

ACTUAL PRIVACY SELF-DISCLOSURE ON ONLINE SOCIAL NETWORK SITES: REFLECTIVE-IMPULSIVE MODEL

Jingzhi, Zhang, City University of Hong Kong, Hong Kong, jzhang257-c@my.cityu.edu.hk

Weiquan, Wang, City University of Hong Kong, Hong Kong, weiquan@cityu.edu.hk

Lara, Khansa, University of Virginia Tech, Blacksburg, Virginia, United States, larak@vt.edu

Sung, Kim, University of Wisconsin–Madison, Madison, Wisconsin, United States,
skim@bus.wisc.edu

Abstract

People are known to disclose their private information on social network sites (SNS) despite their concerns about threats of privacy invasions—a phenomenon dubbed as privacy paradox. Extant research on this phenomenon has primarily focused on the rational factors that affect the intentions of SNS users to disclose private information, rather than their actual disclosure behavior. We draw from the reflective-impulsive model that encompasses both rational factors (i.e., reflective system) and impulses (i.e., impulsive system) to explain users' actual disclosure of private information in SNS. We report two main findings from a survey of SNS users. First, for the reflective system, users use privacy settings to cope with their privacy concerns before engaging in their disclosure behavior. With the inclusion of this coping response, this study extends the widely applied privacy calculus model to identify only rational factors explaining disclosure of private information. Second, disclosure impulses significantly influence users' actual disclosure behavior in SNS, with social herding and attachment to an SNS stimulating their disclosure impulses in the SNS context. Theoretical and practical implications are discussed.

Keywords: online social network sites, privacy concerns, privacy protection via privacy settings, reflective-impulsive model, impulses, actual privacy disclosure.

1. Introduction

Privacy-related issues are a primary concern of people who use information technology (IT) in the information age (Acquisti et al. 2015). Users of social network sites (SNS), such as Facebook or Twitter, particularly expressed serious concerns about unexpected privacy intrusions that place their private information in unscrupulous hands. Despite their reported privacy concerns, SNS users are known to disclose massive amounts of sensitive and occasionally incriminating private information, such as their sexual orientation and political views in SNS. The paradoxical divide between the privacy attitudes of SNS users and their actual disclosure behavior (dubbed as privacy paradox) is problematic to SNS users, providers, and privacy policymakers (Barth and de Jong 2017).

Prior privacy paradox studies have been primarily based on the privacy calculus model, which explores various rational factors that lead to users' intentions in disclosing their private information (Barth and de Jong 2017). The privacy calculus model draws from theory of reasoned action, which assumes that users' behavioral intention is determined through rational analysis. In this analysis, SNS users weigh the benefits (e.g., hedonic value) and costs (e.g., privacy concerns) of intentional privacy disclosure (Dienlin and Metzger 2016; Dinev and Hart 2006).

The present research focuses on users' actual privacy disclosure behavior in SNS instead of their disclosure intentions (Kokolakis 2017). Intentions assume users' deliberations on privacy disclosure; however, people may behave without deliberations. The privacy calculus model is useful in explaining the paradox between privacy disclosure intentions and concerns (Acquisti et al. 2015), but may insufficiently explicate the relationship between actual behavior and privacy concerns. Privacy disclosure intentions and actual disclosure are not always highly correlated (the correlation reported in the literature ranged from 0.01 to 0.53) (Sheeran 2002). Mark et al. (2013) found that the intentional privacy disclosure could only explain 1.5% of the variance of the actual disclosure in the context of location-based systems. Given the significant differences between behavioral intentions and actual behavior in the privacy disclosure context, extending privacy disclosure intentions and studying both deliberations and "out of deliberations" of actual privacy disclosure behavior are imperative.

To include both deliberations and "out of deliberations" of actual privacy disclosure behavior, we apply a dual-system perspective, which argues that actual behavior is not only driven by a reflective, reasoning system but also driven by a reactive, quick system. Specifically, we apply the reflective-impulsive model (RIM) as the dual-system perspective to reveal factors leading to users' actual disclosure of private information in SNS (Deutsch et al. 2016). We select the RIM among other dual-system models for two reasons. First, impulsively disclosing information in SNS is quite striking, and the RIM delineates an impulsive system explaining actual behavior. Qahari-Saremi from DePaul University obtained 342 responses from undergraduates and reported that most experienced impulsively disclosing on Facebook (Turel and Qahari-Saremi 2016). U.S. president Donald Trump was reported on his "Twitter Impulses" since his inauguration (CNN 2017). We choose to apply the RIM as the overarching theoretical framework to explain users' disclosure behavior in SNS, given widespread impulses in SNS. Therefore, via applying RIM, we propose our first research question: To what extent and why will impulses influence privacy disclosure in SNS?

Second, SNS normally provides users with coping methods to deal with the adverse outcomes of privacy disclosure, and the reflective system of the RIM considers individual coping responses to potentially negative outcomes of behavior (see (Hofmann et al. 2008) for a review). Users proactively disclose in SNS, which may lead to negative consequences. Users can configure privacy settings in SNS, such as audience selection and profile availability, to cope with potential consequences and protect their privacy online. The provision of coping responses to alleviate negative consequences in SNS is in line with the RIM, which theorizes the role of coping response in reflective systems given potentially negative consequences of behavior. By contrast, other dual-system models (e.g., Elaboration Likelihood Model) aim to understand the persuasion processes and outcomes. These models generally focus on individuals' attitude change as the outcome of persuasion, but fail to consider their proactive actions. Based on these dual-system models, individuals are not in the stage of coping to deal with adverse consequences of behavior. So, the second research question we tend to answer is that why coping responses will mitigate the effect of privacy concerns on privacy disclosure from a perspective of RIM.

