Asia Pacific Journal of Information Systems
Vol. 30 No. 4 (December 2020), 919-945

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2020.30.4.919

Examining Factors that Determine the Use of Social Media Privacy Settings: Focused on the Mediating Effect of Implementation Intention to Use Privacy Settings

Jongki Kim[a], Jianbo Wang[b,*]

[a] *Professor, School of Business, Pusan National University, Busan, Korea*
[n] *Ph.D. candidate, School of Business, Pusan National University, Busan, Korea*

ABSTRACT

Social media platforms such as Instagram and Facebook lead to potential security risks, which consequently raise public concerns about privacy. However, most people rarely make active efforts to protect their personal data, even though they have shown increasing concerns about privacy. Therefore, this study examines the factors that determine social media users' behavior of using privacy settings and testifies the existence of privacy paradox in such a context. In addition, it investigates the mediating effects of implementation intentions on the relationship between intentions and behaviors. In the study, we collected data through questionnaires, and the respondents were undergraduate and graduate students in South Korea. After a pilot test (n = 92) and a set of face-to-face interviews, 266 usable responses were retrieved for data analysis finally. The results confirmed the existence of the privacy paradox regarding the use of social media privacy settings. And the implication intention did positively mediate the relationship between intention and behavior in the context of social media privacy settings. To the best of our knowledge, our study is the first in the information privacy literature to introduce the notion of implementation intention which is a much more powerful explanation and prediction of actual behavior than the (behavioral) intention.

Keywords: Social Media, Privacy Settings, Privacy Paradox, Implementation Intention

Ⅰ. Introduction

The emergence and development of social media in the past decades has brought significant changes to our daily lives, especially how we communicate and interact. Soon, social media will rapidly attract numerous users because they provide an incredible range of services. social media platforms are designed

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

to encourage people to disclose information that can be public or intimate, thus satisfying the human nature of seeking connection and commonality. Obviously, such instinctive desire of the human to communicate with others is often transformed into various types of disclosure (Millham and Atkin, 2018), which eventually helps build and maintain personal relationships. As an irreplaceable means of daily communication and connection, social media offers easy and open platforms for interaction and provides instant and convenient services to satisfy different users. People can share connections with other users worldwide, such as families, friends, and even total strangers. Thus, social media allows users to enjoy myriad services unrestricted by time and space. Many open-to-all services such as Facebook, Instagram, and Twitter allow millions to freely create online profiles, share personal thoughts, and post much information online, which raises privacy concerns (Acquisti and Gross, 2006; Yang et al., 2020). Apparently, a large amount of personal information stored and posted on social network profiles can be viewed and even used in bad ways by unknown numbers of strangers (Frik and Gaudeul, 2020). During the past few years, frequent data privacy scandals of top-rated companies such as Facebook and Google have alerted global online users to the possibility of privacy threats and risks. One of the well-known incidents was the case of Facebook-Cambridge Analytica data scandal. Millions of Facebook users' personal information was collected by Cambridge Analytica without users' consent and was mainly to be used for political advertisement. This data leak scandal, which was known as the largest data leak in Facebook history, grew to a head in March 2018 and resulted in the rapid decrease of Facebook's market capitalization and Facebook CEO Mark Zuckerberg's testifying in the United States Congress. While according to the Wall Street Journal (8th October 2018), it outlined the first Google data breach and exposed the fact that Google had hidden such an issue from their consumers. It also informed the public that the data breach, which was likely to allow hundreds of third-party apps to access consumers' private information such as names and emails without authorization, had occurred between 2015 and 2018. Social media users around the world have shown higher concerns about their privacy since then. Accordingly, social media platform providers have tried to support users to protect their personal information (Du et al., 2018). To limit access to users' sensitive information, some providers allow users to control the privacy settings on their own accounts; users can decide what and how much information they want to be seen by whom (Madejski et al., 2011).

However, in terms of the use of privacy settings, there exists a trade-off between sharing and protecting. This probably explains that although polls and reports show increasing concerns about privacy, most users rarely try to protect their personal data (Melicher et al., 2016). Such a dichotomy between the privacy attitude and privacy behavior is called the "privacy paradox." To date, several researchers have tried to explain the privacy paradox (attitude-behavior dichotomy) in the information privacy literature. The majority have focused on the relationship between privacy attitude and intention instead of behavior because the intention is assumed to be the most immediate predictor of behavior based on popular theories such as the theory of planned behavior (TPB). However, several studies have proved that there exists a gap between behavioral intention and behavior, which posits the failure to translate intentions to actions. To date, there is limited research addressing the privacy paradox in the context of social media privacy setting use. Therefore, this study

examines the factors that determine the use of social media privacy settings and testifies if the privacy paradox exists in such a research context from the perspective of the attitude-intention-behavior relationship. It also investigates the mediating effects of implementation intention on the relationship between intention and behavior. This study focuses on the following three research questions: (1) What factors determine the use of social media privacy setting? (2) What role does implementation intention play in the relationship between intention and behavior? (3) Does the privacy paradox exist with regard to the use of social media privacy settings? The study findings would help develop education strategies for social media users and provide support for effective privacy protection solutions (Debatin et al., 2009).

Ⅱ. Literature Review

2.1. Privacy Paradox in the Context of Social Media

To date, information privacy has attracted much academic attention. Generally, there are two main streams in privacy relevant literature: one is about information disclosure/revelation behaviors, the other is about privacy-protective behaviors. Studies on the former have mainly been addressed in two contexts: e-commerce and self-disclosure technology (Sun et al., 2015). Especially, the prevalent approaches have focused on the context of self-disclosure technologies such as blogs, microblogs, instant messaging, and social media sites (Lowry et al., 2011). With social media evolving as the main platforms for daily communication and interaction, a wide range of information disclosure issues on social media have been explored by privacy researchers. Large amounts of information are being generated, shared, and stored every day through social media, people start to worry about the possibility of any negative consequences caused by such unlimited disclosure.

Information security problems such as privacy violations kindled public concerns, which attracted several researchers to study information privacy-protective behaviors in the context of social media platforms. As mentioned previously, several social media platforms allow users to decide what information to disclose and whether to use privacy settings to protect their information (Strater and Lipford, 2008). The earliest work in this domain was by Gross and Acquisti (2005), which investigated the information revelation patterns of Facebook users and showed that only a minority of users had modified the default options provided by social media platforms. Acquisti and Gross (2006) investigated the relationship between privacy attitudes and users' beliefs in what data they were sharing, compared with what data they were actually sharing, and their awareness of the privacy mechanisms on Facebook (Boyd and Hargittai, 2010). Some studies investigated the status of privacy settings use (e.g., Krishnamurthy and Wills, 2008), and others examined the factors affecting the use of privacy preference from the perspective of awareness and perception (Debatin et al., 2009; Madejski et al., 2011; Madejski et al., 2012; Netter et al., 2013; Wisniewski et al., 2017). In addition, other factors regarding individual and social characteristics (Spottwood and Hancock, 2017; Tifferet, 2019; Xie and Kang, 2015) and factors that influence different privacy relevant behaviors of social media users (Brandtzæg et al., 2010; Li et al., 2020) were widely explored.

However, with regard to the use of privacy settings, there exists a trade-off between sharing and protecting. Although polls and reports show that

most individuals insist that privacy is a high priority, they behave differently. Most people would voluntarily give their private information in return for certain rewards, although they are well aware of the potential risks (Barth and De Jong, 2017; Ginosar and Ariel, 2017). It was also reported that even concerns could not stop social media users from sharing their private information (Van Zoonen, 2016). Such a dichotomy between privacy attitude and privacy behavior was defined as the '(informational) privacy paradox' (Kokolakis, 2017). In 2007, Norberg and colleagues established the term privacy paradox to explain why consumers provide their personal data anyway even after their claiming that the right to control personal information has been violated in the environment of e-commerce. Regarding the existence of such a paradoxical phenomenon, there was a debate between supporters and challengers. And it is worth noting that more behavioral economic approaches support the existence of the privacy paradox and are dedicated to providing academic evidence (e.g., Aivazpour and Rao, 2020; Barth et al., 2019).

