Collective Privacy Management in Social Media: A Cross-Cultural Validation

HICHANG CHO, National University of Singapore
BART KNIJNENBURG, Clemson University
ALFRED KOBSA and YAO LI, University of California, Irvine

If one wants to study privacy from an intercultural perspective, one must first validate whether there are any cultural variations in the concept of "privacy" itself. This study systematically examines cultural differences in collective privacy management strategies, and highlights methodological precautions that must be taken in quantitative intercultural privacy research. Using survey data of 498 Facebook users from the US, Singapore, and South Korea, we test the validity and cultural invariance of the measurement model and predictive model associated with collective privacy management. The results show that the measurement model is only partially culturally invariant, indicating that social media users in different countries interpret the same instruments in different ways. Also, cross-national comparisons of the structural model show that causal pathways from collective privacy management strategies to privacy-related outcomes vary significantly across countries. The findings suggest significant cultural variations in privacy management practices, both with regard to the conceptualization of its theoretical constructs, and with respect to causal pathways.

CCS Concepts: • **Security and privacy** → *Human and societal aspects of security and privacy*;

Additional Key Words and Phrases: Privacy, collective privacy management, social media, measurement invariance

ACM Reference format:
Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. 2018. Collective Privacy Management in Social Media: A Cross-Cultural Validation. *ACM Trans. Comput.-Hum. Interact.* 25, 3, Article 17 (June 2018), 33 pages.
http://dx.doi.org/10.1145/3193120

1 INTRODUCTION

As privacy risks have become omnipresent and increasingly unpredictable in today's networked society, privacy management has been a salient issue for consumers, researchers, and practitioners. Numerous studies have shown that privacy remains a primary factor shaping user interactions with new technologies, particularly with social and collaborative technologies [60, 104, 123].

Recently, researchers have proposed new conceptualizations and operationalizations of privacy management to understand users' privacy practices as collaborative processes, since privacy in networked environments (e.g., social media) inherently requires interpersonal or group-level

Authors' addresses: H. Cho, Department of Communications and New Media, National University of Singapore, Singapore, 117416; email: cnmch@nus.edu.sg; B. Knijnenburg, 215 McAdams Hall, Clemson University, Clemson, SC 29634-0974, U.S.A; email: bartk@clemson.edu; A. Kobsa and Y. Li, Department of Informatics, University of California, Irvine, Irvine CA 92697-3440, U.S.A; emails: {kobsa, yao.li}@uci.edu.

http://dx.doi.org/10.1145/3193120

coordination by multiple stakeholders [26, 59, 80, 122]. Several conceptual models, such as collaborative privacy management [47], collective privacy management [98], and interpersonal privacy management [59] have been proposed to capture the collective and collaborative process of privacy management in networked environments. Although these studies have advanced the concept of privacy management, there are a few notable gaps in previous research, which should be further addressed by researchers in order to advance our understanding of privacy.

Here we consider "collective privacy management" as the management of collectively-managed information (e.g., information published on social networks), which can be accomplished using either collaborative strategies or individual strategies. For instance, social networking site (SNS) users negotiate "rule of thumbs" about sharing tagged photos and discuss how to protect each other's private information [11, 59]. They also regulate interpersonal boundaries using "friends only" or "secrete group" features to restrict access to a selected group of individuals [103]. Researchers who pursue a quantitative approach have redefined and expanded earlier conceptual models of collective privacy management by adding new, but potentially overlapping, constructs and scales. Evidence for their validity is mostly based on exploratory factor analysis focusing on dimensionality or factorial purity [26, 33]. Other important aspects of measurement validity (such as convergent validity, discriminant validity, and predictive validity) should be confirmed through rigorous validity analyses, which is essential for the development of a robust measurement for a proper evaluation, analysis, and understanding of privacy practices in networked environments.

Given that privacy is a global phenomenon that is culturally shaped [5, 27], the confirmation of measurement validity or a causal/predictive model in a single country may not guarantee its applicability across different cultures. Research has shown the cultural embeddedness of many social dynamics on social media, including social capital formation and relationship maintenance [46, 52], suggesting that collective privacy management may also have culturally specific aspects. However, most studies on collective privacy management to date have been conducted in a single country (mostly in the US), and we do not know to what degree collective privacy management has the same theoretical structure and psychological properties across different cultures. As Steenkamp and Baumgartner [99] correctly noted, if a construct or research model that was validated in one country is applied to another country without taking additional precautions, conclusions based on a comparison of the results are at best ambiguous and at worst erroneous.

The purpose of this study is to address the aforementioned gap. First, drawing on previous theories and studies about privacy [3, 26, 47, 82, 122], we refine and extend measurement scales of collective privacy management to aptly capture aspects of privacy management strategies that Facebook users employ. Second, we validate the construct validity of the measures in a single country by conducting a confirmatory factor analysis (CFA) on our US sample. Third, we perform a structural equation modeling (SEM) analysis to examine the predictive validity of the measures in the US sample, i.e., the degree to which the construct of privacy management can predict associated outcomes such as perceived privacy control and self-disclosure on Facebook. Fourth, we test whether the same measurement model and casual model can be applied to two other countries, namely South Korea and Singapore.

In doing so, this study aims to contribute to the Human-Computer Interaction (HCI) and privacy research community by (a) proposing a theory-based culturally robust measurement of collective privacy management; (b) specifying cultural differences in collective privacy management strategies; and (c) proposing methodological precautions that must be taken in quantitative intercultural or cross-national privacy research. The results show that the original measurement model is only partially invariant and that the causal model varies across countries, suggesting a cultural sensitivity of privacy management both with regard to the conceptualization of its theoretical constructs and with respect to causal pathways.

The remainder of this paper is organized as follows. First, we review previous literature related to collective privacy management, and cross-cultural studies about privacy and information practices.[1] We then present the results, progressing from the measurement model test (US) to the predictive/causal model test (US), the multiple-group measurement model invariance/equivalence test (three country samples), and the predictive/causal model (comparison between the three samples). Finally, we discuss implications for research and practice.

2 LITERATURE REVIEW

2.1 Advancement of Privacy Conceptualization

New technological developments, such as the advent of audio recordings in the 19th century, television, the Internet, and, more recently, social media, often intrude into personal life and affairs, and thus threaten "the right of privacy" or "the right to be let alone" [116]. To preserve personal space, individuals engage in privacy management, which is defined as "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" [118, p. 7]. From this perspective, privacy is conceptualized as personal control or autonomy with which individuals "determine when, how, and to what extent information about them is communicated to others" [118, p. 7].

Many researchers have claimed that privacy is an inherently social issue, to the extent that it involves coordination and conflict between multiple parties, and that it should thus be conceptualized as a collective issue [4, 5, 47, 84]. Once personal information is disclosed to others, the private information is co-owned and co-managed by multiple stakeholders, and the boundary of information changes from a personal boundary to a boundary that is collectively upheld. Because co-ownership entails responsibility to protect the shared information, people coordinate, commit to rules and norms concerning privacy management, and follow them when managing interpersonal boundaries [83, 84]. This results in collective control over the flow of private information within and across social units such as families, groups, and organizations. From this perspective, the privacy of information is managed by a dynamic and recursive process, whereby members negotiate and redefine interpersonal, interactional, and territorial boundaries [3, 4, 6]. Therefore, a proper understanding of psychological aspects of privacy must include the interplay of people, their social world, and their physical environment [3, 66].

Privacy scholars have conceptualized this interpersonal or collective process of privacy management using different terms, such as collaborative privacy management [47, 97], communication privacy management (CPM) [84], networked privacy management [26], collective privacy management [98], collective information practice [37], and interpersonal privacy management [59]. In this study, we use the term "collective privacy management" to describe and explore this phenomenon. While "collaborative privacy management" refers to collaborative actions and decision-makings related to privacy [47], collective privacy management includes both individual and collaborative processes through which multiple stakeholders (including individuals, social ties, and groups) manage shared personal information. Because privacy management occurs at both the individual and the collective levels [33, 59], we choose a broader conceptualization that subsumes both autonomous privacy actions and collaborative/interdependent boundary regulations through which users manage privacy in a communal/networked environment.

[1]For the sake of brevity, we focus on a few central themes in our literature review. Appendix B complements this core literature review and provides a summary of the key findings of twice as many other empirical studies related to privacy, culture, and information disclosure.

2.2 Theoretical Frameworks of Collective Privacy Management

HCI scholars have shown strong interest in designing effective mechanisms to support privacy management in collaborative or collective online settings [7, 10, 19, 20, 56, 97, 98]. Researchers have also focused on challenges in privacy management in SNSs [33, 39, 60, 69]. Due to the interconnectedness of SNS data (e.g., group photos) and context collapse (e.g., flattening of discrete social circles, such as friends, families, and colleagues into one large network), the ownership of and control over private information is distributed across multiple parties [114].

Several technological mechanisms for collective privacy management have been proposed by HCI scholars [7, 97, 98]. However, it is claimed that theoretical conceptualizations and understandings of collective privacy management are yet to be advanced to guide such design efforts [47]. A few attempts have been made to develop conceptual models of collective privacy management and to uncover its underlying dimensions. Most of these studies rely on Altman's theory of privacy and Petronio's CPM theory as theoretical frameworks.

Altman [3, 4] broadens the concept of privacy by analyzing privacy at multiunit levels (e.g., across individuals, groups, time, cultures, and the environment). He points out the dialectical nature of privacy [3]: for effective functioning of a group, members must disclose their personal information to others but must, at the same time, also protect their personal space in order to enjoy a private life and autonomy. People balance the competing needs for privacy and for disclosure through interpersonal boundary regulation processes [3, 4]. Privacy regulation is a dynamic process rather than a state, to the extent that people change the desired level of privacy in response to changes in internal states and external conditions (e.g., cultural differences or the physical environment, such as social crowding and population density). While traditional privacy studies emphasize autonomous and independent control over informational output to others, Altman conceptualizes privacy management as a bi-directional process of regulating both input from others (e.g., others' visits, glances or noise) and output to others (disclosures to others), which are regulated through a variety of behavioral, interpersonal mechanisms including verbal, paraverbal, nonverbal behaviors as well as environmental mechanisms, "such as personal space and territoriality, and culturally defined styles of responding" [5, p. 66].

Petronio's [82, 84, 85] theory of CPM is built on Altman's dialectic conception of privacy. The CPM theory extends Altman's theory of privacy by explicating the ways in which privacy rules and norms are developed through collaborative negotiations. According to the CPM, the boundary regulation process is managed by formulating and coordinating three key boundary rules in a group: boundary ownership, permeability (or access control), and linkages. Boundary ownership refers to specifying or negotiating co-ownership of private information (e.g., ownership of a group photo in Facebook) and deciding rules and norms about co-ownership. Permeability regulations refer to controlling access to the private information. Boundaries around private information can be more or less permeable (i.e., thick and thin boundaries), as people enact various levels of boundary access and protection rules depending on the perceived risk or consequences of information disclosure. Linkage regulations refer to how the boundary can be extended through members' social connections. In summary, through interpersonal boundary management processes, members collaboratively decide who is involved in owning private information and what rules should be applied to co-ownership (i.e., boundary ownership), what information can be accessed by whom and how much access is granted (permeability/access), and how the linkages to potential co-owners are established through current members' personal networks (linkages).

2.3 Empirical Studies and Underlying Dimensions of Collective Privacy Management

Early work on privacy in SNSs focused primarily on users' information disclosure behavior [55, 59, 63, 101, 105]. Limiting disclosure is not the only way in which social network users can regulate

their privacy, though, and in recent years researchers have therefore expanded their view beyond information disclosure boundaries, to include the regulation of relational, territorial, interactional, and network boundaries [78, 122]. Consistent with the theoretical frameworks reviewed above, this research shows that SNS users engage in a wide range of privacy management strategies to regulate privacy in a communal/networked environment. For instance, SNS users engage in interpersonal boundary regulations by segregating their interaction with different audiences using a "friends only" profile [103]. Users also manage their networks by creating multiple profiles on SNSs to prevent different social circles from overlapping (i.e., context collapse) [104]. In line with Altman [3], Facebook users not only regulate information output to others but also actively manage input from others because they are concerned about others posting on their timeline [45]. Efforts in the management of privacy risk in social media often comprise a collaborative practice. This includes, for example, negotiating the ownership of photos with multiple users and co-managing these photos [11, 59], and establishing privacy norms and determining the appropriateness of co-owned content together with friends [33].