This study contributes to the privacy literature by applying the RIM to explain users' actual disclosure of private information in SNS. Specifically, we explore the effects of impulses and coping responses on actual disclosure. We also extend the original RIM in the SNS context by identifying contextual stimuli of impulses.

The remainder of this work is organized as follows. In the following two sections, we first review the theoretical foundation of our research and then present our research model and develop hypotheses. Second, we explain our research method followed by our data analysis. Finally, we elaborate on the theoretical and practical contributions of our study and discuss the limitations of our study and avenues for future research.

2. Theoretical Background

2.1. RIM and Actual Behavior

RIM emanates from classical dual-system theories that conceptually describe two different types of thinking systems guiding human behaviors (Von Helmholtz 1867). One system leads individuals unconsciously and reactively to engage in the behavior, while the other system reflects their reasoning to make a behavioral decision (Deutsch et al. 2016; Strack and Deutsch 2004; Turel and Qahri-Saremi 2016). RIM has advanced this notion of dual-system theories by identifying two systems that determine individuals' behavior, namely, the reflective system and the impulse system (Deutsch et al. 2016). The reflective system elicits behavioral decisions that are based on reasoning thinking, while the impulsive system generates impulses to engage in the behaviors (Deutsch et al. 2016). The findings in biological research have long supplemented that these two kinds of thinking routes of RIM originate from two different areas of the brain (Bechara 2005).

The impulsive system under the RIM focuses impulses that influence individuals' behaviors (Deutsch et al. 2016). It is well-known that individuals' behavior intermittently lacks reasoning (Strack and Deutsch 2004). To account for this lack of reasoning, most prominently, Freud et al. (1933 proposed that unconscious processes (e.g., an impulsive system) play a significant role in determining actual behavior although individuals are not always aware of these processes. The impulsive systems will trigger impulses (also dubbed as impulsions) that influence behaviors (Turel and Qahri-Saremi 2016).

An impulsive system essentially is an associative cluster in which individuals directly associate a stimulus with its behavioral schema. For example, if individuals see something beautiful, then they will directly recall the behavioral schema of disclosure in SNS (for instance, after taking a picture of it, uploading the photo in SNS and sharing it with friends). The underlying bond for the association between stimulus and behavioral schema is an urgent desire elicited by the stimulus.

Consistent with prior research, we define the urgent desire as an *impulse* (Rook 1987). An urgent desire is part of the stable dispositions of individuals. For example, if individuals have urgent desires to exert violence on others, they are predisposed toward violence. Individuals will be susceptible to such an urgent desire (i.e., an impulse) if individuals' desires can be immediately satisfied in a context. For example, the desire for "owning a fine dress" can be immediately satisfied by purchasing in a store, or the desire for "showing off my figure" can be immediately fulfilled by a disclosure in SNS. If a desire is immediately realized, then it will summon the tension with which individuals pay attention to desire (Acquisti 2004). As individuals recognize that the immediate gratification, they would like to be spend efforts right now to achieve the immediate gratification (Acquisti 2004). Then, the stimulus that provokes the desire intensely bond with the behavioral schema. An impulse forms and effects in individuals' manners in such a context relative to the impulsive system.

2.2. Privacy Calculus Model in the Reflective System

In contrast to the impulsive system, the influences of the reflective system on actual behavior are assumed to operate in a thoughtful and effortful manner. A reflective system employs a thoughtful analysis to make decisions on actual behavior. Thus, the reflective system is a relatively slow and effortful process compared with the impulsive system (Deutsch et al. 2016).

Prior privacy studies have primarily focused on the reflective system and behavioral intentions only. In privacy literature, prior research has proposed the privacy calculus model to represent the reflective system. Consistent with the core ideas of the reflective system under RIM, the most widely used privacy calculus model in the privacy literature has stated that an individual’s decision to engage in privacy-related behavior is cognitive and reasoning. In this study, we extend privacy calculus model from intentions to behavior using the privacy calculus model as basis.

Privacy calculus model suggests that privacy self-disclosure intention is a result of *calculus*, in which drivers and inhibitors simultaneously influence intentional disclosure (Kehr et al. 2015). Drivers positively influence intentional disclosure, whereas inhibitors negatively affect intentional disclosure. The set of drivers refer to the values of disclosure behavior. Values are individual views on rewards (i.e., what they can receive) of disclosing privacy. A general review of values recognized that individuals evaluate the (1) utilitarian and (2) hedonic values of rewards from their behaviors (Kim et al. 2005). The two values capture the two basic needs of human beings: the former covers the need “to get something functional or substantial” from performing an act, whereas the latter implies “to get something emotional or spiritual” from performing an act (Barry 1994).