The privacy paradox supporters have made attempts to test and explain the dichotomy phenomenon from two main perspectives. One addresses the relationship between privacy attitude and privacy behavior, and the other focuses on the relationship between privacy intention and privacy behavior. Studies on the attitude-behavior relationship have challenged the common hypothesis that the higher the level of concerns regarding personal information, the less information to provide and share online, the more privacy-protective actions, thus claiming the dichotomy between privacy attitude and privacy behavior. However, studies on the intention-behavior relationship have confirmed the dichotomy between privacy intention and privacy behavior by comparing the self-reported intention with the behavior measured under experimental conditions.

There is no doubt that the mainstream of privacy paradox studies is about varied paradoxical behaviors in the context of social media. For instance, Reynolds et al. (2011) found that despite the high concern regarding their privacy, users did not reduce the number of postings and disclosure of information on Facebook. Hughes-Roberts (2013) also suggested that the level of concern regarding privacy was insufficient to stop or restrict users from sharing information on Facebook. Young and Quan-Haase (2013) examined the factors that motivated Facebook users to disclose information despite their high concerns regarding privacy. They suggested in their study that social media users disclosed information anyway although they showed concerns regarding privacy because they assumed that they have tried protecting themselves from potential risks such as privacy violations by managing the Facebook friend network who can access their personal data. Taddicken (2014) investigated the effects that privacy concerns, attitudes, psychological traits of users, and user's age have on the self-disclosure behaviors while using different kinds of internet applications such as social networking sites. The findings also confirmed that privacy concerns hardly influence self-disclosure, but he did find that perceived social relevance and the number of applications used could moderate the relationship. Van Zoonen (2016) claimed that even though people don't feel secure, they still share personal information on different social media sites. Hallam and Zanella (2017) also showed that people's disclosure behaviors are not consistent with their concerns and demonstrated that privacy concerns had an indirect negative small effect on the disclosure behavior, but it was not strong enough to balance the total direct positive effect of social rewards. Choon (2018) analyzed the privacy paradox on Facebook and Twitter, and he

found that the privacy paradox could be shaped by different kinds of factors, such as a lack of social trust, perceived control over the information disclosed, and limited knowledge and low visibility of institutional surveillance. Just like the examples above, accumulated privacy paradox studies in the research context of social media have focused on disclosure behaviors like self-disclosure on different social media platforms.

However, in this study, we aim to investigate the privacy paradox in a noteworthy but underexplored context – the use of social media privacy settings. To date, there have been a few studies making similar attempts. For example, Oomen and Leenes (2008) examined the relationship between privacy risk perception and the use of privacy-protective technologies. The results of their study indicated that high-level perception of privacy risk was not powerful enough to make people adopt privacy-protective strategies, although they were aware of the risk. Utz and Krämer (2009) assessed the use of privacy settings on social network sites and investigated the factors that predicted the choice of specific settings. They focused on the role of privacy concerns, impression management, individual characteristics including trust and narcissism, and perceived social norms. Across all three studies in their paper, there were several inconsistent results, but they found that most users had changed the default privacy settings and privacy concerns consistently predicted the choice of privacy settings. Young et al. (2013) examined the privacy paradox by distinguishing the difference between the concerns about social privacy and institutional privacy. They suggested that people had shown more social privacy concern, whereas there was less concern about institutional privacy. They also concluded that there were no strategies to protect from institutions utilizing personal information. Mosteller and Poddar (2017) used regulatory focus theory to explain the privacy paradox of social media engagement and privacy protection behaviors. The results indicated that privacy concerns and trust mediated two effective antecedents – privacy violation experience and perceived secondary control over personal information. Gerber et al. (2018) summarized the most popular theoretical explanations for the privacy paradox and reviewed all the relevant factors that predict privacy attitude, behavioral intention, and actual behavior significantly. But they could not make any overall conclusions in the study because of the slight variation in the definitions of the constructs used in different studies.

Despite all these attempts and achievements, there still exist contradicting results and incomplete understanding of the privacy paradox. Further approaches from multifaceted perspectives are required for an in-depth understanding of such a complex dichotomy phenomenon. In this study, therefore, we aim to examine the privacy paradox of social media privacy settings from an underexplored perspective of implementation intention.

2.2. Theory of Planned Behavior and Implementation Intention

Several theories have been applied to interpret the privacy paradox. One of the most popular theoretical basis is the 'privacy calculus' theory. Privacy calculus theory claims that individuals tend to make decisions based on the calculus between the expected risk of privacy and the potential benefit of disclosure (Dinev and Hart, 2006; Xu et al., 2011). That is to say, individuals will disclose their personal information if they perceive more benefits than risks. Previous studies have provided evidence that privacy calculus theory is a well-fitting framework to examine

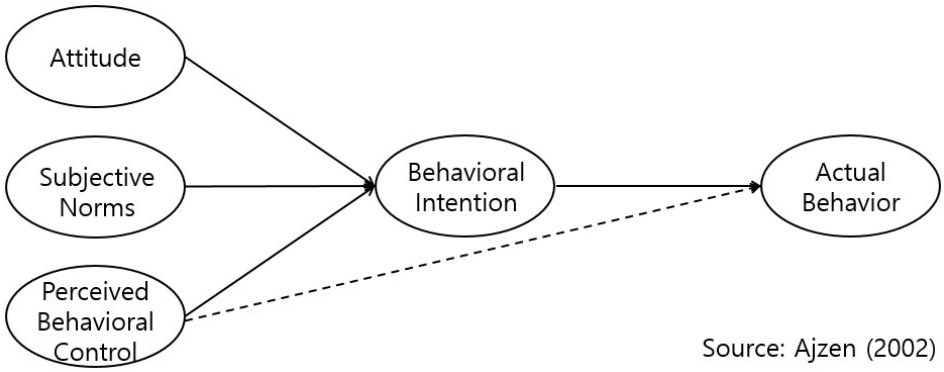
privacy paradox issues. Also, many studies have verified that social media users have the tendency to make decisions based on a risk/cost-benefit calculation. Users disclose and share personal information when anticipated benefits outweigh the expected losses, which is inconsistent with their high concerns about privacy (Debatin et al., 2009; Lee and Kwon, 2015).

However, several studies about individual decision behaviors have proved that different kinds of 'cognitive biases' and 'heuristics' have effects on the process of decision making (Acquisti and Grossklage, 2007). Due to the limited cognitive ability, it is almost impossible for human beings to access and process all information in order to make rational decisions, thus benefits and costs are probably being overestimated or underestimated (Deuker, 2009; Flender and Müller, 2012). For example, 'optimism bias' is one of the most popular cognitive biases examples, which suggests that people have the tendency to believe that compared to themselves, negative incidents and consequences happen to others more (Cho et al., 2010; Dinev and Hu, 2007).

Some studies use the 'risk and trust model' to explain the privacy paradox. Generally, trust directly affects privacy-relevant behaviors, and meanwhile perceived risks do have effects on the corresponding intention but not powerful enough to influence the actual privacy behavior (Flender and Müller, 2012; Norberg et al., 2007). In addition, another theory that has been used a lot to explain various privacy paradox phenomena is the 'quantum theory'. Drawing on quantum theory, some studies proposed a new understanding and explanation for the privacy paradox. Accordingly, individuals' answers about the potential outcomes of their decisions cannot really reveal the actual decision outcomes until the actual decisions are made (Flender and Müller, 2012; Kokolakis, 2017).

In this study, however, we drew on the theory of planned behavior (TPB) and complete it by integrating the implementation intention. As an extension of the theory of reasoned action (TRA), TPB has been widely used to predict human behaviors in various realms. The TRA posits that behavioral intention, which is the immediate antecedent to behavior, is determined by an attitude and subjective norm (Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975). Later, the TPB extended the TRA by considering perceived control over behavioral achievement as a determinant of intention and actual behavior (Armitage and Conner, 2001). Attitude refers to an individual's overall assessment of the behavior; subjective norm refers to an individual's perception of the social normative pressures or relevant others' beliefs that he or she should perform the behavior or not. Perceived behavioral control refers to an individual's perceived controllability of the behavior based on experience and the expected abilities to perform the behavior (Li, 2012).

