, 5*, 100111. https://doi.org/10.1016/j.trip.2020.100111

[49] Liang, F. (2020). COVID-19 and Health Code: How digital platforms tackle the pandemic in China. *Social Media+ Society, 6*(3), 2056305120947657. https://doi.org/10.1177/2056305120947657

[50] Liang, H., and Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7). https://doi.org/10.17705/1jais.00232

[51] Nguyen, V. M., Bell, C., Berseth, V., Cvitanovic, C., Darwent, R., Falconer, M., Hutchen, J., Kapoor, T., Klenk, N., and Young, N. (2023). Promises and pitfalls of digital knowledge exchange resulting from the COVID-19 pandemic. *Socio-Ecological Practice Research*, *Preprints*, *3*, 427-439. https://doi.org/10.1007/s42532-021-00097-0

[52] Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[53] Nunnally J., and Bernstein, I. (1994). *Psychometric Theory*. New York: McGraw Hill.

[54] Osmanlliu, E., Rafie, E., Bédard, S., Paquette, J., Gore, G., and Pomey, M. P. (2021). Considerations for the design and implementation of COVID-19 contact tracing apps: Scoping review. *JMIR mHealth and uHealth, 9*(6), e27102. https://doi.org/10.2196/27102

[55] Roberts, T. H. (2012). A cross-disciplined approach to exploring the privacy paradox: Explaining disclosure behaviour using the theory of planned behaviour. *UK Academy for Information Systems Conference Proceedings*. https://aisel.aisnet.org/ukais2012/7

[56] Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management*, *55*, 102178. https://doi.org/10.1016/j.ijinfomgt.2020.102178

[57] Rubens, M., Attonito, J., Saxena, A., Shehadeh, N., Ramamoorthy, V., and Nair, R. R. (2015). Health promotion and disease prevention strategies for today's physicians. *The American Journal of the Medical Sciences, 349*(1), 73-79. https://doi.org/10.1097/MAJ.0000000000000320

[58] Shahroz, M., Ahmad, F., Younis, M. S., Ahmad, N., Boulos, M. N. K., Vinuesa, R., and Qadir, J. (2021). COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transportation Engineering, 5*, 100072. https://doi.org/10.48550/arXiv.2103.01766

[59] Sheehan, K. B., and Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73. https://doi.org/10.1509/jppm.19.1.62.16949

[60] Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1-36. https://doi.org/10.1080/14792772143000003

[61] Sheeran, P., and Orbell, S. (2000). Using implementation intentions to increase attendance for cervical cancer screening. *Health Psychology, 19*(3), 283-289. https://doi.org/10.1037//0278-6133.19.3.283

[62] Sheeran, P., Webb, T. L., and Gollwitzer, P. M. (2005). The interplay between goal intentions and implementation intentions. *Personality and Social Psychology Bulletin, 31*(1), 87-98. https://doi.org/10.1177/0146167204271308

[63] Singh, H. J. L., Couch, D., and Yap, K. (2020). Mobile health apps that help with COVID-19 management: Scoping review. *JMIR Nursing, 3*(1), e20596. https://doi.org/10.2196/20596

[64] Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns,

individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-mediated Communication, 19*(2), 248-273. https://doi.org/10.1111/jcc4.12052

[65] Thompson, R., Barclay, D. W., and Higgins, C. A. (1995). The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies: Special Issue on Research Methodology, 2*(2), 284-324.

[66] Trestian, R., Celeste, E., Xie, G., Lohar, P., Bendechache, M., Brennan, R., and Ta, I. (2022). The privacy paradox-investigating people's attitude towards privacy in a time of COVID-19. In *2022 14th International Conference on Communications (COMM)* (pp. 1-6). Retrieved from https://ieeexplore.ieee.org/document/9817170

[67] Valentino-DeVries, J., Singer, N., Keller, M. H., and Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. The New York Times, Retrieved from https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[68] Van Gelderen, M., Kautonen, T., Wincent, J., and Biniari, M. (2018). Implementation intentions in the entrepreneurial process: Concept, empirical findings, and research agenda. *Small Business Economics*, *51*, 923-941. https://doi.org/10.1007/s11187-017-9971-6

[69] Vitak, J., and Zimmer, M. (2020). More than just privacy: Using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies. *Social Media+ Society*, *6*(3), 2056305120948250. https://doi.org/10.1177/2056305120948250

[70] Walrave, M., Waeterloos, C., and Ponnet, K. (2020). Adoption of a contact tracing app for containing COVID-19: A health belief model approach. *JMIR Public Health and Surveillance, 6*(3), e20572.