A set of inhibitors refer to privacy concerns. Privacy concerns are “individuals’ subjective views of fairness within the context of privacy.” Prior research has demonstrated that privacy concerns exist in many IS contexts, which require its users to provide personal information including e-commerce, synchronous online social community, and social network sites. In calculus, the influence of one set may outweigh the other set, but each set does not eradicate the contradicting influence of the other set. As a result of privacy calculus, users may sacrifice their privacy concerns in exchange for rewards perceived to be worth having or they may yield to their privacy concerns, thereby giving up rewards (Jiang et al. 2013).

3. Hypothesis Development

To understand actual disclosure behavior in SNS, we draw support from the RIM to develop our theoretical model, as shown in Figure 1. Our model consists of two parts: the reflective and impulsive systems. We posit our hypotheses in the following sections.

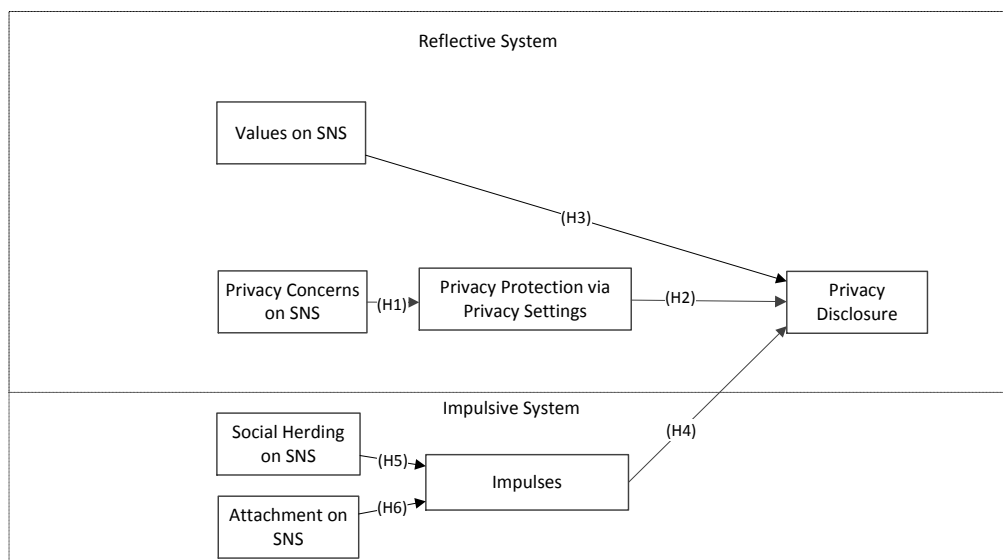


Figure 1. Proposed Theoretical Framework

3.1. Reflective System of Disclosure Behavior

Coping responses in SNS could help individuals deal with potential privacy concerns. Prior privacy literature has identified various coping responses, such as configuring privacy settings, complaining, and removing privacy threats on the Internet. In SNS, the most common and leading coping method provided is in privacy settings, which is now widely accepted and acknowledged by SNS users (Lewis et al. 2008). SNS users often utilize privacy settings to cope with their privacy concerns of disclosure.

Consistent with the framework provided for the reflective system, we first contend that privacy concerns will positively influence the privacy protection via privacy settings (i.e., coping responses in SNS). Concerns originate from opportunities of disclosing privacy to unexpected audiences such as marketing firms, hackers, and cyberbullies. The leakage of privacy in SNS to those unexpected users may lead to adverse outcomes: cyber manhunt, and spam harassment. Thus, individuals may be concerned about the negative outcomes of their privacy self-disclosure. High privacy concerns suggest that users think these adverse outcomes are dangerous and intolerable. When users are highly concerned about their privacy in SNS, they may rationally start to seek ways to control threats. Through privacy protection via privacy settings, they could minimize privacy threats and relieve their privacy concerns (Witte 1992). For example, audience selection represents privacy settings in SNS that may alleviate their privacy concerns which originate from unexpected audiences. If they have minimal privacy concerns, then dealing with the privacy threats will no longer be necessary. Hence, we hypothesize our H1:

H1: Privacy concerns positively influence privacy protection via privacy settings in SNS.

Users' privacy concerns trigger privacy protection via privacy settings, which leads SNS users to disclose. A sense of safety may be generated after mitigating the concerns of individuals about who could access their privacy by managing audience prior to actual disclosure. In SNS, privacy settings provide a homey setting where users hope to express their opinions freely and share their stories and pictures with their SNS friends. By acquiring and utilizing privacy protection products or services, such as the ones we previously mentioned, people are reassured that their privacy is safe. Moreover, the sense of safety provides individuals a context to disclose freely and privately. Therefore, we propose our H2:

H2: Privacy protection via privacy settings positively influences privacy disclosure.

According to the privacy calculus model, we believe that the utilitarian and hedonic values will positively influence actual disclosure behavior (Keith et al. 2013). SNS users can effectively communicate with their circle of friends and acquaintances through disclosure behavior. Compared with other communication technologies such as telephone or instant messages, disclosing in SNS could communicate with the social network by just one-click (Krasnova et al. 2010). The effectiveness of communication is quite useful and functional. Users might think that it is worthy to disclose their privacy in exchange for such a useful reward. The other key value of disclosure in SNS is the hedonic value. By disclosing, some SNS users can interact with and entertain with their friends. Some users may find privacy disclosure playful and interesting (Krasnova et al. 2010). They might think the hedonic value is valuable compared with their privacy concerns especially when they are upset. They may disclose their hobbies and interest in SNS in anticipation of hedonic values. Therefore, we hypothesize the following:

H3: Values positively affects privacy disclosure.