Based on a consistent attitude-intention-behavior progression, TPB <Figure 1> has been widely applied to studies explaining and predicting behavioral intentions and behaviors. However, there exist two potential gaps (i.e., the attitude-intention gap and the intention-behavior gap) in such an attitude-intention-behavior relationship (Grimmer and Miles, 2017). Most studies on information privacy focus on the relationship between attitude and intention under the assumption that intention effectively predicts actual behavior (e.g., Hsieh and Lee, 2020; Wall and Warkentin, 2019; Yang et al., 2020). However, a principal criticism is that individuals' engagements in certain actions are often inconsistent with their behavioral intentions and it is quite complicated to translate behavioral intentions into behaviors. Many published meta-analyses show that TPB models effec-



<Figure 1> Theory of Planned Behavior (TPB)

tively explain the variance in behavioral intentions; however, intentions are poor predictors of actual behaviors (Papies, 2017). The TPB claims that the consistency of the attitude-intention-behavior relationship is questioned and the potential of the dichotomy relationship reconfirmed.

In the socio-psychological literature, however, the so-called intention includes two components: goal intention and implementation intention (Bagozzi and Dholakia, 2003). The intention specified in those widely used human decision-making models such as TPB is actually called the goal intention, which refers to "I intend to achieve behavior X" but it does not guarantee the completion of the behavior. Whereas the implementation intention refers to "I intend to perform the behavior X when I encounter with the situation Y" (Gollwitzer, 1993). Based on the content and structure, it is easy to distinguish goal intentions and implementation intentions. The goal intention addresses what an individual intends to do, while the implementation intention emphasizes details such as when, where, and how an individual is going to perform the behavior (Van Gelderen et al., 2018).

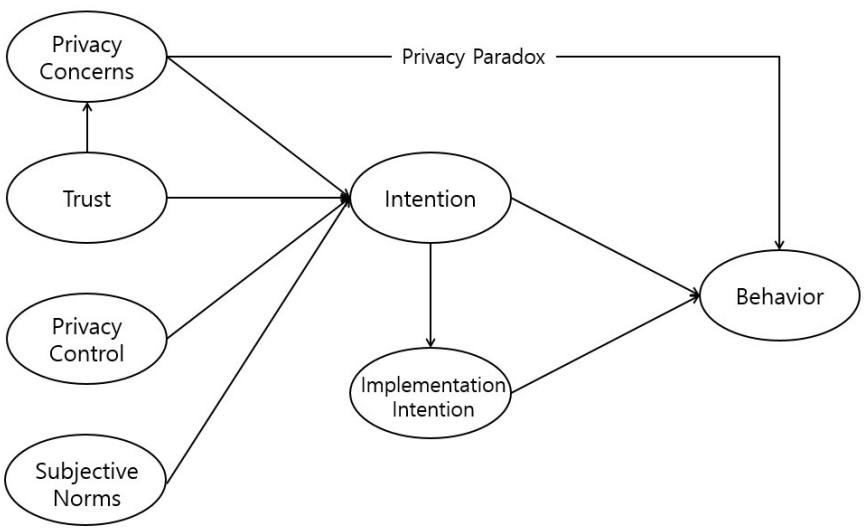
As noted above, although TPB plays a crucial role in explaining and predicting several human behaviors, there are issues such as the so-called intention-behavior gap. Several meta-analyses on TPB studies proved that these models explain intentions better than behaviors (Acikgoz and Sumer, 2019; Gollwitzer and Sheeran, 2006; Van Gelderen et al., 2018). Such findings motivated several researchers to analyze the inconsistency between intentions and behaviors. Sheeran (2002) demonstrated that the intention-behavior gap was a result of intenders' failure to act on their intentions to perform specific behaviors. Then, a significant variable was identified and defined as the implementation intention to bridge the gaps between intentions and behaviors. Gollwitzer and Schaal (1998) explored the impact of implementation intentions on the attainment of goal-directed behaviors. They found that 100% of the strong intenders performed the behavior after forming additional implementation intentions. While only half of the strong intenders completed the behavior without forming any implementation intentions. Gollwitzer (2014) reviewed studies on how implementation intentions work and showed that implementation intentions help people attain their goals. Bieleke et al. (2018) claimed that they were the first to conduct a systematic investigation of the consequences of forming implementation intentions to attain goals. They also proved through

two experiments that facilitating implementation intentions is a powerful strategy to enhance goal achievements. An increasing number of empirical evidence verified the powerful effects of forming implementation intentions in the translating from goal intentions to real actions in various domains such as health behavior, environment-protective behavior, physical activity, diet, and purchase behavior. However, research on integrating implementation intention to help explain and predict privacy-related behaviors in information privacy literature is limited. To fill the gaps, this study examines the mediating role of implementation intention in the relationship between intention and behavior in the context of social media privacy settings.

Ⅲ. Research Model and Hypotheses

3.1. Research Model

After identifying the gaps in the literature, we designed a model <Figure 2> to examine the factors that determine the use of social media privacy settings and to identify if the privacy paradox exists in such a context. In this study, therefore, we integrated Privacy Control, Privacy Concerns, Trust, and Subjective Norm as factors influencing social media users' intention to use privacy settings. We assumed that the implementation intention has positive mediating effects on the relationship between intention and behavior. The primary goal of the current study was to extend the information privacy-related studies by investigating the privacy paradox from a perspective of the attitude-intention-behavior relationship in the context of social media privacy settings. Furthermore, by integrating these factors, behaviors of using social media privacy settings could be accurately explained and predicted. Similar to most other studies, the privacy attitude was assessed as privacy concerns in this study as well. First, we tested the existence of the privacy paradox regarding the use of social media privacy settings by specifying the relationship between privacy concerns and behavior. Then, we examined the factors that determine the use of social media privacy settings. Next, we verified



<Figure 2> Research Model

the mediating effects of implementation intention on the relationship between attitude and behavior.

3.2. Research Hypotheses

3.2.1. The Existence of Privacy Paradox

The majority of the information privacy-related studies support the privacy paradox in different contexts, including e-commerce and the social media environment. These approaches challenge the existing privacy research built on the basis of TPB by proposing that there exists a dichotomy between privacy attitude and privacy behavior (Norberg et al., 2007). The privacy paradox supporters have tried to test or explain the dichotomy phenomenon (Kokolakis, 2017). One stream has mainly focused on the relationship between privacy attitude and behavior (Zafeiropoulou et al., 2013). For instance, individuals with high levels of privacy concerns freely provide personal information or rarely act to protect their privacy. Another stream focused on the dichotomy between privacy intention and behavior (Keith et al., 2013). Specifically, individuals who are afraid of losing control over their own personal information claim that they will engage in privacy-protective behavior, but they rarely put that into action. In other words, great concerns about privacy are insufficient motivators for people to act. This study assumes that there still exists a dichotomy between privacy attitude and behavior regarding the use of social media privacy settings. That is, despite serious concerns about their privacy, social media users rarely act to protect their personal information on social media such as making use of privacy settings. Therefore, we hypothesize that there is a dichotomy between privacy concerns and behavior:

H1: Privacy concerns are not positively related to the behavior of using social media privacy settings.

