To appear in CCF Transactions on Pervasive Computing and Interaction

Antecedents of Collective Privacy Management in Social Network Sites: A Cross-Country Analysis

Yao Li[1] (corresponding author), Hichang Cho[2], Reza Ghaiumy Anaraky[3], Bart Knijnenburg[3], Alfred Kobsa[4]

[1]School of Modeling, Simulation and Training, University of Central Florida

Address: 4000 Central Florida Blvd. Orlando, Florida, 32816, USA

[2]Department of Communications and New Media, National University of Singapore

Address: 21 Lower Kent Ridge Rd, Singapore 119077

[3]Department of Human-Centered Computing, Clemson University

Address: Clemson University, Clemson, SC 29634, USA

[4]Department of Informatics, University of California, Irvine

Address: Donald Bren Hall, Irvine, California 92697, USA

E-mail:

Yao Li: yao.li@ucf.edu

Hichang Cho: hichang_cho@nus.edu.sg

Reza Ghaiumy Anaraky: rghaium@clemson.edu

Bart Knijnenburg: bartk@clemson.edu

Alfred Kobsa: kobsa@uci.edu

Abstract

In this paper, we examine the psychological antecedents of privacy management strategies in social network sites (SNS) and extend the understanding to *collective* privacy management. By surveying Facebook users in the US (N = 454), Singapore (N = 467) and South Korea (N = 472), we are able to test our prediction model in these three countries to examine whether the effects of the antecedents are robust from a cross-country perspective. Although some of the effects are significantly different between the three countries, we find that in general users' privacy attitudes, social norms, and self/collective control beliefs substantially predict the adoption of collective privacy management strategies. These findings contribute to the explanations of users' adoption of behavioral privacy management strategies. We conclude with global and country-specific recommendations regarding future privacy designs for collective privacy management.

Keywords: collective privacy management; social network site; social norm; perceived control belief

1 Introduction

The increasing use of social network sites (SNSs) has caused growing concerns about personal information disclosure. Millions of SNS users share vast amounts of personal information in online social interactions, including their names, photos, locations, and stories from their personal life. This can lead to threats to personal information privacy. Information privacy refers to the ability of the individual to personally control information about oneself [54]. Losing control over personal information may cause privacy risks, including inadvertent disclosure, online stalking, identity theft, unwanted contact, harassment, and personal data misuse by third parties [8]. These privacy risks in online social networking have in turn challenged the continued usage of SNSs and the social relationships between people. Thus, most SNSs provide privacy settings for users to control their information disclosure.

Aside from the embedded privacy settings, users also employ a variety of behavioral coping strategies, namely privacy management strategies, to address their privacy issues [55, 69]. These strategies include using multiple accounts [57], censoring disclosure content [17], and removing unwanted contacts [47]. The adoption of privacy management strategies constitutes an important portion of users' privacy protection behavior and has received growing attention in recent research.

Moreover, several studies have shown that in addition to the strategies mentioned above, which are about individual efforts, certain privacy management strategies involve collective efforts [6, 18, 22, 23]. For example, Facebook users sometimes work together to protect each other's private information in uploaded and tagged photos [6]. Such strategies are necessary because in the interpersonal interactions on SNSs, information is shared interpersonally and once shared, it becomes co-owned and co-managed content [40]. Thus, to systematically consider both individual and collective of privacy management strategies, researchers have developed multi-dimensional measurement scales to quantify these privacy management strategies. For instance, Cho and Filippova proposed four dimensions of collaborative, corrective, preventive, and information control strategies to account for multiple strategies that users implement to individually (e.g., untagging) and collectively (e.g., developing shared rules and norms) manage co-owned content [11].

However, whereas the antecedents of privacy behaviors have been studied in a general sense, few studies have investigated the *psychological antecedents* that predict users' adoption of these collective privacy management strategies. Many prior studies have examined the psychological antecedents of individual privacy management strategies, such as privacy concern [10, 18, 30], risk belief [10], and self-efficacy [10]. The antecedents of collective privacy management strategies remain unexplored. Examining antecedents of different collective strategies is of great importance as it will improve our understanding of what motivates users to choose these strategies in their online privacy management on SNSs. This can in turn inform future privacy design strategies for SNS providers to enhance support that can facilitate users to apply their desired strategies.

Furthermore, there is still a lack of cross-country research on users' adoption of collective privacy management strategies and its antecedents. As SNSs are increasingly popular worldwide, users from different countries may have different privacy norms and values, which in turn result in differences in people's adoption of collective privacy management strategies and the drivers to said adoption. Hence, a cross-country comparison on SNS users' adoption of collective privacy management strategies and its antecedents is needed to examine what aspects of this phenomenon are robust and what aspects significantly differ from a cross-country perspective. Such insights will inform future global and country-specific privacy design strategies and allow multinational

SNS providers like Facebook to cater differently to the privacy management strategies that prevail in different countries.

Thus, in this paper, we aim to answer following research questions:

RQ1: What psychological factors can predict the adoption of collective privacy management strategies?

RQ2: Does the prediction model differ across different countries?

We conduct an online survey with 1393 users from the US, Singapore and South Korea to examine how different antecedents affect the adoption of collective privacy management strategies. In the survey, we measure a set of collective privacy management strategies and psychological antecedents, such as privacy concerns, social norms and behavioral control. We first build a structural model on the US sample to examine hypothesized effects of psychological antecedents on the adoption of privacy management strategies. We then run the same model in Singapore and South Korea to check whether the resulting model similarly applies in different countries. We discuss the possible reasons for discrepancies in cross-country findings and how these can inform future global SNS privacy design strategies.

2 Literature Review and Theory Development

2.1 Collective Privacy Management Strategies in SNS

Previous work has shown that SNS users heavily apply coping strategies to manage their privacy in addition to configuring the embedded privacy settings on SNSs [55, 67]. For example, users send private messages instead of posting publicly or exclude personal information from their posts [67]. Some users segregate different circles of friends [25], or ignore unwanted contacts to maintain their interpersonal boundary [67]. Research has shown that users' privacy concern [10, 18, 30], risk belief [10], and self-efficacy [10] have significant influence on the adoption of individual privacy management strategies.

While these studies have focused on privacy management strategies at the individual level, recent studies have examined collective privacy management strategies [6, 18, 22, 23]. These works are mostly built on Altman's Boundary Regulation theory [3] and Petronio's Communication Privacy Management theory (CPM) [40], postulating that privacy is an interpersonal process that requires

collective efforts between users. Altman defined privacy as "an interpersonal boundary-control process to make ourselves open or close to others, which is dialectic, dynamic and bidirectional" [3]. This bi-directional process involves the regulation of not only the output to others but the input from others. This is particularly true for SNS use, as information disclosure on SNSs is not strictly personal but involves other individuals. CPM extends Altman's theory by recognizing the interpersonal boundary regulation process as a boundary coordination between the owner (the person who shares the information) and the co-owner (the person who receives the information) of the information sharing. Once information is shared, it moves to a shared domain where all the stakeholders can co-manage it. To help maintain each other's desired level of privacy, both owners and co-owners must collectively develop and negotiate privacy norms to coordinate the interpersonal boundary. When such coordination fails (i.e., rules and norms are not mutually understood or there is conflict around each other's privacy expectations), boundary turbulence happens, which can raise privacy concerns and drive the owners and co-owners of the information to restore the coordination. These collective efforts can happen frequently in the process of sharing information on SNSs. One example is that when users tweet personal information to their Twitter audience, the audience becomes the co-owner and can retweet it to another circle of audience. Another more complex example is group photo sharing: When users share group photos of themselves and their friends, their friends become the co-owners of the group photos and can be tagged [46, 68]. In this process, the co-owners' identities, images, behaviors, and locations are potentially exposed. Thus, co-owners take part in the collective coordination of the privacy boundaries to keep each other's personal information safe and private [29].

Research has uncovered a set of coping strategies that users frequently adopt in collective privacy management on SNSs. For example, users either rely on offline social interaction to handle unwanted photos, such as asking their friends to remove the photos [6], or negotiate rules of thumb on what content can be disclosed and collectively define the appropriate audience [18]. More broadly, Cho and Filippova [11] suggest four dimensions that systematically measure the main collective privacy management strategies in SNSs: collaborative strategies, corrective strategies, preventive strategies, and information control. *Collaborative strategies* involve the explicit coordination with SNS friends to collaboratively manage each other's privacy, such as discussing the appropriateness of the shared content. *Corrective strategies* comprise the use of existing privacy management features such as untagging, timeline review, or removing content. *Preventive*

strategies prevent personal information leakage by constraining the audience in advance, such as creating sharing groups and using friend lists. *Information control strategies* concern self-censoring, i.e., deciding whether content is appropriate for sharing. These strategies cover various aspects of collective privacy management that extend beyond the use of the privacy settings that are typically available on SNS platforms.