3.2. Effects and Stimuli of Impulses in the Impulsive System

Aligned with prior research, we believe that SNS users possess urgent desires (i.e., impulse) to disclose in SNS. Some SNS users may be narcissistic, who highly appreciate themselves and have an urgent desire to disclose their self-images. Some users are quite self-respectful, then they have an ideal self-identity in mind and an urgent desire to express who they should be in SNS via privacy disclosure.

An impulse for privacy disclosure leads to disclosure behavior in SNS, and it predisposes individuals to disclose their private information in SNS because the impulse matches individuals' dispositions. For example, when SNS users have an impulse to disclose a selfie in SNS, they predispose to focus on the selfie and how to share it in SNS (uploading, writing a caption, and posting) (Turel and Qahri-Saremi 2016). In SNS, if individuals feel that the desire for disclosure will come soon, then they may intensely wait for the realization of desire. Thus, we believe some individuals have impulses for disclosure in SNS. We propose H5:

H4: An impulse for privacy disclosure positively influences privacy disclosure.

Various stimuli in a context could trigger individual impulses. The stimuli of impulses are generally classified as either external or internal. Internal stimuli originate from the inner states of an individual. By contrast, external stimuli are from the context. We specifically identify one representation of each type of stimuli related to the context of SNS.

Individuals sometimes see a crowd of people doing the same thing — a situation that is conceptualized as social herding (Prechter Jr 2001). In SNS, many kinds of social herding exist in which a crowd of users discloses the same type of information. A typical example of the social herding in SNS is the “positive-body” movement on Instagram. In the movement, many users post the photo of their imperfections in the body in SNS.

Given that individuals’ impulses are easily triggered by others especially in the environment where a crowd of people is doing the same thing (Prechter Jr 2001), we contend that social herding in SNS will trigger impulses of privacy disclosure. Many users disclose private information (such as selfies) in these trendy topics to receive attention from others users, and become popular and attractive (Baddeley 2013; Dholakia et al. 2004). Other SNS users who see those popular people’ disclosure of private information under these trendy topics may produce an urgent desire to become popular and attractive in SNS (Posey et al. 2010). The urgent desire to become popular may stimulate a sudden urge of the users to get involved in these topics and to become popular through disclosing the similar private information if needed. Thus, social herding of SNS will trigger users’ impulse of privacy disclosure, and we posit the following:

H5: Social herding in SNS triggers impulses for privacy disclosure.

The attachment to SNS implies that SNS users developed a special bond with SNS. Most prior research has demonstrated that individuals establish an attachment to their SNS accounts because they can receive care and comfort from their social network. A survey conducted in the U.S. showed that some SNS users, especially teenagers, feel anxious to detach from SNS (Forgas 2011), which implies that some users are attached to SNS.

We believe attachment to SNS also triggers disclosure impulses (as a kind of internal stimulus), and suggests that individuals feel that they are part of the online community through SNS. Being part of a community decides that SNS users would like to have an urgent desire to contribute to such community (Forgas 2011). They will also stand on the position of SNS, so its negative sides are dulled to them. Moreover, individuals who are attached to SNS also fear detaching from the community in SNS. They are afraid of losing the special bond within the community. Under such fear, they will probably have an urgent desire to contribute to SNS by privacy disclosure, which is out of control. In this manner, the impulse for privacy disclosure is activated. We hypothesize that:

H6: Attachment to SNS triggers impulses for privacy disclosure.

4. Research Method

We conducted a survey to test our hypotheses. The survey consists of two parts: a self-reported part and a peer-rated part. In the self-reported part, we measured independent variables (IVs) and control variables (CVs) from respondents, including privacy concerns, values, privacy protection via privacy settings, impulses, attachment, social herding, age, gender, privacy invasion experiences. In the peer-rated part, we measured the dependent variable (DVs) (i.e., privacy disclosure) from respondents’ partners, because we intended to minimize the common method bias by measuring the IVs and DVs with different data sources (Bagozzi 2011; MacKenzie and Podsakoff 2012).

Appendix 1 shows the measurement items used in this study. We adapted our self-reported measurements from existing well-established measurements. We specifically developed a measurement of peer-rated actual disclosure. We first adopted nine items for disclosure behavior from Krasnova et al. (2009; Krasnova et al. (2010. Then we ensured that every item of peer-rated privacy disclosure after adapting is consistent with our context (Weibo), target (partner) and behavior (privacy disclosure) (Kim et al. 2012). To further ensure the content validity, we invited three subject experts to review the 9 items for respondents’ peers and all 9 items have been accepted by them. The finalized peer-rated privacy disclosure items are shown in online appendix 2.

We selected Weibo.com (similar to Twitter.com) as our SNS context because it is the largest and leading SNS in China. Approximately 43.5% of Internet users in China reportedly used Weibo in 2016, and 48.5% of these users posted their information and photos on this platform (CNNIC 2017). Weibo.com allows users to follow others without others’ consent, and the profiles of users are open to the public.