3.2.2. Determinants of Using Social Media Privacy Settings

After identifying the existence of privacy paradox, we investigate the factors determining the use of social media privacy settings. Differing from the existing studies focusing on either the attitude-behavior relationship or the intention-behavior relationship, this study investigates the complete attitude-intention-behavior relationship in the context of social media privacy settings. In other words, we test the attitude-intention relationship and the intention-behavior relationship. TPB has been used to explain human behaviors in various domains, including information privacy literature. These models focused on the motivational factors that determine the performance of a particular behavior and provide a framework to link behavioral, normative, and control beliefs defined as attitude, subjective norms, and perceived control, respectively, to behavioral intentions and behaviors. TPB has contributed toward explaining and predicting intentions and behaviors until being challenged and criticized for the assumption of attitude-behavior consistency. However, several meta-analyses have shown that the TPB model can explain the variance in intentions in up to 50%. Therefore, we integrated behavioral, normative, and control beliefs into our research model to help explain social media users' intention to use privacy settings. To suit this study, we adopted and redefined the behavioral, normative, and control beliefs as privacy concerns, subjective norms, and privacy control, respectively. Several studies on the existence of privacy paradox have assessed privacy concerns and proved the dichotomy between privacy concerns and

information disclosure behavior or privacy-protective behaviors (Acquisiti, 2004; Norberg et al., 2007). Adopted from TPB, subjective norms focus on the interaction with significant others, which guide or constrain individuals' privacy behaviors without the force of laws. In this study, we assume that social media users will use privacy settings if important people around them suggest. In addition, the perceived behavioral control in TPB corresponds to individuals' self-appraisals of the ability to demonstrate a specific behavior. To emphasize the privacy-protective behavior in this study, we adjusted the perceived behavioral control and defined it as privacy control. The greater individuals evaluate their privacy control ability, the more intentions to display a certain behavior. Besides, we introduced trust as another determinant of social media users' intention to use social media privacy settings. Trust is a vital aspect of information privacy studies. Prior studies suggest that trust is the most important influence on information disclosure (Hoffman et al., 1999) because trust can mitigate concerns about privacy and thus motivate users to provide personal information online (Schoenbachler and Gordon, 2002; Zimmer et al., 2010). Furthermore, Dwyer et al. (2007) conceptualized and argued that Trust in Providers would positively determine users' intentions to share information on social media platforms. Specifically, we believe that with the trust in social media platform provider, users would feel it unnecessary to use privacy settings or just retain the default options set by the service providers. Moreover, several studies have proved that trust is a notable antecedent not only to privacy intentions but also to privacy concerns (Bart et al., 2005; Belanger et al., 2002; Hoffman et al., 1999). Thus, we hypothesize that:

H2: Privacy concerns are positively associated with the intention to use social media privacy settings.

H3: Privacy control is positively associated with the intention to use social media privacy settings.

H4: Subjective norms are positively related to the intention to use social media privacy settings.

H5: Trust is negatively associated with the intention to use social media privacy settings.

H6: Trust is negatively related to privacy concerns in the context of social media privacy settings.

3.2.3. The Mediating Effect of Implementation Intention

When explaining the privacy paradox phenomenon of using social media privacy settings, we focused on the role of implementation intention in mediating the relationship between intention and behavior. It is worth noting that the intention in the popular intention models such as TPB refers to the goal intention only (Adam and Fayolle, 2016). As stated earlier, the intention in this study refers to the goal intention that corresponds to a state of willing in which individuals determine a goal of performing a particular behavior, whereas the implementation intention is similar to a state of planning in which individuals specify how to achieve the desired goal behavior by planning when, where, how (Gollwitzer, 1993). There are several pieces of evidence proving the power of implementation intention in addressing the intention-behavior gap (e.g., Sniehotta et al., 2005). Sheeran and Orbell (1999) even proposed that the TPB model should be supplemented by adding implementation intention to improve the correspondence between intentions and behaviors. Schwarzer et al. (2010) also stated that implementation intention should act as a mediator of the relationship between intentions and behaviors. Prestwich and

Kellar (2014) also proposed that implementation intention is an effective mediator to help individuals translate their intentions into behaviors, thus reducing the gap between intention and behavior.

In other words, a certain behavior involves two phases: the motivational phase (goal intention) and the volitional phase (implementation intention). In the motivational phase, people set a goal, while in the volitional phase, people plan how they are going to enact their goal intentions (Gollwitzer and Brandstatter, 1997), which implies that implementation intentions are not formed before the goal intention, but only conjointly or subsequently (Gollwitzer, 1993). The purpose of the implementation intention is to make specific plans to help promote the initiation and efficient execution of goal-directed behavior (Gollwitzer, 1993). Through such processes, people facilitate the translation of goal intention into behavior such that "If the situation X arises, then I'll do behavior Y" (Gollwitzer, 1999). In addition, the implementation intention can increase the probability of acting and its effectiveness does not mitigate over time (Sheeran and Silverman, 2003). By translating goal intention into implementation intention, people identify a specific situation much faster and then respond much efficiently, which can result in a more accurate prediction of behavior (Webb and Sheeran, 2007). Unfortunately, compared with the goal intention, the implementation intention received scant attention in the intention models developed for explaining and predicting human behaviors despite its much better prediction of behavior. To address the gaps, therefore, we hypothesize that:

H7: The intention to use social media privacy settings is positively related to the behavior.

H8: The implementation intention positively mediates the relationship between the intention and the behavior of using social media privacy settings.

H8-1: The intention to use social media privacy settings is positively associated with the implementation intention.

H8-2: The implementation intention is positively associated with the behavior of using social media privacy settings.

Ⅳ. Research Methodology

4.1. Operationalization of Variable and Measurement

To test the privacy paradox phenomenon and examine the factors that determine the use of social media privacy settings, we investigated several existing studies to identify valid factors. Given the controversial issues and literature gaps, we developed a model by integrating seven variables, including Privacy Concerns (PCNS), Trust (TR), Privacy Control (PCOL), Subjective Norms (SN), Intention (IN), Implementation Intention (IIN), and Behavior (BE). To suit the current research context, we made a few adjustments and redefined the variables as follows <Table 1>.

We designed a survey to study how social media users respond to questions regarding the use of social media and privacy settings from different aspects. The items were adopted from prior relevant studies to ensure the validity of the measuring instruments used in this study and we slightly modified them to adjust to the specific research context. The variables were measured through a seven-point Likert scale, ranging from (1) Strongly Disagree to (7) Strongly Agree. Except for demographics, all questions in the survey are listed in <Table 2>.

<Table 1> Operational Definitions of Variables

Variable	Definition	Source
Privacy Concerns	Users' concerns and perceptions of the loss of revealing personal information on social media.	Dinev and Hart (2006)
Privacy Control	Users' beliefs in his or her ability to manage the release and dissemination of personal information on social media.	Xu et al. (2011)
Subjective Norms	Users' perceived social pressure to perform the behavior or not.	Ajzen (1991)
Trust	It is a shortcut for users' trust in social media platform provider. It refers to users' faith that providers will continue to be responsive.	Ramaswami et al. (1997)
Intention	Users' willingness to use privacy settings on social media.	Zhao et al. (2012)
Implementation Intention	The development of plans that specify more details such as where, when, and how users will enact their intentions to use social media privacy settings.	Ziegelmann et al. (2007)
Behavior	The extent to which social media users make use of privacy settings to protect their privacy.	Hoadley et al. (2010)

<Table 2> Measuring Items of Variables

Variable	Item	Source
Privacy Concerns	I am concerned that the information I submit on social media could be misused.	Dinev and Hart (2006)
	I am concerned that others can find private information about me from social media.	
	I am concerned about providing personal information to social media, because of what others might do with it.	
	I am concerned about providing personal information to social media, because it could be used in a way I did not foresee.	
Privacy Control	I believe I have control over who can get access to my personal information through social media.	Xu et al. (2011)
	I think I have control over what personal information is released on social media.	
	I believe I have control over how personal information is used through social media.	
Subjective Norms	People, who are important to me, think that I should use privacy settings while using social media.	Ajzen (1991); Hsu and Kuo (2003)
	People, who are important to me, think that modify social media privacy settings.	
	People around me think that I should check and change social media privacy settings if necessary.	
Trust	Social media platform provider makes good-faith efforts to address most user concerns.	Jarvenpaa and Tractinsky (1999); McKnight et al. (2002)
	Social media platform provider is honest in its dealings with users.	
	Social media platform provider keeps its commitments to its users.	
	Social media platform provider is trustworthy.	

<Table 2> Measuring Items of Variables (Cont.)

Variable	Item	Source
Intention	I am willing to use privacy settings when using social media in the future.	Zhao et al. (2012)
	I will probably use privacy settings on social media if necessary.	
	I will likely change privacy settings if necessary.	
	I intend to use social media privacy settings in the near future.	
Implementation Intention	I have already planned precisely when to modify social media privacy settings.	Gollwitzer and Brandstätter (1997); Ziegelmann et al. (2007)
	I have already planned precisely what to choose for social media privacy settings.	
	I have already planned precisely how to keep using privacy settings even though it feels limited sometimes.	
	I have my own plans regarding how often to change social media privacy settings.	
Behavior	I check the default privacy settings when I use social media.	De Wolf et al. (2014)
	I confirm the privacy settings first before posting things on social media.	
	I modify the privacy settings for my social media if necessary.	
	I take control over the privacy settings to protect my personal information on social media.	