Several studies have proposed privacy designs to support these collective privacy management strategies. One study designs a Facebook application to facilitate collective management of shared data that allows the owner to make an appropriate sharing decision based on the privacy preferences specified by the co-owners [21]. Another study designs a tool called CoPE that notifies the users when they have been tagged in a photo, and allows them to request and control access over the tagged photo [50]. While these studies address the implementation of collective privacy management strategies in the use of SNSs, little research has been done to investigate the antecedents of these strategies. Discovering what antecedents influence the use of collective privacy management is important for privacy scholars to understand the mechanisms behind users' adoption of collective strategies. It can also inform the design of privacy mechanisms in SNSs that support users' collective privacy practices. Hence, the present study will investigate the antecedents of collective privacy management strategies. Given that the antecedents of individual privacy management strategies have been examined in prior studies [10, 18, 30], we will focus on the collective privacy management strategies in the present paper. We apply Cho and Filippova's four categories of collective privacy management strategies [11] in our study as these four categories comprehensively describe different aspects and focus in collective privacy management. In the next section, we will review antecedents of privacy behavior and propose the hypotheses that we aim to test.

2.2 Antecedents of Privacy Behavior

There has been a rich body of research investigating the factors that predict privacy behavior in SNS use, namely Internet skill, demographic differences, attitudinal factors, norms, and network size [18, 32, 33, 48, 73]. Inspired by the Theory of Planned Behavior (TPB) [2], we focus our study on three types of psychological antecedents to answer our research question: attitudes, norms, and perceived behavioral control. TPB is one of the most widely used theories for explaining and predicting human behavior across various domains. It postulates that human behavior is directly

influenced by behavioral intention, and behavioral intention is jointly determined by attitude, subjective norms, and perceived behavioral control towards the behavior [2]. We thus adapted the TPB antecedents to the context of SNS privacy: privacy concern (attitude), social and descriptive norm of information disclosure (norms), and perceived privacy self/collective efficacy (behavioral control).

2.2.1 Privacy Concern

In privacy research, privacy concern is widely used as a measurable proxy for users' attitudes, beliefs and perceptions towards information privacy [48, 70]. Privacy concern is generally regarded as an important predictor of privacy-related behavior [34, 56]. Researchers have shown that privacy concern negatively affects intention to disclose [34, 37], and positively affects the adoption of privacy management strategies [11, 18] as well as privacy-protective behavior [24]. Therefore, privacy concern may increase the adoption of collective privacy management strategies:

H1: Privacy concern positively influences the adoption of (a) collaborative, (b) corrective, (c) preventive, and (d) information control strategies.

2.2.2 Social norms

Researchers have separated two types of normative beliefs: subjective norms (a person's perception of what important others think the person should do) and descriptive norms (a person's perception of what others do) [14]. The more positive a person's perceived social norms about a behavior are, the more likely this person intends to perform that behavior [2]. Most studies agree that social norms of information sharing positively influence disclosure behavior on SNSs [9, 39]. Likewise, privacy social norms (about protecting personal information) negatively influence self-disclosure [36], and positively affect one's disposition to value privacy [70].

Based on these previous findings, we propose that subjective norms and descriptive norms influence the adoption of collective privacy management strategies. In our study, the social norms cover personal information disclosure in SNS use. We argue that social norms about personal information disclosure in SNS are more perceivable, salient and observable than norms about other privacy behaviors, as users can easily perceive how their SNS friends disclose. If users perceive that their SNS friends disclose personal information (i.e., descriptive norms) and that these friends expect them to do the same (i.e., subjective norms), then the perceived prevalence and social

pressures may motivate them to employ fewer privacy management strategies, as they may not want to restrict information that their SNS friends find important:

H2: Subjective norms of information disclosure negatively influence the adoption of (a) collaborative, (b) corrective, (c) preventive, and (d) information control strategies.

H3: Descriptive norms of information disclosure negatively influence the adoption of (a) collaborative, (b) corrective, (c) preventive, and (d) information control strategies.

2.2.3 Self/Collective Efficacy

Bandura's concept of perceived self-efficacy is about "the judgments of how well one can execute courses of action required to deal with prospective situations" [5]. Self-efficacy beliefs can influence choice of activities, preparation for an activity, effort expended during performance, as well as thought patterns and emotional reactions [5]. In privacy research, self-efficacy in privacy management is found to have a significant positive impact on the use of privacy enhancing technologies [10, 35]. Thus, we propose that users who believe they can manage their personal information well will be more likely to adopt collective privacy management strategies:

H4: Privacy self-efficacy positively influence the adoption of (a) collaborative, (b) corrective, (c) preventive, and (d) information control strategies.

As we reviewed earlier, SNS users manage their information privacy collectively rather than in isolation. Thus, we use perceived *collective* efficacy in addition to perceived self-efficacy. Collective efficacy is defined as one's perception concerning a group's capability to perform a behavior [19]. When people operate collectively within an interactive social system, they judge the capability of the social system as a whole. Collective efficacy has been studied in collaborative environments such as computer-supported collaborative learning [63], neighborhoods [45] and schools [20]. While few studies examine the relationship between collective efficacy and information privacy, a recent study [11] found that one's perceived privacy collective efficacy, i.e. one's personal beliefs of joint capability of a social group to perform privacy management, positively influences collective privacy management strategies. Therefore, we propose:

H5: Privacy collective efficacy positively influences the adoption of (a) collaborative, (b) corrective, (c) preventive, and (d) information control strategies.

2.3 Mediation Role of Privacy Concern

Previous research has found that privacy concern is influenced by many psychological factors [48]. For example, previous literature suggests that users' privacy attitudes are often influenced by the norms concerning information disclosure within online communities [37]. It is possible that when users feel that people are concerned with privacy and expect users to be concerned as well, their privacy concerns will be influenced due to the social influence. Therefore, we propose that:

H6: Subjective norms of information disclosure negatively influence privacy concern.

H7: Descriptive norms of information disclosure negatively influence privacy concern.

Similarly, privacy self-efficacy is shown to influence information privacy concerns [35]. Studies have found a negative effect of self-efficacy on privacy concerns [31, 58, 71]. Efficacy beliefs have the potential to regulate emotions and perceptions [4]. Specifically, those with a high level of efficacy are expected to focus more on positive aspects of a situation while those with low efficacy beliefs tend to construe the situation negatively [7]. Numerous studies have shown that efficacy beliefs reduce negative feelings under various contexts such as anxiety, fear, worry and depressive feelings [16]. Similarly, computer self-efficacy reduces computer anxiety and anger [65]. Overall, confidence combined with perceived control is predicted to reduce possible negative reactions related to privacy risks. Thus, we propose that:

H8: Privacy self-efficacy negatively influences privacy concerns.

Although no previous work has studied the influence of privacy collective efficacy on users' privacy concerns in SNS use, we predict that if users perceive that they and their friends are capable to manage their personal information, they will have fewer privacy concerns, as they will feel capable to coordinate their efforts to protect each other's personal information within their social group:

H9: Privacy collective efficacy negatively influences privacy concerns.

By postulating these direct effects of social norms and behavioral control on privacy concerns in H6-H9, we make privacy concerns as a mediator between social norms / behavioral control and privacy management strategies. Although this does not strictly follow the TPB model, we believe that the mediation is necessary. First, there are significant associations between attitude and social norms / behavioral control [2]. These three psychological antecedents are not independent from each other, but indeed interplay with each other. Second, as we reviewed, a number of privacy

studies have empirically tested the relationship between social norms / behavioral control and privacy concerns [31, 37, 58, 71], which can serve as the theoretical foundation for the mediation. Third, adding mediation can better uncover the mechanisms how TPB antecedents influence privacy management strategies. The hypothesized research model to answer our research question is presented in Figure 1.