This SNS also provides privacy settings prior to privacy disclosure. These characteristics are necessary for measuring privacy disclosure and privacy protection via privacy settings.

Data were collected in two. The first stage consisted of participant recruitment and online registration. We required respondents to find a partner and come to a laboratory by pair and then assess each other's disclosure behavior in SNS to measure actual privacy disclosure by peer rating. The partners were expected to be familiar with the participants, so that the former could judge whether the participants disclosed private information.

In Stage 2, 228 participants were required to answer the questionnaire. Particularly, in the peer-rated part of the survey, we asked participants to view three pages of original messages and embedded photos for approximately 10 minutes to measure the partners' privacy disclosure in microblog messages according to the nine items of peer-rated privacy disclosure. Namely, a pair of respondents measure each other's privacy disclosure in Weibo.

In our survey, we used reverse and similar items to guarantee that potential participants devoted sufficient time and attention to their answers. After transforming reverse-coded items, we excluded seven more participants from our final sample for having chosen the same or similar answers for reversed items and other one-variable items. The respondents in our study comprised 221 students, the respondent demographics are provided in Appendix 2.

5. Data Analysis

5.1. Measurement Model

We evaluated the reliability and the convergent and discriminant validity of the reflective constructs based on the standard analytical guidelines to assess the psychometric properties of the measurement items. Table 1 shows that the composite reliability and average variance extracted (AVE) from the reflective variables were substantially above their critical values of 0.7 and 0.5, respectively, which suggests a satisfactory level of reliability. Thereafter, we evaluated the convergent validity of the model by computing the item loadings. The results were above the 0.70 cut-off, thereby indicating satisfactory levels of convergent validity. Finally, adequate discriminant validity was established because the square roots of AVEs of each latent variable exceeded the correlations between the latent variable and other variables (see the cross elements in Table 1). We also checked the discriminant validity by analyzing the cross-loadings of the items. Adequate discriminant validity of the constructs was ascertained because the loading of each item on its latent variable was substantially higher than its loadings on other latent variables, as well as the loadings of other items on that same latent variable (see Table 1). Values in SNS are a formative variable in our model: the weight of hedonic value is 0.666 (t value = 17.234, $p < 0.001$), whereas the weight of utilitarian value is 0.460 (t value = 13.380, $p < 0.001$). These results show that our variables exhibited psychometrically desirable properties.

	Com. Rel.*	AVE	ATA	VAL	IMP	PRD	PC	PP	PPE	SH
ATA	0.90	0.74	1.00							
VAL	n.a.	n.a.	0.72	1.00						
IMP	0.90	0.76	0.40	0.37	1.00					
PRD	0.95	0.70	0.40	0.29	0.22	1.00				
PC	0.83	0.63	0.08	-.16	-0.01	-.03	1.00			
PP	0.96	0.93	0.21	0.14	-0.04	0.20	0.19	1.00		
PPE	0.87	0.78	-.08	-0.06	0.01	-0.06	0.38	-.02	1.00	
SH	0.85	0.60	0.35	0.37	0.41	0.17	-.05	0.01	0.05	1.00

Notes. * = Composite Reliability; n.a. = Not Available; ATA = Attachment to SNS; VAL = Values; IMP = Impulses; PRD = Peer-Rated Disclosure; PC = Privacy Concerns; PP = Privacy Protection via Privacy Setting; SH = Social Herding

Table 1. Properties of Measurement Scales

5.2. Structural Model

All model analyses were conducted using partial least squares (PLS) regression (Barclay et al. 1995). The SmartPLS version 2.0 tool (Ringle et al. 2005) was used to run all tests. The t-values were estimated for the loadings by using a 500-re-sampling bootstrapping technique. Table 2 shows the results of the hypotheses tests in our model, whereas Figure 2 shows the path coefficients and R² values of all variables in the model.

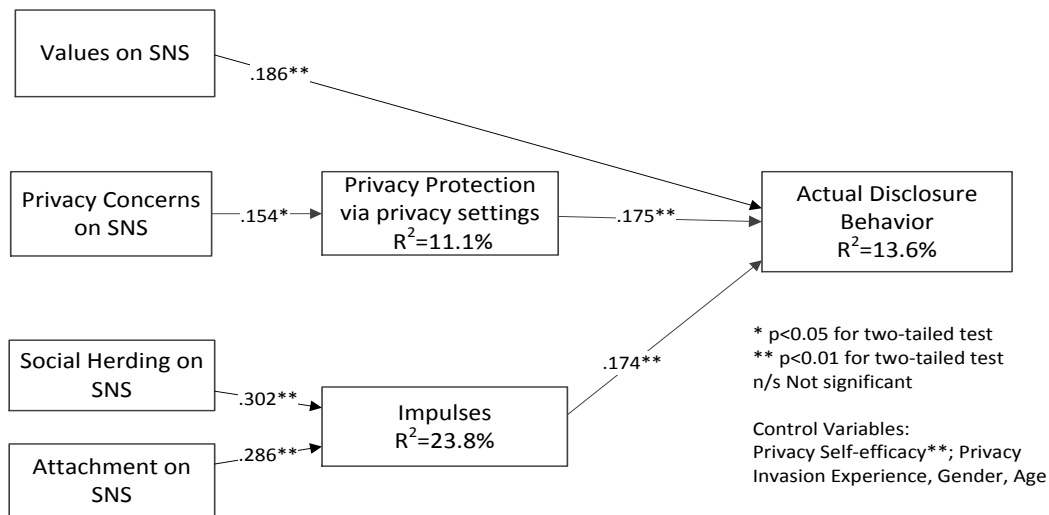


Figure 2. Results of Data Analysis

5.3. Results of Research Hypotheses

In the reflective system, privacy concerns in SNS positively influenced privacy protection via privacy settings (0.159, $p < 0.05$), lending support to H1. Privacy protection via privacy settings positively affected actual disclosure (0.175, $p < 0.01$), thereby supporting H2. Values also positively influenced on actual disclosure (0.186, $p < 0.01$), thus H3 was supported.