4.2. Data Collection

We empirically analyzed the privacy paradox in the context of using social media privacy settings. Data for this study were collected through both online and offline questionnaires. Undergraduate and graduate students from South Korea participated and all of them were current social media users. In the survey, we asked our respondents to complete questionnaires including measurement scales of privacy concerns, trust, privacy control, subjective norms, intention, implementation intention, and the behavior of using social media privacy settings. Additional demographic questions were also asked. For accurate and objective responses, we asked all the respondents to log on to their social media accounts to review the privacy settings on their profiles and posts while answering the survey questions about behavior. To revise and improve the measuring scales before the final data collection, we conducted a pilot test and a set of interviews with 92 undergraduate students from May 7 to May 17, 2019. Accordingly, we excluded these items that lacked reliability and validity: the fourth measuring item of privacy control, the fourth measuring item of trust, and the third item of SN. Besides, we could integrate feedback through face-to-face interviews to simplify the survey questions for better understanding. Finally, a total of 300 subjects participated in the final survey from May 20 to May 31, 2019. After excluding incomplete (n = 4) and unreliable answers (n = 30), we retrieved 266 usable responses for data analysis.

4.3. Data Analysis and Results

In this study, we used SPSS Statistics 25.0 and SmartPLS (Partial Least Square) 2.0 for the data analysis. First, the analysis of demographic questions <Table 3> showed that among the 266 respondents, approximately 48% were male and 52% were female, which mitigates the problem of gender imbalance. In the survey, we asked respondents to choose one

<Table 3> Demographic Characteristics of Respondents

Demographic variable		Frequency	Percent
Gender	Male	128	48.1
	Female	138	51.9
The most used service	Band	3	1.1
	Instagram	167	62.8
	Facebook	55	20.7
	Kakao Story	2	0.8
	Cafes	11	4.1
	Blog	5	1.9
	Twitter	10	3.8
	Others	13	4.9
Personally preferred privacy settings	Public	30	11.3
	Friends	144	54.1
	Friends except…	5	1.9
	Specific friends	8	3.0
	Only me	15	5.6
	It depends	64	24.1
Actual privacy settings currently	Public	66	24.8
	Friends	164	61.7
	Friends except…	1	0.4
	Specific friends	9	3.4
	Only me	15	5.6
	Custom	11	4.1
Have you ever got in trouble or embarrassed due to unexpected privacy settings?	Yes	92	34.6
	No	174	65.4
Categories of social media users	Power users	27	10.2
	Content contributors	58	21.8
	Lurkers	172	64.7
	Others	9	3.4
Total		266	100.0

of the most used social media platforms. Instagram users were ranked first at nearly 63%, while Facebook users second place at approximately 21%. Then, respondents answered questions on social media privacy settings. More than 50% of the respondents showed that they preferred the setting of “Only friend can see” on their social media and 24% like different privacy settings depending on situations. However, several users did not behave accordingly in real settings. In addition, almost more than half of the users reported that they have not faced trouble or were embarrassed due to unexpected privacy settings

yet. According to the 90:9:1 rule for the phenomenon of participation inequality in the use of social media, in most online communities, 90% of the users are lurkers who are known as undetected users who never contribute. They just quietly read or observe instead of giving any feedback; 9% (Content contributor) of users contribute occasionally who do not create original contents they share, like, and comment; only 1% (Power users) of the users account for all the contributions. As in our study, nearly 65% were lurkers, 22% were content contributors, and 10% were power users.

4.3.1. Verification of Measuring Instruments

Before analyzing the research model, we need to test the reliability and validity of the variables and their measuring instruments. The reliability was verified using three criteria: Cronbach's *α* greater than 0.7, composite reliability (CR) greater than 0.7, and

<Table 4> Reliability and Convergent Validity Analysis

Variable	Item	Loading	*t*-value	α	CR	AVE
Privacy Concerns (PCNS)	PCNS1	0.903	63.562	0.920	0.943	0.806
	PCNS2	0.884	47.785			
	PCNS3	0.909	59.102			
	PCNS4	0.896	49.464			
Trust (TR)	TR1	0.827	13.704	0.905	0.933	0.778
	TR2	0.904	26.761			
	TR3	0.919	33.215			
	TR4	0.876	29.879			
Privacy Control (PCOL)	PCOL1	0.924	3.409	0.803	0.874	0.701
	PCOL2	0.868	3.123			
	PCOL3	0.703	2.634			
Subjective Norms (SN)	SN1	0.733	8.247	0.781	0.843	0.644
	SN2	0.760	8.903			
	SN3	0.903	24.125			
Intention (IN)	IN1	0.892	57.741	0.938	0.955	0.842
	IN2	0.940	78.581			
	IN3	0.890	31.508			
	IN4	0.948	121.917			
Implementation Intention (IIN)	IIN1	0.905	73.882	0.903	0.932	0.774
	IIN2	0.906	74.032			
	IIN3	0.869	33.959			
	IIN4	0.837	30.522			
Behavior (BE)	BE1	0.892	49.810	0.927	0.948	0.821
	BE2	0.883	46.413			
	BE3	0.918	77.346			
	BE4	0.931	79.860			

average variance extracted (AVE) exceeding 0.5 (Nunnally, 1978; Thompson et al., 1995). Two kinds of validity were analyzed. Convergent validity was assessed using the factor Loading value greater than 0.7 (Hulland, 1999), while discriminant validity was verified when the square root value of α is greater than 0.7 and correlates more highly than with other factors (Awad and Krishnan, 2006). The analysis results of reliability and convergent validity are shown in <Table 4>. With all values of Cronbach's α > 0.7, CR > 0.7, AVE > 0.5, and factor loading > 0.7, the reliability and convergent validity were reliability in our study.

We assessed discriminant validity and presented the results in a correlation matrix <Table 5>. All square root values of AVE exceed 0.7 and this correlation is higher than the highest cross-factor correlation, and thus discriminant validity was verified. In addition, given that recent studies in IS have emphasized the evaluation of common method bias (CMB), we assessed such influence by applying Harman's single-factor test, which is the most popular technique to detect CMB in business researches. According to the single-factor test, when conducting an exploratory factor analysis with all variables in the study, CMB is not a problem if the first factor accounts for less than 50% of the variance among all other variables (Podsakoff and Organ, 1986). As a result, using SPSS Statistics 25.0, we found that the first factor accounts for 28.197% (less than 50%) of the variance, which suggested that CMB is not problematic in our study.

4.3.2. Evaluation of Model and Hypothesis Testing

4.3.2.1. Analysis of Structural Model

We examined redundancy value, R square value, and communality value to evaluate the explanatory power of the structural model. On the condition that redundancy value is greater than 0 and communality value is greater than 0.5, the explanatory power of the model can be calculated using the square root of multiplying the mean value of R square by the mean value of Communality. If the square root value is greater than the standard of 0.36, 0.25, or 0.1, the predictors in the model are estimated to have a large, medium, or small effect, respectively (Tenenhaus et al., 2005). We found that our model had a significant explanatory power of 0.321 (> 0.25) which is close to 0.36, indicating that the factors

<Table 5> Discriminant Validity Analysis

Variable	Behavior	Implementation Intention	Intention	Privacy Concerns	Privacy Control	Subjective Norms	Trust
Behavior	**0.906**						
Implementation Intention	0.608	**0.880**					
Intention	0.555	0.421	**0.918**				
Privacy Concerns	0.307	0.273	0.417	**0.898**			
Privacy Control	0.153	0.132	0.080	-0.192	**0.837**		
Subjective Norms	0.324	0.325	0.341	0.290	0.030	**0.802**	
Trust	-0.026	0.032	-0.047	-0.193	0.416	0.045	**0.882**