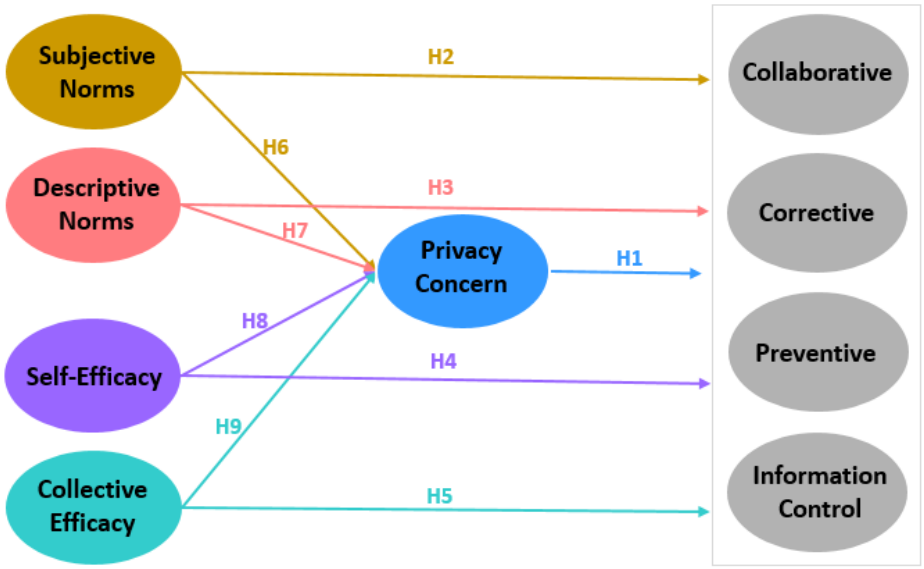

Figure 1: Hypothesized research model

2.4 Differences between Countries

A large number of studies has investigated the cross-country differences in privacy attitudes and behaviors. Most of these studies have for example found that users in individualistic countries have higher levels of privacy concerns than in collectivistic countries, and are thus less likely to disclose personal information and more likely to adopt privacy management behaviors [17, 42, 45, 46, 65]. In SNS use, people in collectivistic countries are more likely to disclose personal information to others [55], limit SNS friends to close ties in ingroups [18], and have a higher level of intimate self-disclosure [18]; users in individualistic countries are more likely to be concerned with their privacy [76], have a variety of social relationships in SNSs [18], and are more likely to adopt privacy protection behaviors [94]. One study discusses the country difference in *collaborative* privacy management [34]. They find that users in collectivistic countries are more likely to perceive the susceptibility of others to personal information exposure as a result of their own Facebook activity.

However, most previous cross-country privacy literature focuses on individual privacy practice. It is still unexplored whether users in different countries would adopt collective privacy management strategies similarly. We will explore this aspect by testing our research model laid out in H1-H9 across three countries: the US, Singapore, and Korea (RQ2).

3 Method

We ran an online survey to collect data. We chose Facebook as the context of the survey because it is one of the most popular SNSs worldwide. The survey was administered by a professional online research company, Qualtrics. Participants were randomly selected from an online panel recruited by Qualtrics. The panel is an opt-in, privacy-protected participant pool. The research company runs regular benchmarking surveys to ensure their panelists are representative of the larger Internet population. Qualtrics helped us recruit survey respondents from three countries: Singapore, South Korea, and the US. This is to test whether the research model can be applied to different countries. These three countries are economically developed and have well-established ICT infrastructures. However, they have different cultures as Singapore and South Korea are more collectivistic than the US. We restricted sampled participants to Facebook users who were older than 18 in South Korea and the US, and 21 in Singapore[1], and to those who visited their Facebook page at least once every two weeks. We translated the survey into Korean using back-translation to ensure the semantic consistency between the two versions. A total of 1393 respondents (US: 454, Singapore: 467, and South Korea: 472) participated in the survey. The percentage of female was 51.32% in the US, 50.54% in Singapore, and 50.42% in South Korea. The mean age was 41.99 (SD = 14.02) in the US, 38.72 (SD = 11.66) in Singapore, and 35.53 (SD = 11.66) in South Korea.

3.1 Measures

The variables in our study were measured by pre-validated scales adapted from previous research. All the measures used a 7-point Likert scale. Table 1 reports the items employed in this study and the validity and reliability of the measures in terms of factor loadings and average variance explained (AVE).

Construct	Items		Item Means (SD)

[1] The IRB in Singapore requires participants to be at least 21 years old.

		Factor Loading	US	SG	KR
Privacy concerns of disclosing personal information on Facebook AVE = 0.713	When using Facebook, I sometime think twice before providing my personal information	0.742	5.428(1.5)	5.530(1.2)	5.114(1.2)
	I am concerned about posting information on Facebook because it might be used in ways I had not foreseen	0.831	5.048(1.6)	5.464(1.1)	5.006(1.3)
	I am concerned that Facebook is collecting too much personal information about me	0.854	4.964(1.7)	5.199(1.2)	4.681(1.3)
	I am concerned that personal information collected by Facebook is readily available to people unauthorized to view or work with the data	0.887	5.006(1.6)	5.313(1.2)	4.675(1.3)
	I am concerned that others share too much information about me via Facebook	0.838	4.307(1.9)	5.012(1.3)	4.512(1.3)
	I am concerned that other persons could misuse the information I post on Facebook	0.874	4.717(1.8)	5.289(1.2)	4.813(1.3)
	In general, I am concerned about privacy while I am using Facebook	0.877	4.837(1.7)	5.452(1.2)	4.855(1.3)
Privacy self-efficacy AVE = 0.735	It's easy to figure out how to manage personal information on Facebook	0.716	4.813(1.5)	4.753(1.3)	4.000(1.4)
	I am confident that I know how to protect privacy on Facebook.	0.917	4.645(1.6)	4.910(1.3)	3.506(1.3)
	I feel confident adjusting the privacy settings in my Facebook account	0.911	4.976(1.5)	4.97(1.3)	3.958(1.4)
	I feel confident untagging myself from photos if I want to.	0.794	5.114(1.5)	5.084(1.3)	4.096(1.4)
	Overall, I am confident that I can protect my privacy on Facebook.	0.921	4.645(1.6)	4.873(1.4)	3.687(1.3)
	Managing personal information on Facebook is entirely within my control	0.863	4.717(1.6)	4.807(1.4)	3.783(1.4)
Privacy collective efficacy AVE = 0.737	I am confident that my friends and I can work together in order to protect privacy on Facebook	0.887	4.765(1.4)	4.572(1.3)	4.187(1.2)
	I am confident that my friends and I can effectively manage privacy since we are a competent group of people	0.896	4.813(1.4)	4.530(1.3)	3.813(1.2)
	I am confident that my friends and I are committed to protect each other's privacy	0.900	4.898(1.4)	4.614(1.3)	4.127(1.2)

	I am confident that my friends and I will do our share of the work in order to protect each other's privacy on Facebook	0.920	4.886(1.4)	4.645(1.3)	4.151(1.2)
	My friends and I look out for each other	0.868	5.410(1.3)	4.934(1.2)	4.578(1.1)
	My friends and I care for each other's privacy	0.891	5.355(1.2)	5.006(1.2)	4.873(1.1)
	My friends and I are willing to help others to protect our privacy	0.871	5.283(1.2)	4.988(1.2)	4.747(1.1)
	This is a close-knit community	0.771	4.681(1.5)	4.578(1.3)	4.241(1.2)
	People within my social network can be trusted	0.742	4.916(1.4)	4.506(1.3)	3.916(1.3)
	We generally mutually agree the same values (or rules) with regards to how to respect each other's privacy	0.824	5.066(1.3)	4.807(1.2)	4.343(1.1)
Subjective norms of sharing personal information on Facebook AVE = 0.875	People who are important to me think that I should share personal information on Facebook.	0.939	3.518(1.7)	3.476(1.4)	3.181(1.3)
	People who influence my behavior think that I should share personal information on Facebook.	0.934	3.235(1.7)	3.434(1.4)	3.151(1.4)
	People who are important to me think it would be a good idea for me to share personal information on Facebook.	0.933	3.452(1.7)	3.458(1.4)	3.199(1.3)
Descriptive norms of sharing personal information on Facebook AVE = 0.666	I believe most of the profiles I view on Facebook reveal their intimate personal information on Facebook.	0.835	4.386(1.5)	4.277(1.2)	3.765(1.2)
	Many people around me disclose intimate details about themselves on Facebook.	0.840	4.675(1.5)	4.259(1.3)	4.006(1.2)
	Many people around me disclose their personal feelings, emotions, and experiences on Facebook	0.772	4.940(1.5)	4.705(1.3)	4.657(1.2)
Privacy management strategies: Collaborative AVE = 0.786	My friends and I negotiate "rules of thumb" about sharing content concerning ourselves	0.920	3.861(1.9)	3.693(1.5)	3.747(1.5)
	My friends and I agree on "rules of thumb" about sharing content concerning ourselves	0.910	4.012(1.8)	3.807(1.5)	3.976(1.5)
	Prior to disclosing content, my friends and I discuss the appropriate privacy settings	0.895	3.620(1.9)	3.729(1.6)	3.861(1.5)
	I ask for approval before disclosing content from those involved	0.851	4.090(1.9)	4.157(1.6)	3.916(1.5)