[71] Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 1. https://doi.org/10.17705/1jais.00281

[72] Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

[73] Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems, 111*(2), 212-226. https://doi.org/10.1108/02635571111115146

<Appendix> Measurement Items

Construct	Item		Source
Privacy Awareness (PA)	PA1	I am aware of the information privacy risks and protective mechanisms.	Ermakova et al. (2014)
	PA2	I am knowledgeable about the risks and how to protect my information privacy.	
	PA3	I follow the news and developments about the information privacy risks and protective mechanisms.	
	PA4	I keep myself updated about risks and solutions to ensure my information privacy.	
Privacy Self-efficacy (PS)	PS1	I am able to use the location services on my smartphone.	Hoffmann and Lutz (2021)
	PS2	I have the necessary ability to use the location services on my smartphone.	
	PS3	I have the skills to solve any problems in using the location services on my smartphone.	
	PS4	I am able to take control of the location settings on my smartphone.	
Privacy Concerns (PC)	PC1	I'm concerned that using location services can be a risk for my privacy.	Kim and Wang (2022)
	PC2	I'm concerned that using location services can have the potential of privacy loss.	
	PC3	I'm concerned that it can be risky to share my location information while using the services.	
	PC4	I'm concerned that using location services can cause serious privacy problems.	
Intention (IN)	IN1	I am willing to use the location-protective settings, such as turning off the location services, to protect my privacy in the future.	Kim and Wang (2020)
	IN2	I will use the location-protective settings, such as turning off the location services, to protect my privacy if necessary.	
	IN3	I will change the location-protective settings, such as turning off the location services, to protect my privacy when it is necessary.	
	IN4	I intend to take control of the location-protective settings, such as turning off the location services, to protect my privacy in the future.	
Implementation Intention (IIN)	IIN1	I have already planned when to use the location-protective settings, such as turning off the location services, to protect my privacy.	Kim and Wang (2020)
	IIN2	I have already planned what to do with the location-protective settings to protect my privacy.	
	IIN3	I have already planned how to keep using the location-protective settings to protect my privacy.	
	IIN4	I have made plans regarding the use of location-protective settings to protect my privacy.	
Behavior (BE)	BE1	I always use the location-protective settings, such as turning off the location services, to protect my privacy.	Kim and Wang (2020)
	BE2	I always modify the location-protective settings, such as turning off the location services, to protect my privacy.	
	BE3	I always modify the location settings, such as turning off the location services, to protect my privacy if necessary.	
	BE4	I always try to take control of the location-protective settings, such as turning off the location services, to protect my privacy.	

◆ About the Authors ◆

Jongki Kim

Jongki Kim is a professor in the School of Business at Pusan National University, Republic of Korea. He holds a Master's degree in Management Information System (MIS) from Arkansas State University, USA, and a Doctoral degree in MIS from Mississippi State University, USA. His research interests span a variety of critical areas, including information security, privacy, e-commerce, technology management, and behavioral economics.

Jianbo Wang

Jianbo Wang is currently pursuing her Ph.D. at Pusan National University's School of Business in Korea, holding a Master's degree in MIS from Chungbuk National University. Her research focuses on a range of pivotal topics, including information security, privacy, behavioral economics, e-commerce, and implementation science.

Wei Zhang

Wei Zhang is a professor of School of Information at Central University of Finance and Economics. He received B.S. in computer sciences in 1998 and M.S. in management sciences in 2001 from Shandong University of Science and Technology, Ph.D. in system engineering in 2005 from Beihang University, respectively. He worked at Research Institute of Chinese Internet economics as a researcher from 2008 to present and at National University of Singapore in 2013 as a visiting scholar. As the principal investigator of the intelligent emotion computing project, he enhanced the main idea and did experiment for the proposed scheme. His research areas are big data, sentiment analysis, and health emergency management.

Submitted: July 5, 2023; 1st Revision: November 19, 2023; 2nd Revision: March 3, 2024; Accepted: March 26, 2024