Several studies have proposed more comprehensive conceptual models to identify underlying dimensions of collective privacy management. Collaborative and collective processes have been found to be key elements of privacy management strategies in social media contexts [79, 114, 122]. Using semistructured interviews and focus-groups, Lampinen and colleagues [59] presented a multidimensional model of privacy management strategies in the context of SNSs: behavioral vs. mental, preventive vs. corrective strategies, and individual vs. collaborative. In addition to behavioral strategies, SNS users often rely on mental strategies, such as simply trusting each other in terms of privacy protection and expecting that their privacy efforts will be reciprocated by their friends. SNS users not only employ preventive strategies (e.g., discriminant information sharing) but also corrective strategies (e.g., untagging, coordinated content removal) to deal with unexpected or unintended outcomes (i.e., boundary turbulence according to the CPM [82]). These coping mechanisms occur at both individual and collaborative levels.

Similarly, Wisniewski and colleagues [122] distinguished between *technology-supported boundary mechanisms*, behaviors supported through SNS interface controls, and *coping mechanisms* that users devise outside of these interface features. They identified seven behavioral boundary coping mechanisms, namely filtering, ignoring, blocking, withdrawal, aggression, compromise, and compliance.

Relatively fewer studies adopted a quantitative approach. Drawing on Altman's theory of privacy [3, 4] and the CPM theory [82, 84], Cho and Filippova [26] proposed a four-dimensional model of networked privacy management. Using focus-group interviews and survey data, the model uncovered four underlying dimensions (i.e., information control, preventive, corrective, and collaborative strategies) of networked privacy management strategies that reflect both individual and group-level processes, preventive and corrective, technological, and behavioral coping mechanisms.

Drawing on the CPM theory, Jia and Xu [47] developed a three-dimensional model of collaborative privacy management. The study confirmed that there are three underlying dimensions of collaborative privacy management: boundary ownership management (e.g., coordinated ownership specification), boundary permeability management (e.g., accessibility control), and boundary linkages management (e.g., in-out group). The study also validated an instrument (with nine survey items) using survey data and SEM analyses.

As noted earlier, however, research on collective privacy management is still nascent, and further research is yet to be conducted to assess whether these research frameworks (and their associated constructs) are not only valid, but also extendable from one country (typically the US) to other countries.

Table 1. A Multidimensional Model of Collective Privacy Management Strategies

Dimensions	Boundary regulation process	Levels/coping types	Examples
Collaborative strategies	Co-ownership management	Interpersonal & group levels/behavioral coping	Coordinated rule settings; Negotiation of co-ownership
Information control	Permeability management	Individual level/ behavioral & mental coping	Discriminant information sharing
Preventive strategies	Permeability management	Interpersonal & individual levels/ behavioral coping & technology-supported coping	Accessibility control (e.g., segregated groups, friends only); Visibility control (e.g., timeline review)
Corrective strategies	Permeability management	Interpersonal & individual levels/ behavioral coping	(Coordinated) content removal (e.g., untagging)
Network management strategies	Linkages management	Individual level/ behavioral coping	Network/boundary extension (filtering out, filtering in)
Audience control strategies	Accessibility & extension management	Individual level/ technology-supported coping	Access control (e.g., privacy settings)

2.4 Conceptualization of Collective Privacy and Key Dimensions

In sum, the literature reviewed above suggests that collective privacy management is multifaceted and multidimensional, but different works propose different sets of dimensions of collective privacy management. Narrow conceptualizations of collective privacy management can lead to an incomplete (and potentially inaccurate) understanding of user behavior and/or mask important differences in privacy management across individuals, groups, and cultures. Privacy management occurs at multiple levels (individual, interpersonal, group, and network levels). Through autonomous and interdependent actions and processes, SNS users manage three fundamental aspects of boundary regulations: boundary ownership, permeability, and linkages. Privacy management is also a dynamic process such that members not only develop preventive measures (preventive strategies) but also coordinate post-hoc actions and strategies (corrective strategies for boundary turbulence). This can be done through technology-supported privacy management as well as a variety of behavioral, mental, and interpersonal coping mechanisms.

To analyze such a comprehensive notion of collective privacy management, we propose the following conceptual model of collective privacy management in this study that combines and extends the previous conceptualizations reviewed above. The model includes six dimensions of collective privacy management reflecting multiple levels (individual and group level), regulation processes (ownership, permeability, and linkages), and types (preventive vs. corrective, behavioral vs. mental vs. technical) (see Table 1 for details). These levels, regulation processes, and types can be exhaustively combined, but such an extremely granular partitioning of privacy management strategies arguably belies users' own conceptual understanding of the strategies they use. Rather,

our conceptual model draws on various existing models for its dimensional structure [26, 47], which we indeed validate in our study. Although our conceptual model may not be exhaustive, it subsumes all fundamental aspects of collective privacy management, which allows for comprehensive analyses of its multiple dimensions across cultures/countries. In appendix A, we list for each dimension the specific types of privacy management strategies that social media users employ in the context of SNSs.

2.5 Cross-Cultural Variance in Privacy Management

According to Altman [5], privacy regulation is a culturally universal and pervasive process as the psychological viability of an individual or a group is essentially dependent on the ability to control social interaction with others (i.e., interpersonal boundary control). However, while the *existence* of a privacy regulation process may be universal, recent research has shown that people differ substantially in the *specific* privacy management strategy that they choose to implement [120], possibly motivated by their personal communication style [77]. Moreover, privacy regulation strategies may be culturally unique, to the extent that personal privacy rules and strategies are the behavioral manifestations of cultural traits. For instance, the Javanese practice of speaking softly and hiding their feelings, and the Japanese strong consensus on refraining from sharing overheard information manifest collectively shared and culturally specific privacy practices [73, 118]. Europeans tend to consider privacy a fundamental human right, whereas people in the US regard it as something that can be negotiated through social or legal contracts [93].

Thus, while the need for privacy regulation may be culturally universal, the specific behavioral mechanisms and techniques used to regulate the desired level of privacy and social interactions may differ across cultures. In Altman's words, "privacy is a universal process that involves culturally unique regulatory mechanisms" [5, p. 66]. Accordingly, it has been claimed that "all cultures have evolved mechanisms by which members can regulate privacy, but that the particular pattern of mechanisms may differ across cultures. Thus, to examine privacy as a cross-cultural phenomenon, the level of analysis must be shifted from particular privacy behaviors to a more holistic, patternlike analysis" [5, p. 70].

2.6 Cross-Country Comparisons of Privacy/Information Behavior Online

Though privacy theorists/scholars have proposed privacy regulation as a culturally specific process, there is a lack of empirical studies that examine cross-cultural variation in privacy practices on SNS, and the role of culture in privacy management and regulation. People's perceptions and behavioral responses towards online privacy can vary across countries because online users in different countries are used to country-specific cultural norms and legal systems that tend to favor different values and interests, such as collective over individual interests or autonomy/independence over bondage/interdependence [65, 107].

Several studies examined cross-national differences in privacy/information behavior using the notion of national cultures, such as individualism and collectivism [17, 18, 27, 61, 67]. While individualists favor personal rights, autonomy, independence, and privacy, collectivists are more likely to emphasize shared values and goals in close, committed, and strong relationships [75, 110, 111]. The tendency of individuals in collectivistic cultures to cooperate and reinforce mutual goals could be associated with greater willingness to disclose personal information [27]. As such, collectivists place less emphasis on keeping personal information private since they are used to sharing information about themselves freely in order to maintain such strong bonds with others.

A few empirical studies lend support for this proposition. For instance, Cao and Everard [18] noted that individuals with high uncertainty avoidance scores would naturally avoid uncertainty about their personal information by limiting others' access. Kim and Yun [52] found that to avoid information access by unwanted friends, Koreans choose to close their own homepages

temporarily rather than de-friend anyone because of their valuation of *Jeong*, a feeling which stresses relational interdependence. Li et al. [61] studied information disclosure across eight different countries, and demonstrated that participants in individualistic countries were less likely to accept disclosure for automation and customization, whereas participants in collectivistic countries were relatively more likely to accept disclosure if it benefits the community.

3 STUDY FOCUS AND RESEARCH QUESTIONS

Our work moves beyond existing privacy research in two important ways. First of all, moving beyond mere information disclosure behavior, our work covers collective privacy management as a broader approach to privacy management. Second, our work addresses how culture influences users' collective privacy management strategies. While each of these issues has been looked at individually already, ours is arguably the first to take both steps simultaneously, thereby implementing Altman's suggestion of conducting a "holistic, patternlike analysis" and directly evaluating his claim that privacy is managed using a "particular pattern of mechanisms [that] may differ across cultures" [5, p. 66].

Our cross-national analysis of collective privacy management strategies also allows us to validate more carefully the instrument that we developed to measure privacy management in collective/communal settings such as SNSs. Using multiple-group CFA we can not only conduct convergent and discriminant validity tests, but also address the topic of *measurement noninvariance*, i.e. "whether instruments designed to measure the relevant constructs are cross-nationally invariant" [99]. If a measurement lacks invariance, findings from a cross-national study based on that measure could be ambiguous or erroneous because we do not know whether cross-national differences observed in a study are due to structural differences between countries, or perhaps because people from different cultures interpret or respond to an instrument in a different way. Finally, our study includes several consequences of privacy management, and we can thus determine whether the presumed causal links between collective privacy management and these consequences differ per country.

In other words, we can ask the following research questions when we analyze a single country only:

RQ1: Does our measurement model of collective privacy management have convergent and discriminant validity in this country?
RQ2: What consequences are associated with collective privacy management in this country?

When addressing multiple countries, we can ask the above questions for *each* country, and additionally the following research questions:

RQ3: Does the measurement of collective privacy management differ significantly per country?
RQ4: Do the consequences associated with collective privacy management differ significantly per country?

We thus make three distinct contributions: Our *methodological* contribution consists of the introduction of measurement invariance testing to the HCI community.[2] Our *theoretical* contribution consists of an evaluation of the culturally different patterns of privacy management and their consequences, as suggested by Altman [5]. Our *practical* contribution is a culturally robust instrument for measuring collective privacy management. We will reflect upon these three contributions in the discussion section of our article.

[2]In fact, we found only a single paper in the entire ACM Digital Library mentioning the term.

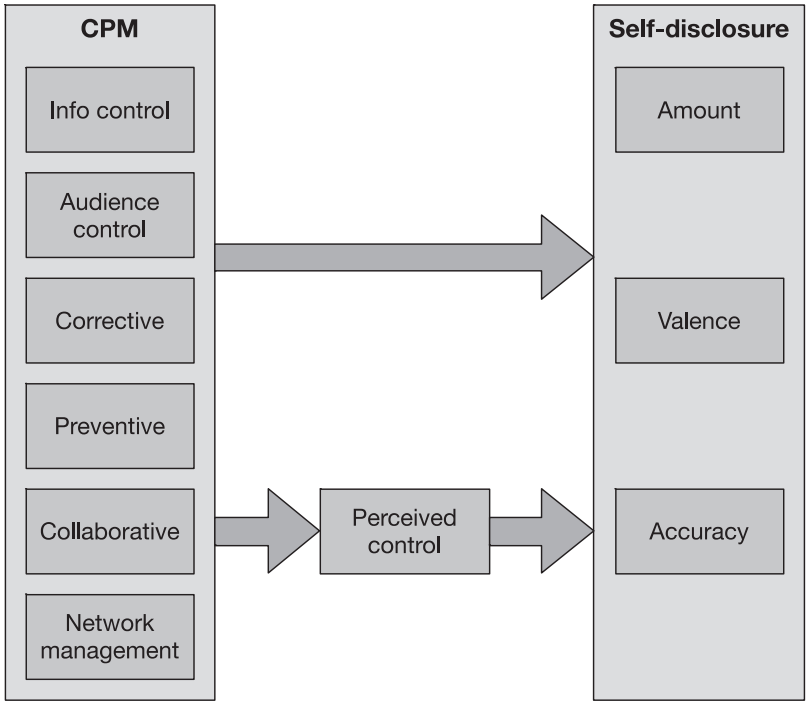

Fig. 1. Research model: Multiple dimensions of CPM strategies and their impacts on self-disclosure.