	My friends ask for approval before uploading content concerning myself	0.881	3.741(1.9)	3.825(1.6)	3.675(1.5)
	I discuss the appropriate privacy settings with my friends before creating a Facebook group	0.905	3.777(1.9)	3.801(1.6)	3.711(1.5)
	I educate my friends about privacy issues	0.841	3.849(1.9)	3.916(1.6)	3.542(1.5)
Corrective AVE = 0.818	I untag myself from photos my friends uploaded	0.864	3.259(1.8)	3.349(1.6)	2.506(2.7)
	I ask friends to remove content concerning myself	0.918	3.054(1.7)	3.042(1.4)	2.325(2.9)
	I delete content posted about me by my friends	0.922	3.030(1.7)	2.910(1.3)	2.259(2.9)
	My friends untag themselves from photos I uploaded	0.898	2.867(1.7)	2.783(1.2)	2.145(2.9)
	My friends ask me to remove content concerning themselves	0.898	2.633(1.6)	2.711(1.3)	2.133(2.9)
	I advise my friends to remove content concerning themselves	0.914	2.904(1.7)	2.729(1.4)	2.223(2.9)
	I advise my friends to untag themselves from photos others uploaded	0.916	2.831(1.7)	2.705(1.3)	2.139(2.9)
Preventive AVE = 0.528	I make use of friend lists to restrict the audience of my posts to certain individuals	0.697	5.801(1.8)	5.705(1.5)	4.958(1.7)
	I use secret groups to share content about my friends	0.736	5.313(1.9)	5.434(1.7)	5.199(1.6)
	I allow my Facebook friends to view only the mutual friends they share with me	0.718	5.861(1.9)	5.825(1.5)	5.380(1.6)
	I use the timeline review function to control what information appears on my timeline	0.754	4.590(1.9)	4.867(1.6)	4.361(1.6)
Information control AVE = 0.713	Before posting on Facebook, I consider the audience that will read my post	0.872	3.054(1.3)	3.717(1.2)	3.289(1.3)
	I adjust the content of my post based on who I think will see it	0.867	4.217(1.6)	4.693(1.3)	4.145(1.4)
	I limit what I share on Facebook to only what is appropriate for all of my friends to see	0.791	4.235(1.3)	4.729(1.2)	3.952(1.2)

Table 1: Factors, items, factor loadings, and item means.

We measured participants' self-reported adoption of four different privacy management strategies: *collaborative strategies*, *corrective strategies*, *preventive strategies* and *information control strategies* [11]. The collaborative and corrective strategies is each measured with 7 items, preventive strategies with 4 items, and information control strategies with 3 items.

We also measured privacy concerns, subjective norms and descriptive norms about personal information sharing, and privacy self-efficacy and privacy collective efficacy. *Privacy concern* is measured by 8 items from CFIP [49], and adapted to the domain of Facebook use. *Subjective norms* and *descriptive norms* are each measured using 3-item scales adapted from [15, 59]. *Privacy self-efficacy* is measured by 6 items adapted from [28]. *Privacy collective-efficacy* describes one's perception about the capability of oneself and one's friends to successfully protect privacy together. We used 10 items adapted from [45] to measure it.

3.2 Data Analysis

We used Mplus to test our models. We first subjected the items to a Confirmatory Factor Analysis (CFA) to check the measurement validity. The CFA measurement model establishes relationships between indicators and latent factors. By the use of CFA, the items for each construct are modelled as linear combinations of the latent factors. All items are ordinal, and hence we used the robust weighted least squares estimator (WLSMV), as it does not assume normally distributed variables and provides a better option for modelling categorical or ordered data. We checked the factor loadings, R-square, AVE and modification indices for measurement validity. Convergent validity is supported when indicators load significantly on their respective factors (standardized factor loadings exceed 0.6) and the AVE is higher than 0.5. Discriminant validity is supported when the correlation between latent factors is lower than .85, and smaller than the square root of the AVE of each factor. We also checked the measurement invariance across the three countries by comparing configural, metric and scalar measurement models. If a metric or scalar model is not significantly worse than a configural model in terms of model fit, we can claim that we have metric invariance for comparing path coefficients across groups, or scalar invariance for comparing means. If any non-invariance exists, checking the factor loadings with large modification indices will help us locate the source of non-invariance.

We then subjected the factors in the US sample to Structural Equation Modeling (SEM) as shown in Figure 1. We aimed to test whether the hypothesized research model fits the US sample. SEM simultaneously fits the measurement model and a series of linear regressions between factors. We added residual correlations among subjective norms, descriptive norms, privacy self-efficacy, and privacy collective efficacy.

Finally, in order to check the robustness of the research model in different countries, we fit the model in the Singapore and Korean samples respectively. To find where the models differ between the three countries, we used multiple group SEM. The grouping variable is country. First, we fit identical models for each country (with intercepts and path coefficients being the same). Second, we fit the same model for each country, but allowed one path, i.e. from subjective norms to collaborative strategies, to be free (namely different among the three countries), while the other estimations were identical. Third, we compared the models in Step 1 and 2 through a Wald test to see if freeing the path significantly improved the model fit. We performed this 3-step process for all the paths one by one to identify the path coefficient(s) that significantly differ between the three countries.

4 Results

4.1 Measurement Model

The results from CFA on the US sample show that the measurement model has acceptable fit indices (χ^2= 10931.782, df = 1139, p<.001; RMSEA = 0.079 < 0.08, 90% CI: [0.077, 0.080], CFI = 0.942 > 0.9, TLI = 0.938 > 0.9). A chi-square test with a p-value greater than 0.05 usually indicates a good model fit. However, it is sensitive to sample size. We thus use other criteria, such as RMSEA, CFI, and TLI together to describe the goodness-of-fit of our model. All standardized factor loadings are above the recommended 0.6 level (Table 1). Each latent variable's AVE is greater than 0.5, indicating adequate convergent validity (Table 1). The square root of each latent variable's AVE is greater than its correlations with other latent variables, indicating adequate discriminant validity (Table 2).

Concern	0.844								
Self-eff.	–0.038	0.857							
Coll. eff.	0.052	**0.605**	0.858						
Subj. norm	0.000	**0.285**	**0.294**	0.935					
Desc. norm	**0.210**	**0.344**	**0.307**	**0.421**	0.816				
Collab.	**0.283**	**0.275**	**0.457**	**0.350**	**0.212**	0.887			
Corrective	**0.277**	0.081	0.029	**0.312**	**0.137**	**0.428**	0.904		
Preventive	**0.488**	**0.311**	**0.313**	**0.268**	**0.248**	**0.665**	**0.488**	0.727	
Info. ctrl.	**0.473**	**0.312**	**0.382**	0.003	**0.286**	**0.322**	0.050	**0.491**	0.844
	Concern	Self-eff.	Coll. eff.	Subj. norm	Desc. norm	Collab.	Corrective	Preventive	Info. Ctrl.

Table 2: Factor correlations
($p < .001$ marked in bold; the diagonal shows the square root of the AVEs)

The measurement invariance test was conducted to ensure that the same constructs are being measured across the three countries. In the measurement invariance test, four strategies and other latent factors achieve partial metric invariance. We freed the factor loadings of 5 non-invariant items, as invariance in up to 20% of parameters is acceptable when conducting multiple group comparisons [52]. Our measurement model is "partially metric invariant," and can thus be used for comparing path coefficients between countries. We summarize the descriptive statistics of our constructs in Table A in Appendix to show an overall comparison of the factors among the three countries, in which the US sample is the baseline. The comparison shows that significant differences exist in each factor across countries. The country differences in privacy self-efficacy, collective efficacy and information control are consistent with prior studies. The country difference in privacy concern is somehow different from prior work, as participants in Singapore, a collectivistic country, have higher privacy concerns than in US.

4.2 Antecedents of Privacy Management Strategies (RQ1)

We fit a structural model on the US sample. The model has a good model fit: $\chi 2 = 4686.721$, df = 1139, $p<.001$; RMSEA = 0.083, 90% CI: [0.080, 0.085], CFI = 0.945, TLI = 0.941. In Figure 2, we report the path coefficients and their significance.