Note: Value in bold is the square root of AVE

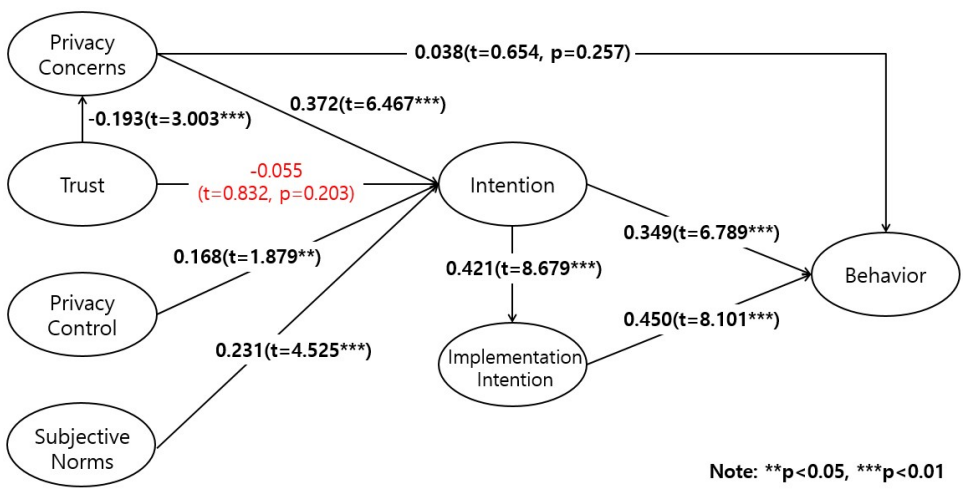
<Table 6> The Explanatory Power of the Model

Variable	R Square	Redundancy	Communality
Trust (TR)	—	—	0.778
Subjective Norms (SN)	—	—	0.644
Privacy Control (PCOL)	—	—	0.701
Privacy Concerns (PCNS)	0.037	0.030	0.806
Intention (IN)	0.250	0.144	0.842
Implementation Intention (IIN)	0.177	0.133	0.774
Behavior (BE)	0.479	0.283	0.821
Mean	0.135	0.084	0.767
The Explanatory Power of Model	0.321		

in our model could explain the dependent variable effectively.

4.3.2.2. Hypothesis Testing

Then, we identified the causal relationship in the model using the path coefficient and *t*-value of each directional relationship. The path coefficient in a partial least squares (PLS) model is similar to the standardized beta coefficient in a regression model (Agarwal and Karahanna, 2000). While the *t*-values are calculated through repetitive processes of bootstrapping, <Figure 3> describes the results of hypothesis analysis with the corresponding path coefficient, *t*-value, and *p*-value of each correlative relationship. First, we tested the privacy paradox, which refers to the dichotomy between privacy concerns and behavior, by identifying the path coefficient value equals 0.038, *t*-value equals 0.654, and *p*-value equals 0.257 that is above the significance level of 0.05. As hypothesized in H1, there was no significant relationship between privacy concerns and behavior. Then, we identified the factors that determined the intention and behavior to use social media privacy settings.



<Figure 3> Hypothesis Testing Results

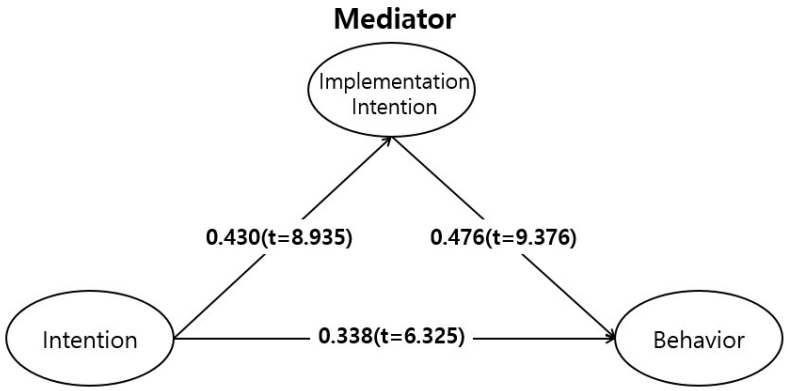
As predicted in H2, H3, and H4, privacy concerns, privacy control, and subjective norms are positively associated with the intention to use social media privacy settings. Given that the path coefficient value = 0.372, *t*-value = 6.467, and *p*-value = 0.000 (< 0.05) between privacy concerns and intention, the path coefficient value = 0.168, *t*-value = 1.879, and *p*-value = 0.031 (< 0.05) between privacy control and intention; and the path coefficient value = 0.231, *t*-value = 4.525, and *p*-value = 0.000 (< 0.05) between SN and intention, thus the three hypotheses H2, H3, and H4 were supported. However, what is assumed in H5 that trust is negatively related to the intention was not supported, due to the criteria *p*-value = 0.203 (> 0.05). While H6, that is, trust is negatively associated with privacy concerns, was also supported by specifying the path coefficient value = −0.193, *t*-value = 3.003, and *p*-value = 0.001 (< 0.05).

4.3.2.3. Analysis of the Mediating Effect of Implementation Intention

Next, we verified the total effect of intention on behavior in two steps: direct and indirect effects. The direct effect of intention on behavior was estimated through the path coefficient value = 0.543 and *t*-value = 11.633. As for the indirect effect of intention on behavior, we first identified the relationship between intention and the mediator implementation intention in which the path coefficient value = 0.435 and *t*-value = 9.367. We then confirmed the relationship between the mediator implementation and behavior in which the path coefficient value = 0.621 and *t*-value = 15.266. Next, we examined the direct and indirect effects simultaneously and illustrated the path coefficient value and *t*-value of each correlative relationship in <Figure 4>. Therefore, the indirect effect was calculated through 0.430 × 0.476 = 0.205. Finally, we testified the significance of the indirect effect by the Sobel test in which the following formula was used.

$$\text{Z Statistics} = \frac{a \times b}{\sqrt{(b_2 \times S_a^2) + (a_2 \times S_b^2)}}$$

The corresponding *t*-value and *p*-value of the indirect effect were estimated by the criteria of *t*-value = 6.463 and *p*-value = 0.000 (< 0.05), which confirmed that the indirect effect of intention on behavior was significant. Therefore, H7 and H8 were supported. The intention is positively associated with behavior and implementation intention partially mediates the relationship between intention and behavior.



<Figure 4> Direct and Indirect Effect Analysis

Ⅴ. Conclusion

5.1. Findings and Results

The study confirmed the existence of the privacy paradox in an underexplored context and examined the factors that determine the use of social media privacy settings. We first analyzed the relationship between privacy concerns and behavior to confirm the existence of a privacy paradox related to the use of social media privacy settings. Then, we investigated the factors that influence the intention and behavior of using social media privacy settings. Next, we focused on the mediating impact of implementation intentions on the relationship between intention and behavior.

The results of our study are summarized in three main aspects. First, we identified the privacy paradox in the use of social media privacy settings by investigating the relationship between privacy concerns and behavior. As predicted in H1, there was no significant relationship between privacy concerns and behavior, thus proving the existence of a privacy paradox regarding the use of social media privacy settings. Such finding supported the earlier studies claiming that despite the increasing concerns about privacy, people rarely take action to protect their personal data.

Second, given that the existence of privacy paradox has been tested, we specified the factors that influence the use of social media privacy settings. As presented in H2, H3, and H4, privacy concerns, privacy control, and SN have positive effects on the intention to use privacy settings. As the concerns about privacy increase, users are more likely to use privacy settings to protect their personal information. Besides, as users have more belief in their abilities to manage their own personal information on social media and the more significant others suggest them to take control over their own social media privacy settings, there are more possibilities that users are willing to use privacy settings.

However, it indicates that trust in a social media platform provider has no direct effect but an indirect effect on the intention mediated by privacy concerns. It is not difficult to imagine that after the frequent data privacy scandals of those top-rated services over the past few years, social media users do not completely trust the provider with their personal information on social media, which contracts H5. As claimed in H6, perhaps users have not lost all of their faith in social media platform providers and part of them still like to believe that the providers are somehow trustworthy that they do not need to worry about their privacy much.