To test these research questions, we evaluate the research model displayed in Figure 1. We consider six dimensions of collective privacy management, each measured with multiple indicators (further explained in Section 4.2). We evaluate the measurement characteristics of these collective privacy management dimensions, as well as their presumed causal effects on users' self-disclosure, which is measured in terms of amount, valence, and accuracy (also further explained in Section 4.2). We argue that the ability to engage in collective privacy management may increase the amount and accuracy of disclosure, and remove social barriers toward posting negative posts. We argue that this is partially due to the collective privacy management strategies giving them more meaningful control over their privacy and information. Perceived control thus acts as a potential mediator between collective privacy management and self-disclosure.

Theoretically, perceived privacy control refers to a person's belief that s/he can control and protect his/her own private and personal information online. The construct is related to perceived control that is defined as the belief about the extent to which a person has control over the environment [87]. Perceived control has been thoroughly defined in many theories such as self-efficacy [8] and the theory of planned behavior [2]. Perceived control is predictive of behavior such that people who are confident in attaining a goal are more likely to enact a target behavior [2].

Perceived control may have a differential impact on self-discourse. On the one hand, having a positive outlook motivates people to engage in goal-attainment efforts [31, 89]. Therefore, SNS users with high levels of perceived information control, believing that a goal (privacy protection/information control) is achievable, engage in conscious information control, leading to selective and reduced self-disclosure [9]. On the other hand, perceived control over information reduces perceived risks of information disclosure, which results in higher levels of disclosure. Stutzman and colleagues [101] and Vitak [113] found that Facebook users who employed privacy settings (i.e., friend lists) revealed more personal information in their profiles because they perceive that

they have effective means to avoid privacy risks. In addition, a high level of perceived control often promotes complacency rather than effective goal-relevant behavior such as self-protection behavior [117]. For instance, Brandimarte and colleagues [12] document a "control paradox" such that people who experience more perceived control over limited aspects of privacy sometimes respond by revealing more information, to the point where they end up more vulnerable to privacy risks. Taken together, we predict that perceived control plays an important mediating role to the extent that the enactment of privacy management strategies increase perceived control, which in turn (positively or negatively) affects self-disclosure.

4 METHOD

4.1 Sample and Data Collection

Data for this study were collected through online surveys ($N = 498$) administered by a professional online research company (Qualtrics). Eligibility was restricted to Facebook users who are older than 18 (US and South Korea) and 21 (Singapore) and who visited their Facebook page at least once every two weeks. We chose Facebook as the study context because it is the most popular SNS in the three countries (it has 2.2 billion monthly active users globally as of the first quarter of 2018 (https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/).

We collected data from three countries, Singapore, South Korea, and the US, to ensure that our research model can be applied to both Eastern and Western cultures. We chose the US as a base group because most research and measurement models of privacy are based on US samples. South Korea and Singapore were chosen as comparison groups because they represent Eastern cultures (one in East Asia and the other in Southeast Asia) and have among the highest percentage of Internet users in Asia. According to Hofstede's national culture indices [44], US scores 91 on individualism (which is the highest among 81 countries), while Singapore and South Korea score 20 and 18, respectively. Previous intercultural privacy studies used these countries as representative for their respective cultures (e.g., individualism and collectivism) [22, 27, 28, 62, 81, 88]. Therefore, we argue that—with certain reservations outlined in our limitations section—the selection of these three countries allows us to assign cultural significance to cross-country differences. We performed back-translation to ensure that the original (English) and translated (Korean) questionnaires had the same linguistic interpretations for all subjects. The three countries are economically developed, have well-established ICT infrastructures and services, and have relatively high Facebook penetration rates. These similarities help remove factors that can potentially confound cross-cultural comparisons.

Participants were randomly selected from an online panel recruited by Qualtrics. The panel is an opt-in, privacy-protected participant pool. It consists of over 20 million panelists (6 million members in North America and 6.4 million in Asia Pacific). The research company runs regular benchmarking surveys to ensure their panelists are representative of the larger Internet population.

A total of 498 (Singapore: 166, South Korea: 166, and the US: 166) respondents participated in the survey. The ratio of females was 44.6% in Singapore, 53% in South Korea, and 44% in US. The mean age was 38.77 (SD = 11.51) for the Singapore sample, 34.30 (SD = 11.10) for the South Korea sample, and 43.22 (SD = 14.10) for the US sample. The majority of the Singapore sample ($n = 124$, 74.7%), the South Korea sample ($n = 92$, 55.4%) and the U.S. sample ($n = 110$, 66.3%) had more than 81 Facebook friends.

4.2 Measures

We employed several prevalidated scales adapted from previous studies, and instruments developed by the authors, to assess variables in the research model. A 7-point Likert-type scale was used for all measures. Measurement items and descriptive statistics are reported in Appendix A.

4.2.1 Self-disclosure. Wheeless and Grotz' [119] General Disclosiveness Scale was employed to assess the degree to which Facebook users disclose personal information via Facebook. For this analysis, three of the subscales were used: amount, accuracy, and valence.

- *Amount* refers to the frequency and duration of information revealed, which was assessed by six items (e.g., "I often discuss my feelings about myself on Facebook," Cronbach's α = .92).
- *Accuracy* refers to the degree of accuracy and sincerity in the act of disclosing information, and was assessed using two items (e.g., "I always feel completely sincere when I reveal my own feelings and experiences on Facebook," α = .82).
- *Valence* refers to the extent disclosure is positive or negative, and was assessed with three items (e.g., "I usually disclose negative things about myself on Facebook," α = .93).

4.2.2 Perceived Privacy Control. We employed a single-item (i.e., "Managing personal information on Facebook is entirely within my control") in order to assess control beliefs related to privacy and information disclosure on Facebook.

4.2.3 Collective Privacy Management Strategies. In order to capture broader aspects of collective privacy management, we developed new items and scales and combined them with the multidimensional scales adapted from Cho and Filippova [26], which include five items adapted from the interpersonal privacy management scale developed by Stutzman and Kramer-Duffield [103]. As noted earlier, we chose this measure for cross-cultural validation because it assesses comprehensive aspects of collective privacy management, which allows for identifying a set of core dimensions and items that can be shared across cultures. The original instrument consists of 19 items, assessing four dimensions of networked privacy management such as collaborative, corrective, preventive, and information control strategies. We employed a total of 35 items (including 16 newly constructed items) to assess six dimensions of privacy management strategies, which include two additional dimensions such as network management and audience control strategies. Of these, five items (two items from preventive strategies and three from information control strategies) were removed from the final measurement model because preliminary exploratory and confirmatory factor analyses showed that these items had factor loadings below .5. Table 1 and Appendix A provide details about each dimension.

- *Corrective strategies* refer to the use of existing privacy management features (e.g., untagging) and coordinated content removal strategies to control the visibility of unwanted content posted about a profile owner (7-item scale: e.g., "I untag myself from photos my friends uploaded," α = .96).
- *Preventive strategies* refer to preventing information leakage by constraining interpersonal/network boundaries and access (4-item scale: e.g., "I make use of friend lists to restrict the audience of my posts to certain individuals" α = .80).
- C*ollaborative strategies* refer to explicit coordination mechanisms (e.g., co-ownership specification) and interpersonal actions to collectively manage each other's privacy (7-item scale; e.g., "My friends and I negotiate 'rules of thumb' about sharing content concerning ourselves," α = .95).
- *Information control strategies* refer to controlling for the type of information considering an "imagined" audience through discriminant sharing (3-item scale; e.g., "I adjust content of my post based on who I think will see it," α = .84).
- *Network management strategies* refer to controlling Facebook network by filtering out strangers (3-item scale; e.g., "I do not use Facebook to make contact with people whom I never heard of." α = .89).

Table 2. The Results of CFA for Each Country Testing the Model Fit of the Baseline Measurement Model

Country	Model fits (CFI > .90, TLI > .90, RMSEA < .08)				Convergent validity (AVE > .5)	Discriminant validity (AVE > r^2)
	χ^2 (*df*)	CFI	TLI	RMSEA (90% C.I.)	Lowest AVE among latent factors	Highest squared correlation between latent factors
US	761.567 *(385)****	.926	.917	.077 (.069–.085)	.529 (preventive strategies)	.648 (between preventive and collaborative)
SG	678.600 *(385)****	.938	.920	.068 (.059–.076)	.533 (preventive strategies)	.465 (between preventive and information control)
KR	659.242 *(386)****	.942	.935	.065 (.057–.074)	.474 (preventive strategies)	.278 (between preventive and information control)

Note: The results show that the measurement model is adequate across countries.
***p <.001.

- *Audience control strategies* refer to regulating the types of audiences who can view the participants' posts on Facebook or contact them (e.g., "6-item scale; e.g., "I adjust Facebook preference settings to control who can view my posts," α = .96).

5 RESULTS

5.1 Baseline Measurement Model (RQ1)

A CFA was conducted to check whether the measurement model has an adequate model fit, and whether the factors display convergent and discriminant validity, *in the US sample*. A CFA measurement model establishes relationships between indicators (questionnaire items) and factors (the latent representations of the constructs measured by these items). The baseline model includes six latent factors of collective privacy management, such as corrective strategies, collaborative strategies, preventive strategies, information control strategies, network management strategies, and audience control strategies. All latent factors were allowed to be correlated with each other.

The results showed that the original measurement model was generally acceptable. Model fit indices were within acceptable ranges (Comparative Fit Index [CFI] >.90, Tucker-Lewis Index [TLI] >.90, Root Mean Square Error of Approximation [RMSEA] <.08; see Table 2 and Appendix A for details). CFI, TLI, and RMSEA are chosen as model fit indices as they represent different approaches (incremental measure vs. absolute measure of fit) of evaluating the degree to which the specified model is consistent with the observed data. *Convergent validity* tests whether the items that are meant to measure each construct are sufficiently strongly related to constitute a robust measurement scale. Convergent validity is supported when indicators load significantly on their respective factors, and the average variance extracted (AVE) from the items of each factors is higher than .50.

The results of CFA confirmed that all standardized factor loadings exceeded .6, and were statistically significant ($p < .001$). All latent factors had an AVE higher than .50, suggesting adequate levels of convergent validity.

Discriminant validity tests whether pairs of latent factors are sufficiently different from one another to constitute conceptually distinct constructs. According to Kenny [50], discriminant validity is supported when the intercorrelation between latent factors is lower than .85. Other rules of thumb suggest that the correlation should be smaller than the square root of the AVE of each factor.

The results showed that the square root of each latent variable's AVE was greater than its correlations with other latent factors, except for preventive strategies. This indicates adequate discriminant validity, except for preventive strategies, which had relatively weak discriminant validity. Specifically, the correlation between preventive strategies and collaborative strategies ($r = .801$) was only marginally below the benchmark and larger than the square root of AVE (.727) for preventive strategies. Thus, we conducted two additional tests for discriminant validity as suggested by Kenny [50] and Gefen et al. [40]. First, a constrained discriminant validity test was conducted in which the correlation between preventive strategies and collaborative strategies was set to the perfect correlation (1.0). The chi-square test shows the original, unconstrained model to be a better fit ($\Delta\chi^2$ (1) = 55.114, $p < 001$). Next, an alternative chi-square difference test was conducted by combining two highly correlated variables into one and running the model again. The chi-square difference was significant ($\Delta\chi^2$ (5) = 66.269, $p < 001$), suggesting that the original, six factor model to be a better fit. Overall, model fit indices worsened when alternative models were tested. The results of tests confirmed that our measurement model of CPM with six CPM constructs has adequate convergent and discriminant validities, though the distinction between preventive strategies and collaborative strategies was not optimal in the US sample.