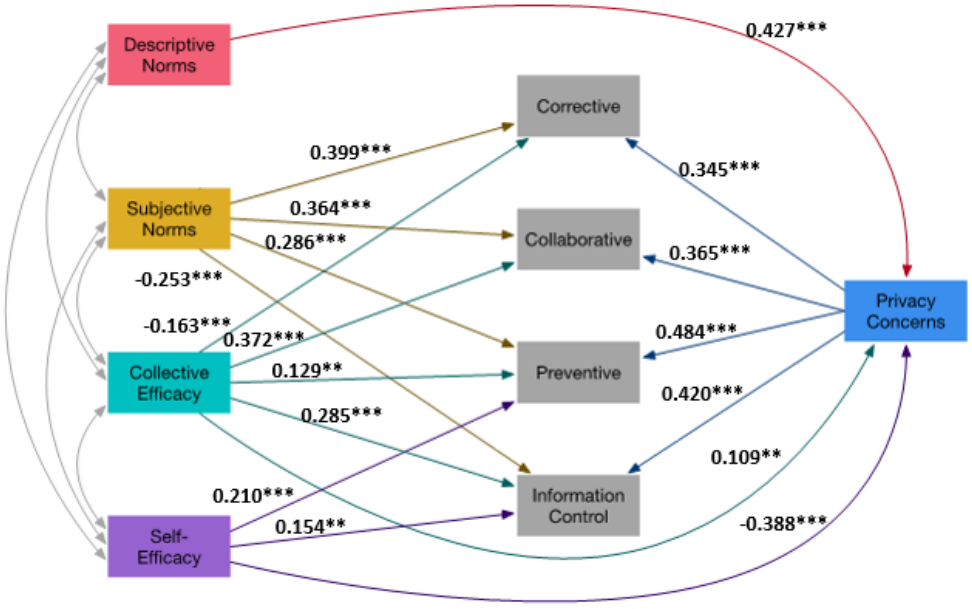

Figure 2: Path coefficients of the US SEM model (*p <.05, ** <.01, *** <.001).

4.2.1 Privacy concern → Privacy management strategies

The model shows that privacy concerns positively influence the adoption of collaborative (H1a), corrective (H1b), preventive (H1c), and information control (H1d) strategies. Hence, **H1a-Hd are supported.**

4.2.2 Social norms → Privacy management strategies

The direct effects of subjective norms on information control strategies (H2d) are negative as expected, but they are positive on collaborative (H2a), corrective (H2b), and preventive strategies (H2c). In other words, Facebook users who believe that their SNS friends expect them to disclose their personal information on SNS are less likely to control shared content, but more likely to coordinate with SNS friends to manage privacy, correct information about them that is inappropriately disclosed, and prevent personal information leakage. Thus, **H2d is supported, but H2a, H2b, and H2c are not supported.** Descriptive norms do not significantly influence the adoption of privacy management strategies directly. **Thus, H3 is not supported.**

4.2.3 Behavioral control → Privacy management strategies

Privacy self-efficacy directly increases users' adoption of preventive (H4c) and information control (H4d) strategies. There is however no effect of privacy self-efficacy on collaborative (H4a) and corrective (H4b) strategies. **H4c and H4d are supported, but H4a and H4b are not supported**.

Privacy collective efficacy positively influences the adoption of collaborative (H5a), preventive (H5c) and information control (H5d) strategies, but negatively influences corrective strategies (H5b). **Thus, H5a, H5c and H5d are supported, but H5b is not supported.**

4.2.4 Mediated Effects Through Privacy Concern

The effects of subjective norms on privacy management strategies are not mediated through privacy concerns, as they do not significantly predict privacy concerns. **H6 is not supported.**

Effects of descriptive norms are fully mediated through privacy concerns. Contrary to our expectations, though, the effect of descriptive norms on privacy concerns is positive: when users perceive that their SNS friends disclose personal information in SNS, their privacy concerns increase. **The result for H7 is contrary to what we hypothesized**. Mediated by privacy concerns, total effects of descriptive norms are positive on the adoption of privacy management strategies.

The effects of privacy self-efficacy on the adoption of privacy management strategies are partially mediated by privacy concerns, as privacy self-efficacy has a negative effect on privacy concerns. Users' perceived capability in managing privacy will lower their privacy concerns in SNS use (**H8 is supported**), and in turn their use of privacy management strategies. Note that this mediation counters—but does not completely offset—the direct effect of privacy self-efficacy (H4) that increases the adoption of preventive and information control strategies: the total effects of privacy self-efficacy on preventive and information control strategies are positive. However, due to the absence of a direct effect on collaborative and corrective strategies, the total effects of privacy self-efficacy on these strategies are negative.

The effects of perceived collective efficacy on the adoption of privacy management strategies are also partially mediated by privacy concerns. Note though that collective efficacy has a *positive* influence on privacy concerns. **H9 is contrary to our hypothesis**. When users believe that they and their SNS friends can manage privacy in SNS use, their privacy concerns will increase. Note that for corrective strategies, this effect counters—but does not completely offset—the negative direct effect of collective efficacy (H8b) that decreases the adoption of corrective strategies. For the other strategies, the mediation via privacy concerns reinforces the positive direct effect of collective efficacy.

4.3 Model Robustness in Different Countries

We ran the same structural model on the Singapore and Korean samples and used multiple-group analysis to locate the significant differences between countries. In Table 3, we report the path coefficients and their significance in the three countries. We highlight the significant differences between countries in bold.

IV	DV				
	Privacy Concerns	**Collaborative**	**Corrective**	**Preventive**	**Information Control**
Privacy Concerns		US: 0.346*** SG: 0.182*** KR: 0.251***	US: 0.304*** SG: 0.167*** KR: 0.281***	US: 0.400*** SG: 0.406*** KR: 0.466***	US: 0.532*** SG: 0.556*** KR: 0.598***
Subjective Norms	**US: 0.093*** **SG: –0.222*** **KR: –0.084****	**US: 0.314*** **SG: 0.143*** **KR: 0.114***	US: 0.349*** SG: 0.215*** KR: 0.244***	US: 0.196*** SG: 0.047 KR: 0.150***	**US: –0.186*** **SG: –0.122*** **KR: –0.016**
Descriptive Norms	**US: 0.384*** **SG: 0.210*** **KR: 0.003**	n.s.	n.s.	n.s.	n.s.
Self-Efficacy	**US: –0.350***	n.s.	n.s.	US: 0.140***	US: 0.187***

	SG: –0.091** **KR: –0.121****			SG: 0.217*** KR: 0.116***	SG: 0.184*** KR: 0.207***
Collective Efficacy	US: 0.091** SG: 0.175*** KR: 0.091**	US: 0.382*** SG: 0.368*** KR: 0.377***	US: –0.097*** SG: –0.102*** KR: –0.112***	US: 0.110 SG: 0.068 KR: 0.163***	US: 0.270*** SG: 0.209*** KR: 0.224***

Table 3: Path coefficients of the SEM model. Bold effects are significantly moderated by country (*p <.05, ** <.01, *** <.001).

4.3.1 Privacy concern → Privacy management strategies

The effects of privacy concerns on privacy management strategies are similar in Singapore and Korea as in the US. Privacy concerns significantly increase the adoption of the four privacy management strategies in three countries.

4.3.2 Social norms → Privacy management strategies/Privacy concerns

Subjective norms have similar effects on corrective and preventive strategies in Singapore and Korea as in the US. However, the effects on other strategies are different across three countries. The effect of subjective norms on collaborative strategies is much stronger in the US than in Singapore and Korea ($\Delta\chi^2(2) = 21.8$, $p<.01$). The effect on information control strategies is positive in Korea, but negative in the US and Singapore ($\Delta\chi^2(2) = 8.2$, $p=.01$). Subjective norms do not significantly influence privacy concerns in the US, but do reduce them in Korea and Singapore ($\Delta\chi^2(2) = 43.9$, $p<.01$). This means that when users believe that their Facebook friends expect them to disclose their personal information, their privacy concerns will decrease in Singapore and Korea, but less likely change in the US.

The effects of descriptive norms on privacy strategies are similarly non-significant in the three countries. However, descriptive norms significantly increase privacy concerns in the US and Singapore, but do not significantly influence in Korea ($\Delta\chi^2(2) = 35.6$, $p<.01$).

4.3.3 Behavioral control → Privacy management strategies/Privacy concerns

The effects of self-efficacy on strategies do not vary significant across three countries. However, the effect of self-efficacy on privacy concerns is much stronger in the US than in Korea and Singapore ($\Delta\chi^2(2) = 9.1$, $p=.01$). The effects of collective efficacy do not vary significant across three countries.

In sum, the resulting models suggest that the effects of certain antecedents on privacy management strategies differ significantly across the US, Korea and Singapore, while other paths hold true across these countries.

The results are summarized in Table 4.