As for the impulsive system, the path between impulses and actual disclosure was significant (0.174, $p < 0.01$), lending support to H4. Moreover, attachment (0.286, $p < 0.01$) and social herding (0.302, $p < 0.01$) significantly influenced impulses for privacy disclosure. Thus, H5 and H6 were supported.

6. Discussion

6.1. Theoretical Implications

This research is one of the first IS studies to apply the RIM to explain users' actual privacy disclosure in SNS. The Privacy paradox is a long-standing puzzle for privacy researchers, and prior researchers have explained the paradox. Numerous prior studies have used the privacy calculus model, which assumes that the factors influencing disclosure intentions can be contradictory, and the influences of contrary factors such as concerns and values of disclosure are accountable for understanding privacy disclosure. The RIM perspective enhances the notions of the privacy calculus model that the contrary factors leading to the actual disclosure are reflective and cognitive, but the factors leading to actual disclosure can also be impulsive and reactive.

The RIM's embedding impulses are intuitively intriguing. The inclusion of impulses progresses the understanding of how people use SNS by providing a framework investigating impulsive factors that relate to particular characteristics of SNS. The SNS context provides a venue that immediately fulfills the natural desire of individuals for privacy disclosure. Individuals may feel captured by the desire for privacy disclosure and form an impulse for privacy disclosure in SNS because of this functionality,

which finally leads to disclosure behavior. SNS also allows individuals to be part of a community and interact with other users, and these functions relate to some stimuli of the impulse for privacy disclosure.

The RIM is theoretically contributory because it incorporates values, privacy concerns, and coping responses to deal with the potentially negative outcomes of privacy disclosure in the reflective system. The incorporation of these reflective factors that relate to particular characteristics of SNS can also progress the understanding of how people use SNS. The SNS context provides efficiency of communication and happiness to users when they interact with friends. These efficiency and happiness are sources of SNS values. This context also requires individuals to loosen their privacy to other users, leading to some potentially negative outcomes which are the origins of privacy concerns. The typical difference between the SNS context and other privacy contexts is that the SNS context normally installs privacy settings for users to deal with their privacy concerns.

This dual-system framework has implications for further research. First, our model may serve as a framework to understand other proactive and voluntary behaviors in IS contexts. The RIM is commonly applied to explain many proactive and voluntary behaviors, such as drinking alcohol, committing a crime, and consumer behaviors (Strack and Deutsch 2006) in other studies. Thus, our study suggests that IS research considers the RIM in deciding proactive behaviors in IS contexts (such as e-health, cybersecurity, technology crime, and e-commerce), especially when impulses are evidently observed in a specific IS context.

Second, our research suggests that including coping responses in dealing with potentially adverse consequences of behaviors. The results enhance understanding of online environments in which IS can lead to adverse consequences. The introduction of coping response between privacy concerns and disclosure behavior can also help explain why privacy concerns are ineffective in discouraging actual disclosure behavior in SNS.

6.2. Practical Implications

Adapting the reflective system to the SNS context reveals that privacy protection via privacy settings leads SNS users to disclose more private information than normal. We utilized these revelations to recommend SNS providers to remind their users about privacy settings which can efficiently protect user privacy and positively influence their actual disclosure. In the long run, reduced online privacy violations enable SNS providers to offer an improved platform for users to virtually interact with one another.

Overly impulsive disclosure behavior results in regrets and complaints (Wang et al. 2011), thus impulses influence actual disclosure, and social herding stimulates impulse. We suggest SNS practitioners to discourage social herding in SNS, especially some controversial and evil social herding. For example, the notorious social herding called “Blue Whale” where some people share how they commit suicide gradually. This kind of social herding may stimulate the impulses in both committing suicide and spreading fear in SNS.

6.3. Limitations

The first limitation of this study is derived from the context of Weibo.com. From a practical standpoint, involving other SNS contexts, such as Moment (similar to Snapchat) and Instagram, is better. Various SNS have different privacy settings and information dissemination methods (Choi et al. 2015). Therefore, the importance of coping or privacy concerns may differ. Future research could apply the RIM in other SNS contexts to identify more factors important under the dual systems.

Second, coping response is not objectively measured but self-reported. We could have better supported our arguments if our coping response measure objectively reflects the extent to which users coped with privacy threats in SNS. However, evaluating actual user coping response in SNS is quite difficult because capturing any change in their coping response prior to disclosure is nearly impossible. Despite this limitation, we believe our self-reported design could demonstrate the effect of coping response on the final disclosure behavior in the SNS context.