5.2 Baseline Structural Model (RQ2)

A structural model was tested using the US sample, in which the amount, valence and accuracy of information disclosure[3] were regressed on the collective privacy management strategies, using perceived control as a potential mediator. The valence scale was reverse coded so that higher values indicate positive valence.

The model was trimmed by iteratively removing nonsignificant effects. Figure 2 shows the resulting model, which has an acceptable model fit (CFI = .94, TLI = .94, RMSEA = .069).

Corrective strategies have an effect on the amount and valence of information disclosure; US Facebook users who employ corrective strategies disclose more about themselves, and their posts have more negative tendencies. C*ollaborative strategies* have a similar effect on the amount and valence of information disclosure, but these effects are now partially mediated by perceived control. *Collaborative strategies* also have an effect on the accuracy of information disclosure that is fully mediated by perceived control. This mediation effect suggests that US Facebook users who employ collaborative strategies disclose more about themselves, and are more sincere and more negative, due to an increase in perceived control. Surprisingly, *information control strategies* have an opposite effect on the amount and valence of information disclosure. In other words, US Facebook users who employ information control strategies disclose *less* about themselves, and their posts have more *positive* tendencies. Finally, *network management strategies, preventive strategies*, and *audience control strategies* have no effect on the amount, valence, and accuracy of information disclosure.

In sum, the results suggest that three of the collective privacy measures (corrective, collaborative, and information control strategies) have an effect on the amount and valence of information

[3]The information disclosure factors showed convergent and discriminant validity.

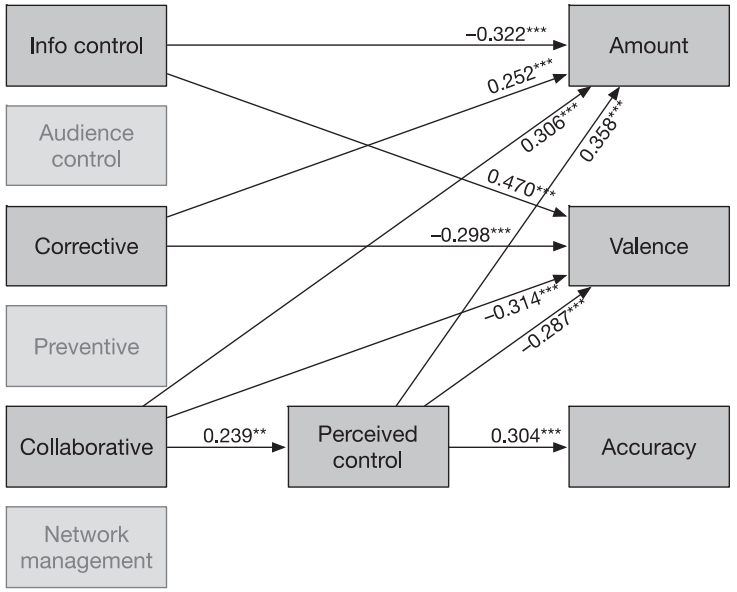

Fig. 2. Predictive model on the US Sample: The paths represent the significant effects of CPM dimensions on self-disclosure ($^{**}p < .01$, $^{***}p < .001$). Three privacy management strategies (information control, corrective, and collaborative) had a significant impact on self-disclosure.

disclosure (with the latter having an opposite effect). Only collaborative strategies have an effect on the accuracy of disclosure, which is mediated by perceived control.

5.3 Measurement Model Invariance Tests (RQ3)

Next, we proceed to examine the equivalence of measurement model across three sampling sites by conducting three measurement invariance tests such as configural, metric, and scalar invariance. If measurement invariance can be demonstrated, then the participants across all country groups interpret the individual questions, as well as the underlying latent factor, in the same way. First, we tested *configural model invariance*, i.e., whether the latent variables can consist of the same set of indicators across groups. Scholars [99, 115] suggested that configural model invariance can be examined by (a) running separate CFAs for each group and (b) checking whether model fits are adequate across the board. They also recommend to use alternative model fit indices (e.g., CFI, TLI, RMSEA) in addition to chi-square statistics. Table 2 and Appendix A summarize the results of baseline CFA for each country. The results show that alternative model fits, convergent validity (AVEs > .50), and discriminant validity (AVEs > the highest squared correlations with other latent factors) were adequate across the board. Standardized factor loadings of all measurement items exceeded .6 and were statistically significant ($p < .001$).

Two exceptions were found. As noted earlier (see Section 5.1), preventive strategies had relatively weak discriminant validity in the US model. We also found that the same construct had marginal convergent validity in the Korean sample (AVE in Korea = .474). Because of the size of correlation matrix among six factors of collective privacy management, which includes 45 estimates (15 intercorrelations × 3 groups), some violations can occur simply due to chance [15]. Therefore, we posit that at least a reasonable extent of convergent and discriminant validity was established in this study.

Table 3. The Results of Measurement Invariance Tests Showing Changes in Model Fit from the Configural Invariance Model to the Scalar Invariance Model

Model	Name	χ^2 (*df*)	$\Delta\chi^2$ (*df*)	CFI	TLI	RMSEA	Notes
1	Configural model	2099.409 (*1156*)***	–	.935	.927	.070	
2	Full metric invariance	2192.533 (*1204*)***	93.124 (*48*)***	.932	.927	.070	Factor loadings constrained
3	Partial metric invariance	2156.372 (*1200*)***	56.963 (*44*) ($p > .09$) Compared with configural model	.934	.929	.069	Two factor loadings of information control were uncon-strained
4	Scalar (full invariance)	2235.565 (*1244*)***	79.193 (*44*)* Compared with partial metric invariance	.932	.929	.069	Factor loadings and intercepts constrained.

Note: The results support partial metric invariance (i.e., model 3 in the table). *p <.05, ***p <.001.

We also estimated a baseline model in line with configural invariance, which estimates the same factor model in the three countries simultaneously, but imposes no further constraints on the model in terms of loadings and intercepts. The fit of the configural invariance model was satisfactory. Although the chi-square was significant (χ^2 [1156] = 2099.409, $p < .001$), the RMSEA of .070 indicated an acceptable fit, and the two other alternative indices were also above the commonly recommended .90 level (CFI = .935, TLI = .927). Therefore, we posit that a configural model is established.

Second, we tested *full metric invariance* by constraining the factor loadings to be invariant across countries. Metric invariance tests whether the strength of the relationship between each factor and its associated items (reflected in the factor loading) are the same across countries. When invariance of factor loadings is demonstrated (i.e., metric invariance), the underlying latent variables are measured in the same way in all groups. As such, predictive relationships (e.g., antecedents and consequences of collective privacy management strategies) can be meaningfully compared across countries. The test of metric invariance requires that the fit of the constrained model (i.e., the metric invariance model) should not be significantly worse than the fit of the baseline model. As shown in Table 3, the results of full metric invariance test indicated that there was a significant increase in chi-square between the model of configural invariance (model 1) and the model of full metric invariance (model 2) ($\Delta\chi^2$ (48) = 93.124, $p < .001$), although the fit did not decrease much in terms of the alternative fit indices (CFI = .932, TLI = .927, RMSEA = .070). Examination of the factor loadings across three different countries revealed that the significant increase in chi-square in the metric model might be due to a lack of invariance of factor loadings associated with "information control strategies." Thus, full metric invariance was not supported.

To test for *partial metric invariance*, the constraints on these parameters (sources of invariance) were sequentially relaxed, starting with the loading that had the largest differences across the three countries. We found that the chi-square of our partial metric invariance model was no longer significantly worse than the fit of the baseline model after two factor loadings were set free

($\Delta\chi^2$ (44) = 56.963, p = .09). The statistics for overall fit of this model are reported in Table 3 (see model 3). TLI and RMSEA slightly improved over the baseline model. Thus, partial metric invariance (with only two out of 30 invariance constraints relaxed) is supported. We tried relaxing additional factor loadings, but this did not result in improved model fit. Hence, we decided to choose the initial partial metric invariance model (model 3) in which the factor loadings of two indicators of "information control strategies" (i.e., "I adjust content of my post based on who I think will see it," and "I limit what I share on Facebook to what is appropriate for all my friends to see") were freely estimated across the three countries. Byrne [14] and Dimitrov [36] suggested that invariance in up to 20% of parameters is acceptable when conducting multiple group comparisons. As such, we can claim that our measurement model is "partially metric invariant," and can be used for comparing effects between countries (as we will do in 5.4).

Third, we tested *scalar invariance model* in which both factor loadings and intercepts were constrained to be equal across the three countries. When invariance of loadings and intercepts is demonstrated (i.e., scalar invariance), the scores given to indicators produce the same factor scores across groups. As such, scalar invariance allows mean-level comparisons between countries. Given that only partial metric invariance was achieved in the previous analyses, only the intercepts of the invariant factor loadings were constrained to be equal across countries. In other words, we only tested the equivalence of intercepts (i.e., scalar invariance) for which metric invariance holds because different slopes (e.g., information control items) can create different intercepts as an artifact. As such, the intercepts for "Information Control" were relaxed in our scalar invariance model (model 4). Scalar invariance was not supported (see model 4 in Table 2): the increase of chi-square relative to partial metric invariance (model 3) was significant $\triangle\chi^2(46) = 79.193, p < .05$, although the fit did not decrease much in terms of the alternative fit indices.

To test for *partial scalar invariance*, the constraints on intercepts were sequentially relaxed, starting with the intercept that had the largest differences across the three countries. More specifically, we relaxed intercepts for "Corrective Strategies" and "Audience Control" successively. The results showed that relaxing these intercepts did not improve model fit. Hence, we chose model 3 (the partial metric invariance model) as the best invariance model.

In sum, the results suggest that the measurement of collective privacy management *differs significantly per country*: there is partial metric invariance, but no scalar invariance. The latter suggests that our measures of collective privacy management strategies cannot be used to make mean-level comparisons between countries because starting points (i.e., intercepts) for different country groups were not the same. We will need to improve our scales to be able to make such comparisons. We can, however, compare the consequences of our collective privacy management measures (i.e., the amount, valence, and accuracy of disclosure) between countries.

5.4 Structural Model Comparison (RQ4)

In Section 5.2, we investigated the effect of the collective privacy management strategies on information disclosure in our US sample. In the current section, we run similar structural models for Singapore and Korea.[4] Each model was trimmed by iteratively removing nonsignificant effects. Figure 3 shows the resulting models. We find an acceptable model fit in both Singapore (CFI = .93, TLI = .92, RMSEA = .066) and Korea (CFI = .92, TLI = .91, RMSEA = .072).

Corrective strategies have the same effect on the amount and valence of information disclosure in Singapore as in the US, but in Korea there is no significant effect on the amount of information disclosure. In contrast to the US where collaborative strategies have an effect on all three

[4]Prior to testing the structural models, we tested the measurement model invariance of self-disclosure scales. Up to full metric invariance was supported, so the comparison of structural models across countries is allowed.