#	Hypotheses	Results	Significantly different across countries?
H1	Privacy concern -> strategies.	Supported	Not different
H2	Subjective norms -> strategies	Partially supported	Partially different
H3	Descriptive norms -> strategies	Not supported	Not different
H4	Privacy self-efficacy -> strategies	Partially supported	Not different
H5	Privacy collective efficacy -> strategies	Partially supported	Not different
H6	Subjective norms -> privacy concern	Not supported	Different
H7	Descriptive norms -> privacy concern	Not supported	Different
H8	Privacy self-efficacy -> privacy concern	Partially supported	Different
H9	Privacy collective efficacy -> privacy concern	Not supported	Not different

Table 4: Summary of the hypothesis testing results.

5 Discussion

The purpose of this study is to examine the psychological antecedents that can predict multiple aspects of privacy management strategies. We conducted a survey in the US, Korea and Singapore to gauge the relationships between the psychological antecedents and privacy management strategies. The resulting model based on TPB shows that privacy concern, social norms and efficacy perceptions directly and indirectly influence the adoption of different privacy management strategies. Additionally, we found that the effects of certain antecedents differ between different countries. Thus, we cannot assume that the prediction model tested in one country would also hold in another country.

5.1 Predicting the Adoption of Privacy Management Strategies

Our first contribution is that we examine the psychological antecedents of multiple dimensions of collective privacy management strategies. Previous studies mostly focus on individual practices [32, 43]. We find that the effects of antecedents on different types of strategies are not uniform. For example, subjective norms increase the adoption of collaborative, corrective, and preventive

strategies, but decrease the adoption of information control. In other words, when users perceive that their friends expect them to share personal information on Facebook, they are less likely to limit their information disclosure but at the same time *more* likely to adopt other privacy management strategies. Arguably, this demonstrates how users compensate for increased disclosure about themselves to meet social norms by relying on other strategies to protect their privacy.

Another example is that effects of perceived behavioral control (operationalized as efficacy beliefs in our study) are different under different types of privacy management strategies. The total effects of self-efficacy increase the adoption of preventive and information control strategies, but decrease the adoption of collaborative and corrective strategies, whereas perceived collective efficacy increases the adoption of collaborative, preventive and information control strategies, but decreases the adoption of corrective strategies. These findings suggest that group efficacy, rather than self-efficacy, is a driver for users to collaboratively manage privacy. Likewise, users have to be confident about both themselves and their SNS friends in order to adopt strategies related to prevention and control. But an increase in perceived self-efficacy and collective efficacy reduces users' need to adopt strategies related to the correction of disclosure, perhaps because their confidence in their own and their friends' ability to engage in effective privacy management makes them less likely to regret and remove content.

Our second contribution is a finer-grained elaboration of the mechanisms through which psychological antecedents influence privacy management strategies. We examine the sub-categories of privacy antecedents, specifically social norms and perceived behavioral control, and the mediation among privacy antecedents. For example, *subjective* norms decrease privacy concerns while *descriptive* norms increase them. Perhaps when users see their friends share large amounts of personal information, experiences and feelings (i.e. descriptive norms), it is highly likely that such sharing may at times inadvertently also involve personal information, experiences and feelings of the users themselves (e.g. when being tagged or mentioned in a post), thus raising concerns about their own privacy. But when they perceive a strong expectation of disclosure (i.e. an injunctive norm) from their friends, they will probably adjust their attitudes and be less likely to worry about their privacy. Similarly, we find that *self*-efficacy decreases privacy concerns while perceived *collective* efficacy increases them. A high level of perceived behavioral control of the user's Facebook friends (i.e., collective efficacy) may be interpreted as a performance expectation

(another type of injunctive norm), thereby increasing social pressure to be concerned about privacy. Self-efficacy, on the other hand, reduces such pressure.

In sum, this study contributes to HCI privacy research by highlighting the importance of distinguishing between multiple aspects of privacy management strategies and privacy antecedents. The majority of privacy studies have focused on limited aspects of these factors [72], or lumped them together into a single construct [18]. We suggest that by taking our finer-grained approach, research should be able to specify, for instance, which aspect of social norms is related to what aspect of privacy management strategies. This can lead to a more precise understanding of the relationships between privacy antecedents and behaviors.

5.2 Cross-Country Differences in the Prediction Model

Our third contribution is an examination of whether the prediction model is robust in different countries. We observe that some effects of the psychological antecedents are consistent across countries, while others are not. One plausible reason for these differences may be the different cultures in the three countries. Culture has been shown to be an important factor affecting users' privacy attitudes and behaviors on SNSs [22, 41, 44, 62]. Researchers have found that users in individualistic countries exhibit relatively higher levels of privacy concerns than those in collectivistic countries [12, 27, 64], and are less likely to disclose personal information [13, 42, 61], while more likely to adopt privacy management behaviors [44, 53]. The US is widely regarded as an individualistic country, whereas Singapore and Korea as collectivistic countries. Subjective and descriptive norms strongly *increase* privacy concerns in the US, an individualistic country. Arguably, when these social norms of sharing contradict users' personal norms, this leads to additional concerns. In collectivistic Korea and Singapore, these social norms have a much weaker relationship with users' privacy concerns, or even *decrease* them. Social psychologists generally believe that collectivists feel more committed to the group and are more willing to internalize the social norms to act in accordance with them [60]. Collectivists regard themselves as part of the group; they are more willing to sacrifice their own privacy needs for the group, and expect other group members to do the same. Thus, collectivists internalize prevailing social norms about information sharing into their own attitudes, which makes them less concerned about their own privacy.

Similarly, the effects of subjective norms on the adoption of privacy management strategies, especially collaborative and information control, are greater in the US than in Singapore or Korea. This suggests that in individualistic countries, users will conform with the norms by exerting less control over their information, but instead adopting other strategies to meet their personal privacy needs. Conversely, the effects of social norms on privacy management strategies are weaker in collectivistic countries because employment of privacy management strategies may be perceived as counter-normative. In addition to the differences between individualistic and collectivistic countries, some effects slightly differ between the two collectivistic countries, Singapore and Korea, such as the effect of social norms and self-efficacy on privacy concerns. The effect size of social norms is larger in Singapore than in Korea. One possible reason might be that users in Singapore live in a more authoritarian society with higher surveillance. Thus, they tend to be more compliant with the norms of information sharing on social media. The effect size of self-efficacy is larger in Korea than in Singapore. While Korea and Singapore are both collectivistic countries, Korea scores higher on uncertainty avoidance than Singapore. Higher uncertainty avoidance is positively correlated with self-efficacy [1], which might be a reason why the effect of self-efficacy is stronger in Korea than in Singapore.

Our findings also show that certain effects are consistent across countries, such as the effects of privacy concerns on privacy strategies. Privacy concerns are positively associated with the employment of all available privacy management strategies regardless of culture, and the magnitude of its impact is considerable compared with other predictors. This is in line with the results of other privacy studies in SNS [11, 24, 38].

Overall, we found both variant and invariant relationships between psychological antecedents and privacy management strategies among different countries. These findings question the generalizability of a privacy research model, as well as any specific findings, that are based on a single-culture study. We argue that further research is needed to specify the country boundary conditions under which privacy-related attitudes, control beliefs and social norms perceptions can have different implications for privacy management practices. Additionally, these findings further attest to the difficulty of privacy research. Depending on which privacy constructs we focus on and/or in which country we test our model, we may get partially differing results. Specificity in terms of both conceptualization and country context should be a key consideration in future

research, when examining the complex relationships between norms, attitudes, perceived control, and privacy behavior.

5.3 Design Implications

The goal of SNS is to encourage information sharing without making users uncomfortable about the consequences for their privacy [66]. Our results identify a concrete set of factors on which SNS providers need to focus their attention and efforts to make it easier for SNS users to manage their personal information privacy. Specifically, multinational SNS providers should take users' country into account in the development of privacy management mechanisms. SNSs should provide features that support both individual and group level privacy management. In SNSs where users from different countries interact with each other, users from collectivistic countries may need some collaborative features to manage their information privacy. For instance, features that remind and support users to negotiate the privacy management with each other can be included on Facebook.

Moreover, SNS features that can enhance users' privacy self-efficacy should be sought, as they will reduce users' privacy concerns and motivate them to use more privacy management strategies, especially in individualistic societies. On the other hand, as social norms increase users' privacy concerns in individualistic societies, SNS providers should promote mechanisms that allow users to make better decisions under social norms (peer pressure) and protect their personal information. For instance, the interface of Facebook could include the popular privacy features the one's SNS contacts frequently use, which might motivate the users to raise privacy awareness and adopt privacy management strategies.