Third, we tested the mediating impact of implementation intention on the relationship between intention and behavior in the context of social media privacy settings. To identify the total effect of intention on behavior, we analyzed both direct and indirect effects of intention on behavior. The analysis results indicated that the intention has significant direct and indirect effects on behavior. The mediator implementation intention helps explain and predict the behavior more effectively and more accurately. It is worth noting that privacy concerns are positively related to the intention of using social media privacy settings, but have no significant relationship with the behavior. We found that in the relationship of attitude, intention, and behavior, consistency between attitude and intention was easily achieved, while the problem resided in the translation from intention to behavior. As noted earlier, the intention has a limited ability to explain and predict behavior. Therefore, we argue that with the mediator implementation intention, intention can be translated

into behavior effectively, which can reduce the gap between intention and behavior, thus resulting in bridging the dichotomy between attitude and behavior.

5.2. Discussion and Implication

The implications of our study can be assessed mainly from two perspectives. From a theoretical perspective, the study contributes to the existing information privacy literature by examining and explaining the privacy paradox in a significant but under-studied context: the use of social media privacy settings from a complete perspective of attitude-intention-behavior relationship. We tested the existence of a privacy paradox and investigated the factors to explain and even predict the use of social media privacy settings. In addition, we constructed implementation intention to mediate the relationship between intention and behavior, and thus addressed the privacy paradox related to the use of social media privacy settings. Despite its better ability to explain and predict behavior, the implementation intention has rarely been used in information privacy literature. We hope this study will attract more information privacy researchers to the concept of implementation intention while considering privacy-related behaviors in the future.

From a practical perspective, the findings of our study offer practitioners insights regarding the privacy paradox in the use of social media privacy settings. Furthermore, our study provides the theoretical foundation for not only social media privacy policymakers but also platform interface engineers and designers, especially those who are responsible for privacy settings. After several large-scale data breaches on social media, users are gradually losing their faith in service providers. It is a big fall but also an opportunity for service providers to win back their users' trust. While investing in the privacy policy, other efforts such as privacy settings and user interface should not be ignored. The service providers and other third parties encourage users to provide and share more information, whereas users are concerned about their privacy. Such a trade-off relationship should be considered seriously and wisely until a balance between the parties is achieved. To gain a long-term win-win relationship, social media providers should offer a more flexible and user-friendly system to protect and take control over their own personal information more effectively and efficiently. As mentioned earlier, frequent data breaches via social media have definitely increased users' concerns about their privacy. However, despite such serious concerns, users rarely take action to protect their personal information on social media. The study provides guidelines for social media users to manage and protect their privacy in the social media world. Therefore, users should be cautious when providing and sharing information on social media.

5.3. Limitations and Future Research

There might be several possible limitations in this study. First, we only identified the existence of a privacy paradox in the context of social media privacy setting use. We suggest that future studies should try to explain the privacy paradox in under-studied contexts such as the use of social media privacy settings, and thus investigate the factors that influence the dichotomy between privacy attitude and behavior, that is, the privacy paradox. As a complex phenomenon, the privacy paradox needs further approaches from multiple perspectives.

Second, we examined the factors that determine the use of social media privacy settings in the present

study. However, we only specified the antecedents to the intention and emphasized the mediating role of implementation intention in bridging the relationship between intention and behavior. Fortunately, we confirmed that the implementation intention positively mediated the intention-behavior relationship and had better explanatory power than intention. Therefore, we assume that future studies should focus more on the notion of implementation intention in the information privacy literature. For instance, further studies must investigate the antecedent factors of implementation intention to improve the ability to explain and predict actual behaviors.

Third, to some extent, data collected in this study were self-reported. To measure the use of social media and privacy settings, we designed a series of survey questions that relied on the respondents' own reports. To gather relatively more accurate data, however, we gave respondents additional instructions so that they could check their social media accounts for reference while responding to the survey questions, especially those regarding the behavior of using social media privacy settings. Despite all this, the data used in this study may have the same disadvantages as self-reported data. Such subjective and biased data may cause measurement errors, thus influencing the analysis results. Therefore, instead of surveys, we encourage future research to apply other methods to collect more objective and unbiased data.

Fourth, as noted earlier, respondents in this study were undergraduate and graduate students in South Korea. The choice and size of the sample may be unable to represent all social media users perfectly. Thus, the study results may not be generalizable beyond the research context. Future research should choose samples with wider ranges and a larger number of subjects.

5.4. Conclusion

In the study, we first confirmed the existence of a privacy paradox by testing the relationship between privacy concerns and behaviors of using social media privacy settings. We then identified the factors that determine the use of social media privacy settings by verifying the dichotomy between privacy concerns and behavior. Considering the mediator implementation intention to bridge the gaps between privacy attitudes, intentions, and behaviors, we explain and predict the use of social media privacy settings effectively and efficiently, thus alleviating the privacy paradox. Therefore, we encourage more information privacy researchers to consider the implementation intention in future studies. We hope the study findings will offer practitioners insights about the privacy paradox regarding the use of social media privacy settings and provide a theoretical foundation for privacy policymakers and platform interface engineers and designers. To retrieve users' trust and build a long-term win-win relationship, we suggest social media providers offer more flexible and user-friendly systems to share as much information as they want and enjoy various benefits without worrying about their privacy. Furthermore, we hope this study will alert users to the possibility of a privacy threat and risks of social media and provide guidelines to social media users to actively protect and manage their own privacy while using social media.

<References>

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

[2] Acquisti, A. (2004). Privacy in electronic commerce

and the economics of immediate gratification. *In Proceedings of the 5th ACM Conference on Electronic Commerce*, EC'04, 21-29.

[3] Acquisti, A., and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle and G. Danezis (eds.), *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, 36-58.

[4] Adam, A. F., and Fayolle, A. (2016). Can implementation intention help to bridge the intention-behaviour gap in the entrepreneurial process? An experimental approach. *The International Journal of Entrepreneurship and Innovation, 17*(2), 80-88.

[5] Agarwal, R., and Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665-694.

[6] Aivazpour, Z., and Rao, V. S. (2020). Information disclosure and privacy paradox: The role of impulsivity. A*CM SIGMIS Database: The DATABASE for Advances in Information Systems, 51*(1), 14-36.

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

[8] Ajzen, I., and Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

[9] Armitage, C. J., and Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology, 40*(4), 471-499.

[10] 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, 30*(1) 13-28.

[11] 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.

[12] Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*(4), 133-152.

[13] 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.

[14] 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.

[15] Belanger, F., Hiller, J. S., and Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

[16] 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.

[17] Boyd, D., and Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8), 1.

[18] Brandtzæg, P. B., Lüders, M., and Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human-Computer Interaction, 26*(11-12), 1006-1030.

[19] Cho, H., Lee, J. S., and Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995.

[20] Choon, M. J. K. (2018). Revisiting the privacy paradox on social media: An analysis of privacy practices associated with Facebook and Twitter. *Canadian Journal of Communication, 43*(2). doi: 10.22230/cjc.2018v43n2a3267

[21] De Wolf, R., Willaert, K., and Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies

in Facebook. *Computers in Human Behavior, 35*, 444-454.

[22] Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

[23] Deuker, A. (2009). Addressing the privacy paradox by expanded privacy awareness-the example of context-aware services. In *IFIP prime life international summer school on privacy and identity management for life* (pp. 275-283). Springer, Berlin, Heidelberg.

[24] Dinev, T., and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.

[25] Dinev, T., and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

[26] Du, J., Jiang, C., Chen, K. C., Ren, Y., and Poor, H. V. (2018). Community-structured evolutionary game for privacy protection in social networks. *IEEE Transactions on Information Forensics and Security, 13*(3), 574-589.

[27] Dwyer, C., Hiltz, S., and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*, 339.

[28] Fishbein, M., and Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Massachusetts: Addison-Wiley Publishing Company.

[29] Flender, C., and Müller, G. (2012). Type indeterminacy in privacy decisions: The privacy paradox revisited. In *International Symposium on Quantum Interaction* (pp. 148-159). Springer, Berlin, Heidelberg.

[30] Frik, A., and Gaudeul, A. (2020). A measure of the implicit value of privacy under risk. *Journal of Consumer Marketing, 37*(4), 457-472.

[31] 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.

[32] Ginosar, A., and Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management, 54*(7), 948-957.