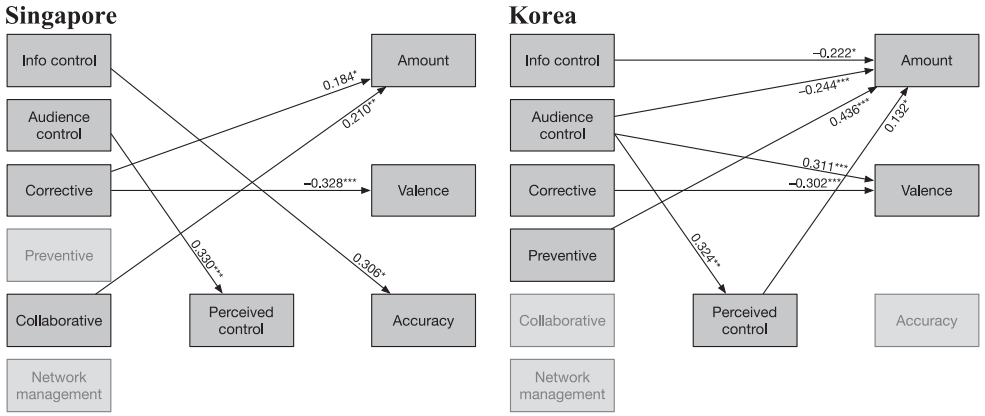

Fig. 3. Predictive models on the Korea and Singapore samples: paths in the diagrams represent significant impacts of CPM dimensions on self-disclosure. The impacts of privacy management strategies on self-disclosure differ significantly per countries.

self-disclosure factors, *collaborative strategies* only have an effect on the amount of information disclosure (and no significant effect on valence and accuracy) in Singapore, and in Korea collaborative strategies have no effect on information disclosure at all. Also in contrast to the US, *information control strategies* have an effect on the accuracy of information disclosure (rather than the amount and valence) in Singapore, and in Korea information control strategies only have an effect on the amount of disclosure. *Audience control strategies* had no effects in the US; in Singapore they have an effect on perceived control (although perceived control has no further effect on information disclosure in this country). In Korea, audience control strategies have a negative effect on the amount disclosure, as well as a positive effect that is mediated by perceived control. In other words, Korean Facebook users who use the audience control strategy disclose less information about themselves, although this strategy slightly increases their disclosure due to a higher perceived control. Finally, *network management strategies* have no effect on the amount, valence, and accuracy of information disclosure, just like in the US.

In sum, the results suggest that the effects of the collective privacy management measures on the amount, valence, and accuracy of information disclosure differ significantly per country. With the exception of the effect of corrective strategies on the valence of information disclosure, not a single effect is significant in all three countries. This suggests that not only the measurement of the collective privacy management strategies is different between countries (RQ3), but also the consequences of the use of these strategies on users' information disclosure (RQ4).[5]

6 DISCUSSION

Privacy is a multifaceted, evolving concept [3, 80], and measurement has been a key challenge for proper evaluation, theorization, and prediction of privacy-related attitudes and behaviors [94, 95]. Also, the growth of multinational research on privacy [5, 17, 32, 71, 73] raises many important

[5]It is true that the significant associations between variables observed in this study could potentially be due to common-method biases, since all variables in this study were measured using a single source. It is suggested that common-method biases are not a significant threat to validity when intercorrelations among variables are below .90. As noted earlier, the highest factor correlation in our study was .80. We also checked multicollinearity in our regression model, which is problematic when variance inflation factors are above 5.00. We found that all variance inflation factors are below 1.57. These results suggest that our study is not affected by common-method biases or multicollinearity.

questions about the degree to which theory or research developed in one country can contribute to our understanding of privacy practices in other countries. Given that most measurement or research models of (collective) privacy practices have been developed in the US [24, 68, 97, 121, 122], research should not only critically examine the validity of these models but also investigate the appropriateness of these models for explaining and predicting privacy attitudes and behaviors across countries. The present study describes the results of the first large-scale effort to address these issues simultaneously. The focus was on cross-culturally validating the measurement model and causal pathways related to collective privacy management strategies. Specifically, this study (a) revisits and extends the conceptual and operational definitions of collective privacy management; (b) empirically tests the validity of measurement and predictive models of collective privacy management using multinational samples; and (c) explores the degree to which privacy research developed in one country can be applied in other countries. In so doing, we advance the notion of collective privacy management by addressing three crucial elements of theory development: the refinement and extension of the theoretical constructs, the specification of their relationship with theoretically associated constructs (i.e., the definition of the nomological network), and generalization across cultures.

To recap, we find that the refined measurement model of collective privacy management exhibits desirable psychometric properties in the context of social media. The results also demonstrate that the causal (structural) model using collective privacy management constructs fits the data satisfactorily, and that these constructs can predict consequences, such as self-disclosure. Overall, the findings suggest that our measurement model is a useful tool for analyzing collective privacy management strategies and their consequences. However, the results of multiple group CFA also show that the measurement model has only partial invariance, indicating that social media users in different countries interpret the same measurement instruments in different ways. Also, cross-national comparisons of the structural model show that causal pathways from collective privacy management strategies to privacy-related outcomes (such as self-disclosure and perceived control) vary significantly across countries. Overall, the results suggest a cultural susceptibility of privacy practices: differences were found in both the measurement model and the structural (causal) model across three countries. In other words, we find that collective privacy management may have cultural differences not only in its psychometric properties but also its consequences.

6.1 Cross-National Comparison of the Collective Privacy Management Measurement Model

To address the conceptual concerns about privacy management in networked environments [79, 122, 123], this study provides a refined conceptual framework and measurement instrument for scholars to use as a starting point when studying collective privacy management. We refined and expanded the existing measurement model and instrument of collective privacy management, by adding two additional dimensions and enhancing existing dimensions with new items. When the revised measurement model was examined separately in each country, the results of CFA displayed adequate levels of model fit and construct validity, though we find relatively weaker convergent validity and discriminant validity for one construct: preventive strategies. The resulting six-dimensional model of collective privacy management reported here provides useful insights into the measurement of the relatively new and complex concept of collaborative privacy practices in a networked environment. The study finds a core set of dimensions and items that represent different aspects of collective privacy management.

Although the collective privacy management measurement model displayed adequate validity within each of the three countries, we find only weak invariance of the model *across* the three countries. Particularly, the results supported configural invariance and partial metric invariance

but failed to support scalar invariance, suggesting that the exact meaning and scaling of collective privacy management dimensions are likely to differ across cultures. Although further research is needed, there are a few possible reasons why a measure can fail to achieve invariance. As for partial metric invariance, it is possible that some items are more appropriate (or interpreted differently) in one country than in another. For instance, two items of information control strategies (i.e., "I adjust the content of my post based on who I think will see it," and "I limit what I share on Facebook to what is appropriate for all my friends to see") were found to be sources of metric invariance. Specifically, factor loadings for these two items in Singapore (1.523, 1.417) were substantially higher than those in the US (1.047, .920) and Korea (1.009, .650). A possible reason might be that Singaporian Facebook users are more sensitive to "self-censorship" because they live in a more authoritarian society with higher surveillance. It can also be due to other differences in response sets such as propensity for some Asian cultures to avoid using extreme response categories [21].[6]

As noted above, configural invariance and partial metric invariance observed in our study allow for cross-cultural comparison of our (structural) research model. However, any comparison of country means using traditional statistical procedures (such as MANOVA) would be premature due to the lack of scalar invariance found in this study. Studying differences in prevalence or preference of various types of collective privacy management strategies across cultures would be an interesting topic for privacy researchers and managers. However, this type of comparative analyses would be inappropriate or even erroneous given that no existing measure of collective privacy management provides the evidence of scalar invariance across countries.

Overall, the findings illustrate that the assumption of measurement invariance cannot be taken for granted in privacy research. Many privacy studies consider a single country (mostly the US), tacitly assuming that the same instrument, measurement model, and predictive model can be applied (or generalized) to other countries. Our findings challenge this assumption, and warn us to be skeptical about the cultural generalizability of studies with exclusively US participants. To wit, if individuals in different countries have a different understanding of certain items, then we cannot have confidence that empirical findings from one country can be generalized to another. Moreover, we suggest that cross-cultural studies will have to conduct formal tests to ensure that any cultural differences (or similarities) observed are not merely due to artifacts of measurement.

More generally, we argue that demonstration of invariance of a measurement instrument across groups is a prerequisite condition if one wishes to compare groups and make meaningful inferences about differences across groups. Otherwise, we may discover erroneous group differences that are in fact artifacts of measurement, or we may miss true group differences that have been masked by these artifacts [21]. Despite its importance, measurement invariance/comparability is implicitly assumed but rarely tested directly in most cross-cultural privacy research. In fact, the authors' review of articles on this topic from 1996 to 2016 indicate that out of 26 articles involving cross-cultural comparisons of attitudes, values, and behavior pertaining to information privacy, only two privacy studies [51, 64] tested measurement invariance across different cultural groups. The two studies measured privacy concerns using relatively well-established instruments (e.g., IUIPC). Given that collective privacy management is a relatively understudied concept and its measurement models are novel, we argue that the assumption check of measurement model is thus even more important.

Taken together, this study raises serious concerns regarding the use of a single universal scale of collective privacy management or making direct mean-level comparisons of collective privacy management strategies across cultures. Hence, we suggest that prior to assessing collective

[6]In fact, Korean respondents did not choose "7" for certain items. Similarly, only a few Singaporean and Korean respondents chose "1: strongly disagree" or "7: strongly agree" for many items.

privacy management strategies (or developing research models using the associated constructs) in different countries, the measurement model should be corrected/adjusted/validated properly. Additional work (combining, omitting, and perhaps adding new culturally specific dimensions) would be necessary in order to adapt and validate the collective privacy management measure across countries. A similar approach would be needed when evaluating privacy enhancing technologies or mechanisms developed to support collective privacy management practices across cultures.

6.2 Cross-national Comparison of the Collective Privacy Management Predictive Model

To test the predictive validity of collective privacy management constructs, we developed a causal model in which our six collective privacy management measures served as antecedents of four outcome measures (i.e., three self-disclosure variables and perceived control). We employed SEM to test these relationships. Like conventional linear regression, SEM does not "prove" causality, but instead requires researchers to make assumptions about the causal direction in the model. The relationship between privacy management strategies, perceived control, and self-disclosure is based on substantive theoretical arguments that suggest that providing users with sufficient privacy control increases the amount and accuracy of their disclosures, and facilitates the disclosure of negatively valenced posts.[7]

We compared the structural models across the three countries to check whether a research model validated in one county is applicable to another. To recap, the results of SEM analyses show that the structural models vary across our three country samples. Interestingly, the collective privacy management constructs play a larger role in predicting the outcome variables in the US than in Singapore and South Korea.

These findings are generally in line with previous cross-cultural literature that distinguishes between national cultures based on individualism and collectivism: Whereas individualists' behaviors are determined by their own capacities, attributes, and internal beliefs (e.g., personal control and competency), collectivists are more dependent on social situations and external environments [38]. As such, we can expect a tighter relationship between privacy actions and self-disclosure in the US sample to the extent that individuals' decisions regarding self-disclosure is determined by their own actions related to privacy. On the other hand, self-disclosure in collectivistic cultures might be contingent on factors other than privacy management practices, such as relational interdependency [52] and generalized reciprocity [23], leading to a relatively weaker relationship between collective privacy management and self-disclosure.

Similarly, we find that the role of perceived control is more pronounced in the US. Perceived control predicted all three types of self-disclosure in the US model but predicted only one type (i.e., amount) in the Korea model and none in the Singapore model. While the need for control seems to be universal [8], personal control is more critical in individualistic cultures than in collectivistic cultures [38] because the notions of agency, autonomy, and perceived control are more prominent in individualistic cultures than in collectivistic cultures. It is worthwhile to note that perceived control is predicted by collaborative strategies in the US model, whereas it is predicted by audience control strategies in Singapore and South Korea. The findings suggest that US Facebook users are likely to have a higher level of perceived control when they themselves (together with their friends) engage in privacy actions. On the contrary, in Singapore and South Korea, perceived control is more likely to be determined by privacy control mechanisms/affordances (i.e., privacy preference settings to control audience groups) provided by the service provider (i.e., Facebook).

[7]Future work could employ experimental designs or longitudinal studies to further test the causal relationships implied in this study.