Although we did not directly evaluate inter-cultural dynamics, our results suggest that cross-country collaboration and communication via SNSs can result in *conflicting* uses of privacy management strategies. Future work should investigate the existence of such inter-cultural conflicts and explore potential solutions. An example solution could be to require employees in inter-cultural teams to undergo cultural sensitivity training with an explicit SNS focus.

5.4 Limitations

We only included three countries in our study, three US, Singapore and Korea. They may not well represent other countries. Thus, we do not know whether the prediction model applies in other countries. Second, our study relied on participants' self-reported adoption of privacy management

strategies. Researchers have argued the importance of using actual behavior in privacy studies [26], as stated behavior may differ from actual behavior [51]. However, it is not feasible for this study to collect participants' actual adoption of privacy management strategies. Collaborative strategies, for example, require coordination among SNS friends, and are thus not tied explicitly to a particular privacy setting. The use of such strategies is thus hard to capture without asking the participants to self-report. Future studies could explore ways to study these coping strategies unobtrusively in real-world situation.

Finally, our research model was inspired by TPB. We focus on the three core components in TPB to predict privacy management strategies. Our model does not include other confounders that might affect users' privacy management strategies, such as ease of use of the privacy management strategies, which might influence users' willingness to adopt. We suggest this as a future direction to examine both intrinsic and extrinsic antecedents of privacy management strategies.

However, we enhanced the traditional TPB by allowing relationships among social norms, perceived behavioral control and privacy concern, and by adding new predictors such as descriptive norms and perceived collective efficacy. Most of our adaptations were based on privacy literature, but at the expense of a closer adherence to the TPB model.

6 Conclusion

This paper examines the psychological antecedents that can predict collective privacy management strategies. It also tests whether the prediction model applies similarly to different countries, the US, Singapore and Korea. We empirically verify that privacy concern, social norms and efficacy perception influence the adoption of different privacy management strategies. Some of the antecedents' effects vary between the three countries. We highlight the importance of distinguishing between multiple aspects of privacy management strategies and privacy antecedents. We suggest that privacy research, prediction models, and privacy design should be adjusted to account for cross-country differences in privacy perceptions, attitudes, and behaviors.

7 Acknowledgment

On behalf of all authors, the corresponding author states that there is no conflict of interest.

8 References

[1] Afsar, B. and Masood, M. 2018. Transformational Leadership, Creative Self-Efficacy, Trust in Supervisor, Uncertainty Avoidance, and Innovative Work Behavior of Nurses. *The Journal of Applied Behavioral Science*. 54, 1 (Mar. 2018), 36–61. DOI:https://doi.org/10.1177/0021886317711891.

[2] Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. 50, 2 (1991), 179–211. DOI:https://doi.org/10.1016/0749-5978(91)90020-T.

[3] Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company, Monterey, California 93940 ($6.95 cloth).

[4] Bandura, A. 1997. *Self-Efficacy in Changing Societies*. Cambridge University Press.

[5] Bandura, A. 1982. Self-efficacy mechanism in human agency. *American Psychologist*. 37, 2 (1982), 122–147. DOI:https://doi.org/10.1037/0003-066X.37.2.122.

[6] Besmer, A. and Richter Lipford, H. 2010. Moving beyond untagging: photo privacy in a tagged world. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), 1563–1572.

[7] Boardley, I.D., Jackson, B. and Simmons, A. 2015. Changes in Task Self-Efficacy and Emotion Across Competitive Performances in Golf. *Journal of Sport and Exercise Psychology*. 37, 4 (Aug. 2015), 393–409. DOI:https://doi.org/10.1123/jsep.2014-0331.

[8] Boyd, D.M. and Ellison, N.B. 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*. 13, 1 (Oct. 2007), 210–230. DOI:https://doi.org/10.1111/j.1083-6101.2007.00393.x.

[9] Chang, C.-W. and Chen, G.M. 2014. College students' disclosure of location-related information on Facebook. *Computers in Human Behavior*. 35, (Jun. 2014), 33–38. DOI:https://doi.org/10.1016/j.chb.2014.02.028.

[10] Cho, H. 2010. Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self- Protection Strategies. *Journal of Information Privacy and Security*. 6, 1 (2010), 3–27.

[11] Cho, H. and Filippova, A. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. (2016).

[12] Cho, H., Rivera-Sánchez, M. and Lim, S.S. 2009. A multinational study on online privacy: global concerns and local responses. *New Media & Society*. 11, 3 (May 2009), 395–416. DOI:https://doi.org/10.1177/1461444808101618.

[13] Cho, S.E. and Park, H.W. 2013. A qualitative analysis of cross-cultural new media research: SNS use in Asia and the West. *Quality & Quantity*. 47, 4 (Jun. 2013), 2319–2330. DOI:https://doi.org/10.1007/s11135-011-9658-z.

[14] Cialdini, R.B., Reno, R.R. and Kallgren, C.A. 1990. A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*. 58, 6 (1990), 1015–1026. DOI:https://doi.org/10.1037/0022-3514.58.6.1015.

[15] Constructing a TpB questionnaire: Conceptual and methodological considerations: 2006. *http://www.uni-bielefeld.de/ikg/zick/ajzen%20construction%20a%20tpb%20questionnaire.pdf*.

[16] Cybulski, M., Cybulski, L., Krajewska-Kulak, E. and Cwalina, U. 2017. The level of emotion control, anxiety, and self-efficacy in the elderly in Bialystok, Poland. *Clinical Interventions in Aging*. 12, (Feb. 2017), 305–314. DOI:https://doi.org/10.2147/CIA.S128717.
[17] Das, S. and Kramer, A. 2013. Self-Censorship on Facebook. *ICWSM* (2013).
[18] 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, (Jun. 2014), 444–454. DOI:https://doi.org/10.1016/j.chb.2014.03.010.
[19] Earley, P.C. 1993. East Meets West Meets Mideast: Further Explorations of Collectivistic and Individualistic Work Groups. *The Academy of Management Journal*. 36, 2 (1993), 319–348. DOI:https://doi.org/10.2307/256525.
[20] Goddard, R.D. 2001. Collective efficacy: A neglected construct in the study of schools and student achievement. *Journal of Educational Psychology*. 93, 3 (2001), 467–476. DOI:https://doi.org/10.1037/0022-0663.93.3.467.
[21] Hu, H., Ahn, G.-J. and Jorgensen, J. 2011. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. *Proceedings of the 27th Annual Computer Security Applications Conference* (2011), 103–112.
[22] James, T.L., Wallace, L., Warkentin, M., Kim, B.C. and Collignon, S.E. Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*. DOI:https://doi.org/10.1016/j.im.2017.01.001.
[23] Jia, H. and Xu, H. 2016. Autonomous and Interdependent: Collaborative Privacy Management on Social Networking Sites. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), 4286–4297.
[24] Jiang, Z. (Jack), Heng, C.S. and Choi, B.C.F. 2013. Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*. 24, 3 (May 2013), 579–595. DOI:https://doi.org/10.1287/isre.1120.0441.
[25] Kelley, P.G., Brewer, R., Mayer, Y., Cranor, L.F. and Sadeh, N. 2011. An Investigation into Facebook Friend Grouping. *INTERACT*. P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, and M. Winckler, eds. Springer Heidelberg. 216–233.
[26] Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. 64, (Jan. 2017), 122–134. DOI:https://doi.org/10.1016/j.cose.2015.07.002.
[27] Krasnova, H. and Veltri, N.F. 2010. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. *2010 43rd Hawaii International Conference on System Sciences (HICSS)* (Jan. 2010), 1–10.
[28] Lampe, C., Wohn, D.Y., Vitak, J., Ellison, N.B. and Wash, R. 2011. Student use of Facebook for organizing collaborative classroom activities. *International Journal of Computer-Supported Collaborative Learning*. 6, 3 (Sep. 2011), 329–347. DOI:https://doi.org/10.1007/s11412-011-9115-y.
[29] Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. 2011. We're in it together: interpersonal management of disclosure in social network services. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011), 3217–3226.
[30] Lankton, N., McKnight, D. and Tripp, J. 2016. Privacy Management Strategies: An Exploratory Cluster Analysis. (2016).

[31] Lee, J.-M. and Rha, J.-Y. 2016. Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*. 63, (Oct. 2016), 453–462. DOI:https://doi.org/10.1016/j.chb.2016.05.056.

[32] Lewis, K., Kaufman, J. and Christakis, N. 2008. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*. 14, 1 (2008), 79–100. DOI:https://doi.org/10.1111/j.1083-6101.2008.01432.x.