[33] Gollwitzer, P. M. (1993). Goal achievement: The role of intentions. E*uropean Review of Social Psychology, 4*(1), 141-185.

[34] Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist, 54*(7), 493-503.

[35] Gollwitzer, P. M. (2014). Weakness of the will: Is a quick fix possible? *Motivation and Emotion, 38*(3), 305-322.

[36] Gollwitzer, P. M., and Brandstätter, V. (1997). Implementation intentions and effective goal pursuit. *Journal of Personality and Social Psychology, 73*(1), 186-199.

[37] Gollwitzer, P. M., and Schaal, B. (1998). Metacognition in action: The importance of implementation intentions. *Personality and Social Psychology Review, 2*(2), 124-136.

[38] 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.

[39] Grimmer, M., and Miles, M. P. (2017). With the best of intentions: A large sample test of the intention-behaviour gap in pro-environmental consumer behaviour. International Journal of Consumer Studies, 41(1), 2-10.

[40] Gross, R., and Acquisti, A. (2005). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71-80.

[41] Hallam, C., and Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217-227.

[42] Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook news

feed privacy outcry. *Electronic Commerce Research and Applications, 9*(1), 50-60.

[43] Hoffman, D. L., Novak, T. P., and Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85.

[44] Hsieh, S. H., and Lee, C. T. (2020). Traces of mobility: Examining location disclosure on social networks with mobile location tagging. *Telematics and Informatics, 49*, 101366.

[45] Hsu, M. H., and Kuo, F. Y. (2003). The effect of organization-based self-esteem and deindividuation in protecting personal information privacy. *Journal of Business Ethics, 42*(4), 305-320.

[46] Hughes-Roberts, T. (2013). Privacy and social networks: Is concern a valid indicator of intention and behaviour? *In Proceedings of the 2013 International Conference on Social Computing*, 909-912.

[47] Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

[48] Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2). doi: 10.1111/j.1083-6101.1999.tb00337.x

[49] Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

[50] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

[51] Krishnamurthy, B., and Wills, C. E. (2008). Characterizing privacy in online social networks. *In Proceedings of the First Workshop on Online Social Networks*, 37-42.

[52] Lee, N., and Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. Expert Systems with Applications, 42(5), 2764-2771.

[53] Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

[54] Li, Y., Vishwamitra, N., Hu, H., and Caine, K. (2020). Towards A taxonomy of content sensitivity and sharing preferences for photos. *In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-14.

[55] Lowry, P. B., Cao, J., and Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163-200.

[56] MacMillan, D., and McMillan, R. (2018, October 8). Google exposed user data, feared repercussions of disclosing to public. *Wall Street Journal*, https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194

[57] Madejski, M., Johnson, M., and Bellovin, S. M. (2011). *The failure of online social network privacy settings*. Columbia University, Technical Report CUCS-010-11. doi: 10.7916/D8NG4ZJ1

[58] Madejski, M., Johnson, M., and Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. *In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 340-345.

[59] McKnight, D. H., Choudhury, V., and Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

[60] Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M., and Leon, P. G. (2016). (Do Not) Track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies, 2016*(2), 135-154.

[61] Millham, M. H., and Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media &*

Society, 20(1), 50-67.

[62] Mosteller, J., and Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *Journal of Interactive Marketing, 39*, 27-38.

[63] Netter, M., Riesner, M., Weber, M., and Pernul, G. (2013). Privacy settings in online social networks-preferences, perception, and reality. *In 2013 46th Hawaii International Conference on System Sciences*, 3219-3228.

[64] 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.

[65] Nunnally J. C. (1978). An overview of psychological measurement. In B. B. Wolman (ed.), *Clinical diagnosis of mental disorders* (pp. 97-146). Boston, MA: Springer.

[66] Oomen, I., and Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management* (pp. 121-138). Boston, MA: Springer.

[67] Papies, E. K. (2017). Situating interventions to bridge the intention-behaviour gap: A framework for recruiting nonconscious processes for behaviour change. *Social and Personality Psychology Compass, 11*(7), e12323.

[68] Podsakoff, P. M., and Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531-544.

[69] Prestwich, A., and Kellar, I. (2014). How can the impact of implementation intentions as a behaviour change intervention be improved? *European Review of Applied Psychology, 64*(1), 35-41.

[70] Ramaswami, S. N., Srinivasan, S. S., and Gorton, S. A. (1997). Information asymmetry between salesperson and supervisor: Postulates from agency and social exchange theories. *Journal of Personal Selling & Sales Management, 17*(3), 29-50.

[71] Reynolds, B., Venkatanathan, J., Gonçalves, J., and Kostakos, V. (2011). Sharing ephemeral information in online social networks: Privacy perceptions and behaviours. *In IFIP Conference on Human-Computer Interaction*, 204-215.

[72] Schoenbachler, D. D., and Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2-16.

[73] Schwarzer, R., Richert, J., Kreausukon, P., Remme, L., Wiedemann, A. U., and Reuter, T. (2010). Translating intentions into nutrition behaviors via planning requires self-efficacy: Evidence from Thailand and Germany. *International Journal of Psychology, 45*(4), 260-268.

[74] Sheeran, P. (2002). Intention-behavior relations: A conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1-36.

[75] Sheeran, P., and Orbell, S. (1999). Implementation intentions and repeated behaviour: Augmenting the predictive validity of the theory of planned behaviour. *European Journal of Social Psychology, 29*(2-3), 349-369.

[76] Sheeran, P., and Silverman, M. (2003). Evaluation of three interventions to promote workplace health and safety: Evidence for the utility of implementation intentions. *Social Science & Medicine, 56*(10), 2153-2163.

[77] Sniehotta, F. F., Scholz, U., and Schwarzer, R. (2005). Bridging the intention-behaviour gap: Planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. *Psychology & Health, 20*(2), 143-160.

[78] Spottswood, E. L., and Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication, 22*(2), 55-70.

[79] Strater, K., and Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *People and Computers XXII Culture, Creativity, Interaction, 22*, 111-119.

[80] Sun, Y., Wang, N., Shen, X. L., and Zhang, J. X. (2015). Location information disclosure in location-

based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278-292.

[81] 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.

[82] Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis, 48*(1), 159-205.

[83] 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.

[84] Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior, 93*, 1-12.

[85] Utz, S., and Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2), 2.

[86] 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*(4), 923-941.

[87] Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472-480.

[88] Wall, J. D., and Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management, 56*(8), 103157.

[89] Webb, T. L., and Sheeran, P. (2007). How do implementation intentions promote goal attainment? A test of component processes. *Journal of Experimental Social Psychology, 43*(2), 295-302.

[90] Wisniewski, P. J., Knijnenburg, B. P., and Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies, 98*, 95-108.

[91] Xie, W., and Kang, C. (2015). See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior, 52*, 398-407.

[92] Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). Information privacy concerns: Linking perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 1.

[93] Yang, Q., Gong, X., Zhang, K. Z., Liu, H., and Lee, M. K. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management, 52*, 102065.

[94] Young, A. L., and Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500.

[95] Zafeiropoulou, A. M., Millard, D. E., Webber, C., and O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? *In Proceedings of the 5th Annual ACM Web Science Conference*, 463-472.

[96] Zhao, L., Lu, Y., and Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.

[97] Ziegelmann, J. P., Luszczynska, A., Lippke, S., and Schwarzer, R. (2007). Are goal intentions or implementation intentions better predictors of health behavior? A longitudinal study in orthopedic rehabilitation. *Rehabilitation Psychology, 52*(1), 97-102.

[98] Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., and Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115-123.

◆ About the Authors ◆

Jongki Kim

Jongki Kim is a professor in the School of Business at Pusan National University, Republic of Korea. He has a master's degree in MIS from Arkansas State University in USA and a doctor's degree in MIS from Misissippi State University in USA. His research interests include information security, privacy, e-commerce, management of technology, and behavioral economics.

Jianbo Wang

Jianbo Wang is a Ph.D. candidate in the School of Business at Pusan National University in Korea. She has a master's degree in MIS from Chungbuk National University in Korea. Her research interests include information security, privacy, behavioral science, and e-commerce, etc.

Submitted: August 18, 2020; 1st Revision: November 28, 2020; Accepted: December 10, 2020