Overall, the findings highlight methodological precautions and implications when conducting intercultural privacy research. The practical implications of this study are that researchers should do privacy studies in a single country only (and preferably only with long-time residents), or should be methodologically very cautious when doing multi-country studies. Similarly, insights about social media users found in a single country should not be automatically generalized to those in other countries unless proper testing of assumptions and modification of measurement and research models are performed. For instance, when designing or developing new technical mechanisms or policies to support social media users' privacy management, user testing/evaluation should be done by including culturally diverse participants, and by employing culturally-modified instruments, given the cultural sensitivity of privacy management found in this study. One may even argue that the appropriate privacy mechanisms differ per cultural setting, which suggests a need for localized privacy interfaces. We also suggest that the survey instrument developed and validated in this study is useful when assessing multiple aspects of collective privacy management strategies. Because much of users' private information is co-owned and co-managed in social media and computer-supported collaborative work (CSCW) settings, the survey instrument can be utilized to examine how users of social computing technologies manage collective privacy through different strategies. However, as noted above, we also recommend that researchers should be aware of the cultural sensitivity of our survey questions.

7 LIMITATIONS AND DIRECTIONS FOR FUTURE STUDIES

Like many multinational and intercultural studies, we explain cultural variations in privacy using the notion of national cultures, such as individualism/collectivism. However, there are ongoing debates about using nations as proxies for culture [75], and large multiethnic nations such as the US and Singapore are a reminder of the limitations of this assumption. In research, cultural orientations such as individualism vs. collectivism, independent vs. interdependent self-construal, and allocentrisim vs. ideocentrism can be measured at multiple levels [90, 91]. In our article, we choose Hofstede's definition that "culture is the collective programming of the mind that distinguishes the members of one group from others" [44, p. 6]. In this context, the group is at the nation level because national cultures, which people acquire in their earliest youth, are much deeper rooted in the human mind than other group level cultures, such as school cultures, organizational cultures, and so on.

The reason why our study conceptualizes individualism/collectivism as a characteristic at the country level, is that individualism and collectivism are two separate dimensions at the individual level (i.e., individuals carry both individualism and collectivism such that one person can be more individualistic and more collectivistic at the same time) [53, 92, 109]. At the country level, on the other hand, it is a unidimensional construct because a country can only be either individualistic or collectivistic [54]. Given that our study's focus is on methodological concerns when examining macro-level differences, national cultures rather than individual-level cultural orientations are deemed more appropriate for our study.

In privacy research, it has been consistently shown that users in individualistic national cultures have higher levels of privacy concerns than in collectivistic national cultures, and are thus less likely to disclose personal information and more likely to adopt privacy management behaviors [27, 61, 70, 72, 86, 100]. We thus follow the same way to use individualism to distinguish the cultures in the three countries, US, Singapore, and South Korea. As noted earlier, according to Hofstede's cultural framework, US scores 91 on individualism, while Singapore and South Korea score 20 and 18, respectively. Other cross-cultural research also shows that US has a relatively individualistic culture and Singapore and South Korea have a relatively collectivistic culture [22, 27, 28, 76, 81, 88]. Because culture consists of different values, orientations, norms,

and characteristics that can be assessed at the microlevel and macrolevel, we suggest that future studies should assess the construct of culture at both the national level and the individual level to achieve a more holistic understanding on the cultural influence on privacy management.

In our study, we selected three countries (US, Singapore, and South Korea) to represent distinct cultural values such as individualism and collectivism [44]. Indeed, previous work has shown that differences in cultural values manifest themselves in unique approaches to privacy [27, 61, 70, 72, 86, 100], and that these countries can indeed serve as representatives for their respective cultures when it comes to such effects [22, 27, 62, 88]. However, this does not rule out the possibility that some of the differences we find between countries are in fact not cultural differences, but instead caused by certain omitted variables that vary between our samples of these countries. We tested for two possible omitted variables: gender and age. We first established measurement invariance for both of these variables, and then considered structural effects. Gender did not differ significantly between our country samples, and thus could not have explained the between-country differences in the regression coefficients. Age did differ between our country samples, but none of the regression coefficients in our models changed by more than 10% when the samples were resampled in a way that equalizes the distribution of age—except one.[8] For more robust findings, future studies should consider using additional factors (e.g., education, being a privacy victim) as covariates that may intrinsically vary between countries [64]. Sampling from more countries to represent diverse cultures is also recommended.

In this study, we focus on self-disclosure because it is the most common type of disclosure in the context of Facebook. Numerous studies (including intercultural privacy studies) have examined the relationship between privacy and self-disclosure [25, 48, 57, 58, 74, 106, 108], so we focus on the same construct to make our findings relevant to previous studies. However, SNSs users also share information about others, and future studies should broaden the concept to include this important aspect of information disclosure.

This study demonstrates cross-cultural differences in collective privacy management both in terms of the measurement model and predictive model. We point out methodological precautions that must be taken in multinational privacy research and suggest methodological approaches to address the problems. We suggest that more theoretical inquiries should be conducted to provide fuller explanations for cross-cultural differences in collective privacy management observed in this study. Whereas the study provides explanations for some research findings, there are a few results that may require additional research for further explanations.

8 CONCLUSION

Social media are widely used across cultures, and it is important to understand users' behavior in different cultures and countries. Given that privacy remains a primary factor that inhibits their use of social and collaborative technologies, it is imperative to know the types of privacy management strategies that users from different cultures prefer or selectively employ. With these insights, practitioners and designers would be able to develop effective privacy support mechanisms, privacy policies, and practices that are better suited for people from different cultures. The findings suggest that measurement can be a key barrier to our ability to understand privacy practices across cultures or to interpret the findings of cross-cultural studies with confidence. Hence, more concerted efforts must be taken to develop a robust collective privacy management model that can be used confidently across cultures.

[8]The coefficient of the effect of collective strategies on the amount of disclosure dropped by 28% in the resampled Singapore dataset, and was no longer significant.

APPENDIX

A MEASUREMENT ITEMS AND FACTOR LOADINGS

Construct	Items	Factor loading		
		KR	SG	US
Collaborative	My friends and I negotiate "rules of thumb" about sharing content concerning ourselves	0.795	0.814	0.878
	My friends and I agree on "rules of thumb" about sharing content concerning ourselves	0.749	0.870	0.838
	Prior to disclosing content, my friends and I discuss the appropriate privacy settings	0.865	0.878	0.924
	I ask for approval before disclosing content from those involved	0.845	0.838	0.820
	My friends ask for approval before uploading content concerning myself	0.893	0.86	0.898
	I discuss the appropriate privacy settings with my friends before creating a Facebook group	0.910	0.903	0.921
	I educate my friends about privacy issues	0.770	0.785	0.812
Corrective	I untag myself from photos my friends uploaded	0.849	0.789	0.885
	I ask friends to remove content concerning myself	0.927	0.797	0.951
	I delete content posted about me by my friends	0.933	0.905	0.912
	My friends untag themselves from photos I uploaded	0.821	0.810	0.887
	My friends ask me to remove content concerning themselves	0.841	0.741	0.847
	I advise my friends to remove content concerning themselves	0.896	0.805	0.844
	I advise my friends to untag themselves from photos others uploaded	0.879	0.802	0.879
Preventive	I make use of friend lists to restrict the audience of my posts to certain individuals	0.730	0.740	0.678
	I use secret groups to share content about my friends	0.654	0.566	0.660
	I allow my Facebook friends to view only the mutual friends they share with me	0.741	0.831	0.754
	I use the timeline review function to control what information appears on my timeline	0.621	0.756	0.806
Information control	Before posting on Facebook, I consider the audience that will read my post	0.909	0.705	0.845
	I adjust the content of my post based on who I think will see it	0.883	0.890	0.732
	I limit what I share on Facebook to only what is appropriate for all of my friends to see	0.673	0.877	0.738

Construct	Items	Factor loading		
		KR	SG	US
Network management	I never accept invitation of people whom I never met before	0.856	0.795	0.827
	When I use Facebook, I ignore people whom I never heard of and who try to contact me	0.980	0.911	0.927
	I don't use Facebook to make contact with people whom I never heard of	0.882	0.810	0.694
Audience control	I adjust the privacy settings to control who can view my profile on Facebook	0.781	0.890	0.873
	I adjust the privacy settings to control who can view my posts on Facebook	0.914	0.879	0.840
	I adjust the privacy settings to control who can contact me using Facebook	0.927	0.832	0.858
	I adjust the privacy settings to control who can post on my timeline	0.922	0.956	0.921
	I adjust the privacy settings to control who can see my timeline	0.914	0.904	0.947
	I adjust the privacy settings to control tags that people add and tagging suggestions	0.815	0.938	0.870
Self-disclosure (Amount)	I frequently talk about myself on Facebook	0.868	0.862	0.803
	I often discuss my feelings about myself on Facebook	0.917	0.931	0.820
	I usually write about myself extensively on Facebook	0.927	0.890	0.856
	I often express my personal beliefs and opinions	0.681	0.805	0.839
	I disclose my close relationship with other people on Facebook	0.660	0.705	0.712
	I often disclose my concerns and fears on Facebook	0.805	0.763	0.774
Self-disclosure (Accuracy)	My postings on Facebook about my feelings, emotions, and experiences are always accurate self-perceptions	0.894	0.808	0.893
	I always feel completely sincere when reveal my own feelings and experiences on Facebook	0.904	0.756	0.806
Self-disclosure (Valence)	I often reveal more undesirable things about myself than desirable things on Facebook	0.901	0.835	0.822
	I usually disclose negative things about myself on Facebook	0.947	0.943	0.926
	I normally reveal my "bad" feelings I have about myself on Facebook	0.885	0.948	0.898

Notes: Factor loadings are standardized and based on CFA for each country sample.

B INTERCORRELATIONS AMONG ALL LATENT FACTORS

	M (SD)	1	2	3	4	5	6	7	8	9
1. Collaborative	3.824 (1.467)	**.861**								
2. Corrective	2.695 (1.332)	.418	**.878**							
3. Preventive	4.151 (1.278)	.655	.405	**.719**						
4. Information control	5.496 (.979)	.350	.112	.482	**.803**					
5. Network management	5.281 (1.412)	− .010	− .026	.150	.293	**.858**				
6. Audience control	5.118 (1.273)	.216	.088	.418	.331	.303	**.900**			
7. Amount	3.264 (1.390)	.347	.265	.310	− .035	− .142	.036	**.819**		
8. Accuracy	3.919 (1.368)	.141	.070	.172	.146	.009	.141	.591	**.852**	
9. Valence	2.571 (1.414)	.295	.403	.278	− .079	− .096	.008	.656	.419	**.903**

Notes: The bold numbers in the diagonal row are square roots of the average variance extracted (AVE).

C SUMMARY OF PREVIOUS STUDIES RELATED TO PRIVACY, SELF-DISCLOSURE, AND PRIVACY/INFORMATION CONTROL

Study	Method	Key findings
Acquisti and Gross [1]	Survey ($N = 294$) with data mining, college students in the US	Privacy concerns is a weak predictor of actual privacy-related information disclosure on Facebook. Privacy concerned individuals join Facebook and reveal great amounts of personal information.
Brandtzæg, Lüders, M. and Skjetne [13]	In-depth interviews ($N = 16$) and explorative usability tests, Norwegian participants	Having too many Facebook "friends" and having access to different social capital disrupt the sharing process due to experiences of social surveillance, context collapse, and distributed control of interpersonal privacy.
Cao et al. [16]	A systematic review of previous SNS research published in information systems journals (2004–2013)	Several key themes emerged. Privacy is an important factor related to trust and interpersonal relationship.
Cheung, Lee, and Chan [25]	Survey ($N = 405$), undergraduate students in Hong Kong	Social influence is the strongest factor affecting self-disclosure in social networking sites, followed by perceived benefits. However, perceived privacy risk does not have any significant impact on self-disclosure.