[33] Litt, E. 2013. Understanding social network site users' privacy tool use. *Computers in Human Behavior*. 29, 4 (Jul. 2013), 1649–1656. DOI:https://doi.org/10.1016/j.chb.2013.01.049.

[34] Min, J. and Kim, B. 2014. How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*. (2014), n/a-n/a. DOI:https://doi.org/10.1002/asi.23206.

[35] Mohamed, N. and Ahmad, I.H. 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*. 28, 6 (Nov. 2012), 2366–2375. DOI:https://doi.org/10.1016/j.chb.2012.07.008.

[36] Nemec Zlatolas, L., Welzer, T., Heričko, M. and Hölbl, M. 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*. 45, (Apr. 2015), 158–167. DOI:https://doi.org/10.1016/j.chb.2014.12.012.

[37] Nov, O. and Wattal, S. 2009. Social computing privacy concerns: antecedents and effects. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2009), 333–336.

[38] Nov, O. and Wattal, S. 2009. Social computing privacy concerns: antecedents and effects. *Proceedings of the 27th international conference on Human factors in computing systems* (New York, NY, USA, 2009), 333–336.

[39] Pai, P. and Tsai, H.-T. 2016. Reciprocity norms and information-sharing behavior in online consumption communities: An empirical investigation of antecedents and moderators. *Information & Management*. 53, 1 (Jan. 2016), 38–52. DOI:https://doi.org/10.1016/j.im.2015.08.002.

[40] Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.

[41] 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 U.K. who use online communities. *European Journal of Information Systems*. 19, 2 (Apr. 2010), 181–195. DOI:https://doi.org/10.1057/ejis.2010.15.

[42] 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 U.K. who use online communities. *European Journal of Information Systems*. 19, 2 (Apr. 2010), 181–195. DOI:https://doi.org/10.1057/ejis.2010.15.

[43] Ridings, C.M., Gefen, D. and Arinze, B. 2002. Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems*. 11, 3–4 (Dec. 2002), 271–295. DOI:https://doi.org/10.1016/S0963-8687(02)00021-5.

[44] Rui, J. and Stefanone, M.A. 2013. Strategic Self-presentation Online: A Cross-cultural Study. *Comput. Hum. Behav.* 29, 1 (Jan. 2013), 110–118. DOI:https://doi.org/10.1016/j.chb.2012.07.022.

[45] Sampson, R.J., Raudenbush, S.W. and Earls, F. 1997. Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. *Science*. 277, 5328 (Aug. 1997), 918–924. DOI:https://doi.org/10.1126/science.277.5328.918.

[46] Shi, P., Xu, H. and Chen, Y. 2013. Using contextual integrity to examine interpersonal information boundary on social network sites. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2013), 35–38.

[47] Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J. and Cranor, L.F. 2013. The Post That Wasn'T: Exploring Self-censorship on Facebook. *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (New York, NY, USA, 2013), 793–802.

[48] Smith, H.J., Dinev, T. and Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*. 35, 4 (Dec. 2011), 989–1016.

[49] Smith, H.J., Milberg, S.J. and Burke, S.J. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*. 20, 2 (Jun. 1996), 167–196. DOI:https://doi.org/10.2307/249477.

[50] Squicciarini, A.C., Xu, H. and Zhang, X. 2011. CoPE: Enabling Collaborative Privacy Management in Online Social Networks. *Journal of the American Society for Information Science and Technology*. (2011).

[51] Staddon, J., Acquisti, A. and LeFevre, K. 2013. Self-Reported Social Network Behavior: Accuracy Predictors and Implications for the Privacy Paradox. *2013 International Conference on Social Computing (SocialCom)* (Sep. 2013), 295–302.

[52] Steenkamp, J.-B.E.M. and Baumgartner, H. 1998. Assessing Measurement Invariance in Cross-National Consumer Research. *Journal of Consumer Research*. 25, 1 (Jun. 1998), 78–90. DOI:https://doi.org/10.1086/209528.

[53] Steenkamp, J.-B.E.M. and Geyskens, I. 2006. How Country Characteristics Affect the Perceived Value of Web Sites. *Journal of Marketing*. 70, 3 (Jul. 2006), 136–150. DOI:https://doi.org/10.1509/jmkg.70.3.136.

[54] Stone, E.F., Gueutal, H.G., Gardner, D.G. and McClure, S. 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*. 68, 3 (1983), 459–468. DOI:https://doi.org/10.1037/0021-9010.68.3.459.

[55] Strater, K. and Lipford, H.R. 2008. Strategies and Struggles with Privacy in an Online Social Networking Community. *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1* (Swinton, UK, UK, 2008), 111–119.

[56] Stutzman, F., Capra, R. and Thompson, J. 2011. Factors mediating disclosure in social network sites. *Computers in Human Behavior*. 27, 1 (Jan. 2011), 590–598. DOI:https://doi.org/10.1016/j.chb.2010.10.017.

[57] Stutzman, F. and Hartzog, W. 2012. Boundary regulation in social media. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work* (2012), 769–778.

[58] Syed H. Akhter 2014. Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*. 31, 2 (May 2014), 118–125. DOI:https://doi.org/10.1108/JCM-06-2013-0606.

[59] Taylor, S. and Todd, P.A. 1995. Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*. 6, 2 (Jun. 1995), 144–176. DOI:https://doi.org/10.1287/isre.6.2.144.

[60] Triandis, H.C. 1995. *Individualism & collectivism*. Westview Press.
[61] Tsoi, H.K. and Chen, L. 2011. From Privacy Concern to Uses of Social Network Sites: A Cultural Comparison via User Survey. *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)* (Oct. 2011), 457–464.
[62] Ur, B. and Wang, Y. 2013. A cross-cultural framework for protecting user privacy in online social media. *Proceedings of the 22nd International Conference on World Wide Web* (2013), 755–762.
[63] Wang, S.-L. and Lin, S.S.J. 2007. The effects of group composition of self-efficacy and collective efficacy on computer-supported collaborative learning. *Computers in Human Behavior*. 23, 5 (Sep. 2007), 2256–2268. DOI:https://doi.org/10.1016/j.chb.2006.03.005.
[64] Wang, Y., Norcie, G. and Cranor, L.F. 2011. Who is Concerned About What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. *Proceedings of the 4th International Conference on Trust and Trustworthy Computing* (Berlin, Heidelberg, 2011), 146–153.
[65] Wilfong, J.D. 2006. Computer anxiety and anger: the impact of computer use, computer experience, and self-efficacy beliefs. *Computers in Human Behavior*. 22, 6 (Nov. 2006), 1001–1011. DOI:https://doi.org/10.1016/j.chb.2004.03.020.
[66] Wisniewski, P., Islam, A.K.M.N., Knijnenburg, B.P. and Patil, S. 2015. Give Social Network Users the Privacy They Want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Feb. 2015), 1427–1441.
[67] Wisniewski, P., Lipford, H. and Wilson, D. 2012. Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2012), 609–618.
[68] Wisniewski, P., Xu, H., Lipford, H. and Bello-Ogunu, E. 2015. Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology*. 66, 9 (Sep. 2015), 1883–1896. DOI:https://doi.org/10.1002/asi.23299.
[69] 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, (Feb. 2017), 95–108. DOI:https://doi.org/10.1016/j.ijhcs.2016.09.006.
[70] Xu, H., Dinev, T., Smith, H.J. and Hart, P. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings* (Paris, France, 2008).
[71] Yao, M.Z. and Zhang, J. 2008. Predicting User Concerns about Online Privacy in Hong Kong. *CyberPsychology & Behavior*. 11, 6 (Dec. 2008), 779–781. DOI:https://doi.org/10.1089/cpb.2007.0252.
[72] Youn, S. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*. 43, 3 (Sep. 2009), 389–418. DOI:https://doi.org/10.1111/j.1745-6606.2009.01146.x.
[73] Young, A.L. and Quan-Haase, A. 2009. Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. *Proceedings of the Fourth International Conference on Communities and Technologies* (University Park, PA, 2009), 265–274.

9 Appendix

DV	US	Singapore	South Korea
Corrective	Baseline	0.080	–0.441***
Collaborative		0.077	–0.052
Preventive		0.443***	–0.138*
Information control		–0.188***	–0.573***
Privacy concerns		0.393***	–0.115
Subjective norms		–0.071	–0.248***
Descriptive norms		–0.337***	–0.652***
Privacy self-efficacy		–0.148**	–0.849***
Privacy collective efficacy		–0.343***	–0.656***

Table A: Comparison of overall (marginal) effects of country on privacy management strategies, privacy concerns, norms, and efficacy[2].

[2] Our measurement invariance test did not support full scalar invariance; thus, comparisons of intercepts should be interpreted with caution.