Acknowledgments:

The work described in the article was partially supported by grants from the Research Grants Council of Hong Kong S.A.R. (Project no. CityU 9041718), the National Natural Science Foundation of China (NSFC) (Project no. 71471156), and the Shenzhen Research Institute of the City University of Hong Kong.

Appendix 1: Measurement Items

Variable	Item	Item in English (on a 7-point scale: 1 “strongly disagree” to 7 “strongly agree;” unless otherwise noted)	References
Privacy Concerns on Weibo.com	PC1	I am concerned that the information I submit on weibo.com could be misused.	(Dinev and Hart 2006)
	PC2	I am concerned that a person can find private information about me on weibo.com.	
	PC2	I am concerned about submitting information on weibo.com, because of what others might do with it.	
Privacy Protection via Privacy Settings	PP1	I protect my profile through the privacy settings of weibo.com.	(Debatin et al. 2009)
	PP2	I have seriously set the options of my privacy settings on weibo.com.	
Utilitarian Value	UV1	The weibo.com is convenient to inform all my friends about my ongoing activities.	(Kim et al. 2005), (Krasnova et al. 2010)
	UV2	The weibo.com allows me to save time when I want to share something new with my friends.	
	UV3	I find weibo.com efficient in sharing information with my friends.	
Hedonic Value	HV1	When I am bored I often login to weibo.com.	(Krasnova et al. 2010)
	HV2	I find weibo.com entertaining.	
	HV3	I spend enjoyable and relaxing time on weibo.com.	
Impulses for privacy disclosure	Impul1	"Just do it" describes the way I disclose information on weibo.com.	(Rook and Fisher 1995) (Rook 1987)
	Impul2	"I think of it, I disclose it" describes my disclosure behavior on weibo.com.	
	Impul3	"Disclose now, think about it later" describes my disclosure behavior on weibo.com.	
Attachment to Weibo.com	Atach1	Weibo.com is part of my everyday activity.	(Ren et al. 2012; Schifferstein and Zwartkruis-Pelgrim 2008)
	Atach2	Weibo.com has become part of my daily routine.	
	Atach3	I feel out of touch when I haven't logged onto weibo.com for a while.	
Social Herding in SNS	SH1	I disclose myself on weibo.com because of the proportion of my friends that disclose themselves.	(Posey et al. 2010)
	SH2	I follow others in disclosing on weibo.com.	
Peer-Rated Disclosure	Dscl1	This person has lots of micro-blogging messages on weibo.com.	(Posey et al. 2010)

on Weibo.com	Dsc12	This person frequently updates his (her) micro-blogging message on weibo.com.	(Krasnova et al. 2009),(Posey et al. 2010)
	Dsc13	This person keeps his/her friends updated about what is going on in his (her) life through micro-blogging message on weibo.com.	
	Dsc14	This person often expresses his (her) feelings about himself (herself) on micro-blogging message of weibo.com.	
	Dsc15	This person often expresses his (her) personal beliefs and opinions on micro-blogging message of weibo.com.	
	Dsc16	This person's micro-blogging message disclosures on weibo.com cover fairly many aspects, e.g., personality, activities, work or study etc.	
	Dsc17	This person intimately discloses who he really is, openly and fully through micro-blogging message on weibo.com.	
	Dsc18	This person often discloses intimate, personal things about himself (herself) on micro-blogging message of weibo.com.	
	Dsc19	From this person's weibo.com message it would be easy to find out his (her) life.	
	Privacy Self-efficacy	Efcy1	
Efcy2		I have the expertise needed to avoid privacy invasions towards my online personal information on weibo.com.	
Efcy3		I could successfully avoid privacy invasions towards my online personal information on weibo.com.	
Prior Privacy Invasion Experience	PrvExp1	How often have you personally been the victim of what you felt was an improper invasion of your privacy on social networking websites?	(Smith et al. 1996)
	PrvExp2	How many times of personal information misuse have you encountered in the past?	

Appendix 2: Descriptive Statistics of the Sample (Gender, Grade, and Birth year)

Item	Frequency	Item	Frequency
Gender		Partnership familiarity (1~5, mean=4.10)	
Male	130 (58.8%)	Not familiar at all	0
Female	91 (41.2%)	Slightly familiar	5 (2.3%)
		Somewhat familiar	60 (27.1%)
		Moderately familiar	67 (30.3%)
		Extremely familiar	89 (40.3%)
Grade		Birth Year	
Freshman	3 (1.3%)	1980~1985	7 (3.2%)
Sophomore	9 (3.9%)	1986~1987	18 (8.1%)

Junior	23 (10.1%)	1988	25 (11.3%)
Senior	26 (11.4%)	1989	49 (22.2%)
Graduate-1 st Year	101 (44.3%)	1990	65 (29.4%)
Graduate-2 nd Year	42 (18.4%)	1991~1992	42 (19.0%)
Graduate-3 rd Year	3 (1.3%)	1993~1995	15 (6.8%)
PhD	21 (9.2%)		