Study	Method	Key findings
Christofides, Muise and Desmarais [29]	Survey ($N = 343$), Undergraduate students in Canada	Information disclosure and control on Facebook are different processes that are affected by different aspects of personality. Information disclosure and information control were not significantly correlated. While disclosure was significantly predicted by the need for popularity, levels of trust and self-esteem predicted information control.
Christofides, Muise and Desmarais [30]	Survey ($N = 573$), 288 Canadian adolescents and 285 adults	Differences in information disclosure and privacy behavior between young and old Facebook users were found. Adolescents reported disclosing more information on Facebook and using the privacy settings less than adults.
Debatin et al. [34]	Survey ($N = 119$), US college students and in-depth interviews ($N = 8$)	Users claimed to understand privacy issues, yet reported uploading large amounts of personal information. Risks to privacy invasion were ascribed more to others than to the self, a phenomenon related to the third-person effect.
Dienlin and Metzer [35]	Survey ($N = 1156$) nationally representative Facebook users in the US	Self-disclosure and self-withdrawal (e.g., content removal) are distinct from each other. Privacy benefits increased self-disclosure whereas privacy self-efficacy positively predicted self-withdrawal. Privacy concern has significant effects on disclosure (negative effect) and withdrawal (positive effect).
Gross and Acquisti [41]	Data mining of US university students' Facebook profiles ($N = 4540$)	Facebook users generally provided personal data. Limiting privacy preferences are hardly used; only a small number of members change the default privacy preferences, which are set to maximize the visibility of users' profiles.
Hargittai and Marwick [43]	Focus-group interviews ($N = 40$), US university students	Contrary to the notion of privacy paradox, young adults understand and care about the potential risks associated with disclosing information online and engage in at least some privacy-protective behaviors on social media. However, they feel that once information is shared, it is ultimately out of their control due to the networked nature of privacy online.

Study	Method	Key findings
Hajil and Lin [42]	Survey ($N = 500$), college students in the US	Perceived control has positive effects on information-sharing behavior in Facebook by reducing perceived privacy risk and increasing positive attitude toward information sharing.
Joinson et al. [48]	Study 1: Survey ($N = 759$), Online panelists Study 2: Experiment ($N = 180$)	Participants' dispositional privacy concerns, as well as their level of trust in the requestor of personal information, and perceived privacy during the interaction, predicted whether or not they acceded to the request for personal information.
Keith et al. [49]	Experiments, Study 1 ($N = 509$) US college students Study 2 ($N = 380$) US college students and their acquaintances	Self-efficacy has a direct impact on mobile app users' initial trust in location-based app vendors, as well as their perceived risk of disclosing information. Perceived risk negatively influences information disclosure.
Posey et al. [86]	Survey ($N = 529$), British and French working professionals	Positive social influence to use an online community increases online community self-disclosure; reciprocity increases self-disclosure; online community trust increases self-disclosure; and privacy risk beliefs decrease self-disclosure. Meanwhile, a tendency toward collectivism increases self-disclosure.
Special and Li-Barber [96]	Survey ($N = 127$), US undergraduate students	Levels of self-disclosure, but not privacy levels, were associated with greater levels of satisfaction with Facebook. Females have higher privacy settings on Facebook than males.
Stutzman et al. [102]	Longitudinal analysis of panel data of CMU Facebook users ($n =$ over 20,000)	Over time Facebook users exhibited increasingly privacy-seeking behavior, progressively decreasing the amount of personal data shared publicly with unconnected profiles in the same network.
Tsay-Vogel et al. [112]	Survey ($N = 2789$), US undergraduate students	This study examines the effects of Facebook use on privacy perceptions and self-disclosure behaviors across a 5-year period from 2010 to 2015. Findings support the socializing role of Facebook in cultivating more relaxed privacy attitudes, subsequently increasing self-disclosure in both offline and online contexts.
Zlatolas et al. [124]	Survey ($N = 828$), Facebook users in Slovenia	Privacy control has a positive indirect effect on self-disclosure on Facebook by reducing privacy concern.

Notes: This is not an exhaustive list of privacy studies, and we only summarize the findings related to our study.

REFERENCES

[1] Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies*. George Danezis and Philippe Golle (Eds.), Springer Berlin, 36–58. doi:10.1007/11957454_3

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

[3] Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brook, Cole Publishing Company, Monterey, CA.

[4] Irwin Altman. 1976. Privacy: A conceptual analysis. *Environment and Behavior* 8, 1 (March 1976), 7–29. doi:10.1177/001391657600800108

[5] Irwin Altman. 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues* 33, 3 (July 1977), 66–84. doi:10.1111/j.1540-4560.1977.tb01883.x

[6] Irwin Altman, Anne Vinsel, and Barbara B. Brown. 1981. Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Psychology* 14, 1 (December 1981), 107–160. doi:10.1016/S0065 2601(08)60371-8

[7] Pauline Anthonysamy, Awais Rashid, James Walkerdine, Phil Greenwood, and Georgios Larkou. 2012. Collaborative privacy management for third-party applications in online social networks. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, ACM, New York, NY, 5–9. doi:10.1145/2185354.2185359

[8] Albert Bandura. 1997. *Self-efficacy: The Exercise of Control*. W. H. Freeman, New York.

[9] Vladlena Benson, George Saridakis, and Hemamaali Tennakoon. 2015. Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People* 28, 3 (August 2015), 426–441. doi:10.1108/ITP-10-2014-0232

[10] Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, and Gorrell Cheek. 2009. Social applications: Exploring a more secure framework. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 2–11. doi:10.1145/1572532.1572535

[11] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, ACM, New York, NY, 1563–1572. doi:10.1145/1753326.1753560

[12] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2010. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (May 2013), 340–347. doi:10.1177/1948550612455931

[13] Petter Bae Brandtzaeg, Marika Lüders, and Jan Haavard Skjetne. 2010. Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction* 26, 11–12 (November 2010), 1006–1030. doi:10.1080/10447318.2010.516719

[14] Barbara M. Byrne. 1989. Multigroup comparisons and the assumption of equivalent construct validity across groups: Methodological and substantive issues. *Multivariate Behavioral Research* 24, 4 (December 1989), 503–523. doi:10.1207/s15327906mbr2404_7

[15] Donald Thomas Campbell and Donald William Fiske. 1959. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin* 56, 2 (March 1959), 81–105. doi:10.1037/h0046016

[16] Jinwei Cao, Kamile Asli Basoglu, Hong Sheng, and Paul Benjamin Lowry. 2015. A systematic review of social networking research in information systems. *Communication of the Association for Information Systems* 36, 1 (May 2015), 727–758.

[17] Jinwei Cao and Andrea Everard. 2007. Influence of culture on attitude towards instant messaging: Balance between awareness and privacy. In *Proceedings of the Human-Computer Interaction: Interaction Platforms and Techniques (HCI'07). Lecture Notes in Computer Science*. Julie A. Jacko (Eds.), 236–240. doi: 10.1007/978-3-540-73107-8_26

[18] Jinwei Cao and Andrea Everard. 2008. User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management* 11, 2 (April 2008), 30–57. doi:10.1080/1097198X.2008.10856466

[19] Barbara Carminati and Elena Ferrari. 2008. Privacy-aware collaborative access control in web-based social networks. In *Data and Applications Security XXII 5094*. Springer, Berlin, 81–96. doi:10.1007/978-3-540-70567-3_7

[20] Barbara Carminati, Elena Ferrari, and Andrea Perego. 2009. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security* 13, 1 (December 2009), 1–40. doi: 10.1145/1609956.1609962

[21] Fang Fang Chen. 2008. What happens if we compare chopsticks with forks? The impact of making inappropriate comparisons in cross-cultural research. *Journal of Personality and Social Psychology* 95, 5 (November 2008), 1005–1018. doi:10.1037/a0013193

[22] Jim Qingjun Chen, Ruidong Zhang, and Jaejung Lee. 2013. A cross-culture empirical study of m-commerce privacy concerns. *Journal of Internet Commerce* 12, 4 (November 2013), 348–364. doi:10.1080/15332861.2013.865388

[23] Xiao-Ping Chen and Chao C. Chen. 2004. On the intricacies of the Chinese guanxi: A process model of guanxi development. *Asia Pacific Journal of Management* 21, 3 (September 2004), 305–324. doi:10.1023/B:APJM.0000036465.19102.d5

[24] Yunan Chen and Heng Xu. 2013. Privacy management in dynamic groups: Understanding information privacy in medical practices. In *Proceedings of the 2013 Conference on Computer-Supported Cooperative Work*. ACM, New York, NY, 541–552. doi:10.1145/2441776.2441837

[25] Christy Cheung, Zach W.Y. Lee, and Tommy K.H. Chan. 2015. Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research* 25, 2 (April 2015), 279–299. doi:10.1108/IntR-09-2013-0192

[26] Hichang Cho and Anna Filippova. 2016. Networked privacy management in Facebook: A mixed-methods and multinational study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, New York, NY, 503–514. doi:10.1145/2818048.2819996

[27] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. A multinational study on online privacy: Global concerns and local responses. *New Media & Society* 11, 3 (May 2009), 395–416. doi:10.1177/1461444808101618

[28] Jayoung Choi and Loren V. Geistfeld. 2004. A cross-cultural investigation of consumer e-shopping adoption. *Journal of Economic Psychology* 25, 6 (December 2004), 821–838. doi:10.1016/j.joep.2003.08.006

[29] Emily Christofides, Amy Muise, and Serge Desmarais. 2009. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology and Behavior* 12, 3 (June 2009), 341–345. doi:10.1089/cpb.2008.0226

[30] Emily Christofides, Amy Muise, and Serge Desmarais. 2012. Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science* 3, 1 (January 2012), 48–54. doi:10.1089/cyber.2010.0087

[31] Karina Davidson and Kenneth Prkachin. 1997. Optimism and unrealistic optimism have an interacting impact on health-promoting behavior and knowledge changes. *Personality and Social Psychology Bulletin* 23, 6 (June 1997), 617–625. doi:10.1177/0146167297236005

[32] Marco De Boni and Martyn Prigmore. 2002. Cultural aspects of internet privacy. In *Proceedings of the UKAIS Conference*. 40–46. doi:10.1.1.14.6032&rep=rep1

[33] Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35, 1(June 2014), 444–454. doi:10.1016/j.chb.2014.03.010

[34] Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, 1 (December 2009), 83–108. doi:10.1111/j.1083-6101.2009.01494X

[35] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* 45, 3 (April 2015), 285–297. doi:10.1002/ejsp.2049

[36] Dimiter M. Dimitrov. 2010. Testing for factorial invariance in the context of construct validation. *Measurement and Evaluation in Counseling and Development* 43, 2 (July 2010), 121–149. doi:10.1177/0748175610373459

[37] Paul Dourish and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction* 21, 3 (September 2006), 319–342. doi:10.1207/s15327051hci2103_2

[38] P. Christopher Earley. 1993. East meets West meets Mideast: Further explorations of collectivistic and individualistic work groups. *Academy of Management Journal* 36, 2 (April 1993), 319–348. doi:10.2307/256525

[39] Nicole B. Ellison, Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy online*. Sabine Trepte and Leonard Reinkcke (Eds.), Springer, Berlin, 19–32. doi:10.1007/978-3-642-21521-6_3

[40] David Gefen, Detmar Straub, and Marie-Claude Boudreau. 2000. Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems* 4, 1 (October 2000), 607–612.