References

- Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proceedings of the 5th ACM Conference on Electronic Commerce (EC'04)*, New York, USA: ACM, pp. 21-29.
- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509-514.
- Bagozzi, R. P. 2011. "Measurement and Meaning in Information Systems and Organizational Research: Methodological and Philosophical Foundations," *MIS Quarterly* (35:2), pp. 261-292.
- Barclay, D., Higgins, C., and Thompson, R. 1995. "The Partial Least Squares (Pls) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp. 285-309.
- Barth, S., and de Jong, M. 2017. "The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—a Systematic Literature Review," *Telematics and Informatics*.
- Bechara, A. 2005. "Decision Making, Impulse Control and Loss of Willpower to Resist Drugs: A Neurocognitive Perspective," *Nature neuroscience* (8:11), pp. 1458 - 1463.
- CNN. 2017. "Cnn to Trump Campaign: No 'Enemies' Ad, Thank You Very Much,"
- CNNIC. 2017. "2016 Sns Users Behavior Analysis Report in China."
- 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), pp. 83-108.
- Deutsch, R., Gawronski, B., and Hofmann, W. 2016. *Reflective and Impulsive Determinants of Human Behavior*. Psychology Press.
- Dienlin, T., and Metzger, M. J. 2016. "An Extended Privacy Calculus Model for Sns: Analyzing Self-Disclosure and Self-Withdrawal in a Representative Us Sample," *Journal of Computer-Mediated Communication* (21:5), pp. 368-383.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.
- Forgas, J. P. 2011. "Affective Influences on Self-Disclosure: Mood Effects on the Intimacy and Reciprocity of Disclosing Personal Information," *Journal of Personality and Social Psychology* (100:3), pp. 449-461.
- Freud, S., Spratt, W. J. H., and Strachey, J. 1933. *New Introductory Lectures on Psycho-Analysis*. Norton New York.
- Hofmann, W., Friese, M., and Wiers, R. W. 2008. "Impulsive Versus Reflective Influences on Health Behavior: A Theoretical Framework and Empirical Review," *Health Psychology Review* (2:2), pp. 111-137.
- Jiang, Z. J., Heng, C. S., and Choi, B. C. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.
- Kankanhalli, A., Tan, B. C., and Wei, K.-K. 2005. "Contributing Knowledge to Electronic Knowledge Repositories: An Empirical Investigation," *MIS Quarterly* (29:1), pp. 113-143.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.

- 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), pp. 1163-1173.
- Kim, S. S., Malhotra, N. K., and Narasimhan, S. 2005. "Research Note—Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research* (16:4), pp. 418-432.
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp. 122-134.
- Krasnova, H., Kolesnikova, E., and Guenther, O. 2009. "" It Won't Happen to Me!": Self-Disclosure in Online Social Networks," in: *15th Americas Conference on Information Systems*. San Francisco, CA: pp. 1-9.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.
- Lewis, K., Kaufman, J., and Christakis, N. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," *Studierende und Privatsphäre: Eine Analyse der Privatsphäre-Einstellungen in einem sozialen Online-Netzwerk*. (14:1), pp. 79-100.
- MacKenzie, S. B., and Podsakoff, P. M. 2012. "Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies," *Journal of Retailing* (88:4), pp. 542-555.
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities," *European Journal of Information Systems* (19:2), pp. 181-195.
- Prechter Jr, R. R. 2001. "Unconscious Herding Behavior as the Psychological Basis of Financial Market Trends and Patterns," *The Journal of Psychology and Financial Markets* (2:3), pp. 120-125.
- Ren, Y., Harper, F. M., Drenner, S., Terveen, L. G., Kiesler, S. B., Riedl, J., and Kraut, R. E. 2012. "Building Member Attachment in Online Communities: Applying Theories of Group Identity and Interpersonal Bonds," *Mis Quarterly* (36:3), pp. 841-864.
- Ringle, C. M., Wende, S., and Will, S. 2005. "Smartpls 2.0 (M3) Beta." Hamburg, Germany.
- Rook, D. W. 1987. "The Buying Impulse," *Journal of Consumer Research* (14:2), pp. 189-199.
- Rook, D. W., and Fisher, R. J. 1995. "Normative Influences on Impulsive Buying Behavior," *Journal of Consumer Research* (22:3), pp. 305-313.
- Rosen, P., and Sherman, P. 2006. "Hedonic Information Systems: Acceptance of Social Networking Website," in: *12th Americas Conference on Information Systems*. Acapulco, Mexico.
- Schifferstein, H. N., and Zwartkruis-Pelgrim, E. P. 2008. "Consumer-Product Attachment: Measurement and Design Implications," *International journal of design* (2:3).
- Sheeran, P. 2002. "Intention—Behavior Relations: A Conceptual and Empirical Review," *European review of social psychology* (12:1), pp. 1-36.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS quarterly* (20:2), pp. 167-196.
- Strack, F., and Deutsch, R. 2004. "Reflective and Impulsive Determinants of Social Behavior," *Personality and Social Psychology Review* (8:3), pp. 220-247.
- Strack, F., and Deutsch, R. 2006. "Reflective and Impulsive Determinants of Consumer Behavior," *Journal of Consumer Psychology* (16:3), pp. 205-216.
- Turel, O., and Qahri-Saremi, H. 2016. "Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective," *Journal of Management Information Systems* (33:4), pp. 1087-1116.
- Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.
- Von Helmholtz, H. 1867. *Handbuch Der Physiologischen Optik*. Voss.
- Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communications Monographs* (59:4), pp. 329-349.