[41] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. ACM, New York, NY, 71–80. doi:10.1145/1102199.1102214

[42] Nick Hajli and Xiaolin Lin. 2016. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics 133*, 1 (January 2016), 111–123. doi:10.1007/s10551-014-2346-x

[43] Eszter Hargittai and Alice Marwick. 2016. What can I really do? Explaining the privacy paradox with online apathy. *International Journal of Communication* 10, 1 (July 2016), 3737–3757. http://ijoc.org/index.php/ijoc/article/view/4655/1738

[44] Geert Hofstede H, Gert Jan Hofstede, and Michael Minkov. 2010. *Cultures and Organizations: Software of the Mind* (3th ed.). McGraw Hill Professional, New York, NY.
[45] Yongick Jeong and Yeuseung Kim. 2017. Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior* 69, 1 (April 2017), 302–310. doi:10.1016/j.chb.2016.12.042
[46] Yong Gu Ji, Hwan Hwangbo, Ji Soo Yi, P. L. Patrick Rau, Xiaowen Fang, and Chen Ling. 2010. The influence of cultural differences on the use of social network services and the formation of social capital. *International Journal of Human-Computer Interaction* 26, 11–12 (November 2010), 1100–1121. doi:10.1080/10447318.2010.516727
[47] Haiyan Jia and Heng Xu. 2016. Autonomous and interdependent: Collaborative privacy management on social networking sites. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 4286–4297. doi:10.1145/2858036.2858415
[48] Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. Privacy, trust, and self-disclosure online. *Human-Computer Interaction* 25, 1 (February 2010), 1–24. doi:10.1080/07370020903586662
[49] Mark J. Keith, Jeffry S. Babb, Paul Benjamin Lowry, Christopher P. Furner, and Amjad Abdullat. 2015. The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*. 25, 6 (December 2015), 637–667. doi:10.1111/isj.12082
[50] David Kenny. (Jan 2018). Multiple Latent Variable Models: Confirmatory Factor Analysis. Retrieved January 17, 2018 from http://davidakenny.net/cm/mfactor.htm.
[51] Dan J. Kim. 2008. Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems* 24, 4 (April 2008), 13–45. doi:10.2753/MIS0742-1222240401
[52] Kyung-Hee Kim and Haejin Yun. 2007. Crying for me, crying for us: Relational dialectics in a Korean social network site. *Journal of Computer-Mediated Communication* 13, 1 (October 2007), 298–318. doi: 10.1111/j.1083-6101.2007.00397.x
[53] Uichol Kim, Harry Charalambos, Triandis, Çiğdem Kâğitçibaşi, Sang-Chin Choi, and Gene Yoon. 1994. *Individualism and Collectivism: Theory, Method, and Applications*. Sage Publications, Thousand Oaks, CA.
[54] Bradley L. Kirkman, Kevin B. Lowe, and Cristina B. Gibson. 2006. A quarter century of culture's consequences: A review of empirical research incorporating Hofstede's cultural values framework. *Journal of International Business Studies* 37, 3 (May 2006), 285–320. doi:10.1057/palgrave.jibs.8400202
[55] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12 (December 2013), 1144–1162. doi:10.1016/j.ijhcs.2013.06.003
[56] Jan Kolter, Thomas Kernchen, and Günther Pernul. 2010. Collaborative privacy management. *Computers and Security* 29, 5 (2010), 580–591. doi: 10.1016/j.cose.2009.12.007
[57] Hanna Krasnova, Elena Kolesnikova, and Oliver Guenther. 2009. It won't happen to me!: Self-disclosure in online social networks. In *Proceedings of AMCIS 2009*, AIS/ICIS, Atlanta, Georgia, 343–354. doi:10.7892/boris.47460
[58] Hanna Krasnova, Natasha F. Veltri, and Oliver Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering* 4, 3 (June 2012), 127–135. doi:10.1007/s12599-012-0216-6
[59] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 3217–3226. doi:10.1145/1978942.1979420
[60] Airi Lampinen, Fred Stutzman, and Markus Bylund. 2011. Privacy for a networked world: Bridging theory and design. In *Proceedings of CHI'11 Extended Abstracts on Human Factors in Computing Systems*. ACM, New York, NY, 2441–2444. doi:10.1145/1979742.1979579
[61] Yao Li, Alfred Kobsa, Bart P. Knijnenburg, and M.-H. Carolyn Nguyen. 2017. Cross-cultural privacy prediction. In *Proceedings on Privacy Enhancing Technologies* 3, 2 (April 2017), 113–132. doi:10.1515/popets-2017-0019
[62] Sun Sun Lim, Hichang Cho, and Milagros Rivera Sanchez. 2009. Online privacy, government surveillance and national ID cards. *Communications of the ACM* 52, 12 (December 2009), 116–120. doi:10.1145/1610252.1610283
[63] Heather Richter Lipford, Andrew Besmer, and Jason Watson. 2008. Understanding Privacy Settings in Facebook with an Audience View. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, USENIX Association Berkeley, CA, 1–8.
[64] Paul Lowry, Jinwei Cao, and Andrea Everard. 2011. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27, 4 (April 2011), 163–200. doi:10.2753/MIS0742-1222270406
[65] David Lyon. 2001. *Surveillance Society: Monitoring Everyday Life*. Open University, Philadelphia, PA.
[66] Stephen T. Margulis. 2003. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59, 2 (June 2003), 411–429. doi:1111 1540 4560 00071

[67] Bryan A. Marshall, Peter W. Cardon, Daniel T. Norris, Natalya Goreva, and Ryan D'Souza. 2008. Social networking websites In India and the United States: A cross-national comparison of online privacy and communication. *Issues in Information Systems* IX, 2 (2008), 87–94.

[68] Alice E. Marwick and Danah Boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1 (February 2011), 114–133. doi:10.1177/1461444810365313

[69] Alice E. Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7 (November 2014), 1051–1067. doi:10.1177/1461444814543995

[70] Sandra J. Milberg, Sandra J. Burke, H. Jeff Smith, and Ernest A. Kallman. 1995. Values, personal information, privacy and regulatory approaches. *Communications of the ACM* 38, 12 (December 1995), 65–74. doi:10.1145/219663.219683

[71] Sandra J. Milberg, H. Jeff Smith, and Sandra J. Burke. 2000. Information privacy: Corporate management and national regulation. *Organization Science* 11, 1 (January 2000), 35–57. doi:10.1287/orsc.11.1.35.12567

[72] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information System* 23, 2 (March 2014), 103–125. doi:10.1057/ejis.2013.17

[73] Masahiko Mizutani, James Dorsey, and James H. Moor. 2004. The Internet and Japanese conception of privacy. *Ethics and Information Technology* 6, 2 (June 2004), 121–128. doi:10.1023/B:ETIN.0000047479.12986.42

[74] Ricarda Moll, Stephanie Pieschl, and Rainer Bromme. 2014. Trust into collective privacy? The role of subjective theories for self-disclosure in online communication. *Societies* 4, 4 (December 2014), 770–784. doi:10.3390/soc4040770

[75] Daphna Oyserman, Heather M. Coon, and Markus Kemmelmeier. 2002. Rethinking individualism and collectivism: Evaluation of theoretical assumptions and meta-analyses. *Psychology Bulletin* 128, 1 (January 2002), 3–72. doi:10.1037//0033-2909.128.1.3

[76] Zafer D. Ozdemir, John H. Benamati, and H. Jeff Smith. 2016. A cross-cultural comparison of information privacy concerns in Singapore, sweden and the united states. In *Proceedings of the 18th Annual International Conference on Electronic Commerce: E-Commerce in Smart Connected World (ICEC'16)*. ACM, New York, NY, 4–9. doi:10.1145/2971603.297160

[77] Xinru Page, Bart P. Knijnenburg, and Alfred Kobsa. 2013. FYI: Communication style preferences underlie differences in location-sharing adoption and usage. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'13)*. ACM, New York, NY, 153–162. doi:10.1145/2493432.2493487

[78] Xinru Page, Alfred Kobsa, and Bart P. Knijnenburg. 2012. Don't disturb my circles! boundary preservation is at the center of location-sharing concerns. In *Proceedings of the 6th International AAAI Conference on Weblogs and Social Media*. AAAI Press, Palo Alto, CA, 266–273.

[79] Xinru Page, Karen Tang, Fred Stutzman, and Airi Lampinen. 2013. Measuring networked social privacy. In *Proceedings of the 2013 Conference on Computer-Supported Cooperative Work Companion*. ACM, New York, NY, 315–320. doi:10.1145/2441955.2442032

[80] Leysia Palen and Paul Dourish. 2003. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 129–136. doi:10.1145/642611.642635

[81] Cheol Park and Jong-Kun Jun. 2003. A cross-cultural comparison of internet buying behavior: Effects of internet usage, perceived risks, and innovativeness. *International Marketing Review* 20, 5 (October 2003), 534–553. doi:10.1108/02651330310498771

[82] Sandra Petronio. 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory* 1, 4 (November 1991), 311–335. doi:10.1111/j.1468-2885.1991.tb00023.x

[83] Sandra Petronio. 2012. *Boundaries of Privacy*. Sunny Press, Albany, NY.

[84] Sandra Petronio. 2015. Communication privacy management theory. In *The International Encyclopedia of Interpersonal Communication*. John Wiley & Sons, Hoboken, New Jersey. doi: 10.1002/9781118540190.wbeic132

[85] Sandra Petronio. 2012. *Boundaries of Privacy: Dialectics of Disclosure*. Sunny Press, Albany, NY.

[86] Clay Posey, Paul Benjamin Lowry, Tom L. Roberts, and T. Selwyn Ellis. 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 System* 19, 2 (April 2010), 181–195. doi:10.1057/ejis.2010.15

[87] Fred Rothbaum, John R. Weisz, and Samuel S. Snyder. 1982. Changing the world and changing the self: A two-process model of perceived control. *Journal of Personality and Social Psychology* 42, 1 (January 1982), 5–36. doi:10.1037/0022-3514.42.1.5

[88] Jian Rui and Michael A. Stefanone. 2013. Strategic self-presentation online: A cross-cultural study. *Computers in Human Behavior* 29, 1 (January 2013), 110–118. doi:10.1016/j.chb.2012.07.022

[89] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, doi:10.1145/3025453.3025926

[90] Theodore M. Singelis. 1994. The measurement of independent and interdependent self-construals. *Personality and Social Psychology Bulletin* 20, 5 (October 1994), 580–591. doi: 10.1177/0146167294205014

[91] Theodore M. Singelis and William J. Brown. 1995. Culture, self, and collectivist communication linking culture to individual behavior. *Human Communication Research* 21, 3 (March 1995), 354–389. doi: 10.1111/j.1468-2958.1995.tb00351.x

[92] Theodore M. Singelis, Harry C. Triandis, Dharm P. S. Bhawuk, and Michele J. Gelfand. 1995. Horizontal and vertical dimensions of individualism and collectivism: A theoretical and measurement refinement. *Cross-Culture Research* 29, 3 (August 1995), 240–275. doi: 10.1177/106939719502900302

[93] Edith G. Smit, Guda Van Noort, and Hilde A.M. Voorveld. 2014. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behavior in Europe. *Computers in Human Behavior* 32, (March 2014), 15–22. doi: 10.1016/j.chb.2013.11.008

[94] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20, 2 (June 1996), 167–196. doi: 10.2307/249477

[95] H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35, 4 (December 2011), 989–1015. doi: 10.2307/41409970

[96] Whitney P. Special and Kirsten T. Li-Barber. 2012. Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior* 28, 2 (March 2012), 624–630. doi:10.1016/j.chb.2011.11.008

[97] Anna Cinzia. Squicciarini, Heng Xu, and Xiaolong Zhang. 2011. CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology* 62, 3 (March 2011), 521–534. doi:10.1002/asi.21473

[98] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th International Conference on World Wide Web*. ACM, New York, NY, 521–530. doi:10.1145/1526709.1526780

[99] Jan-Benedict E. M. Steenkamp and Hans Baumgartner. 1998. Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research* 25, 1 (June 1998), 78–90. doi:10.1086/209528

[100] Jan-Benedict E. M Steenkamp and Inge Geyskens. 2006. How country characteristic affect the perceived value of web sites. *Journal of Marketing* 70, 3 (July 2006), 136–150. doi:10.1509/jmkg.70.3.136

[101] Fred Stutzman, Robert Capra, and Jamila Thompson. 2011. Factors mediating disclosure in social network sites. *Computers in Human Behavior* 27, 1 (January 2011), 590–598. doi:10.1016/j.chb.2010.10.017

[102] Fred Stutzman, Ralph Gross, and Alessandro Acquisti. 2013. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality* 4, 2 (2013), 7–41.

[103] Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 1553–1562. doi:10.1145/1753326.1753559

[104] Frederic Stutzman and Woodrow Hartzog. 2012. Boundary regulation in social media. In *Proceedings of the ACM 2012 Conference on Computer-Supported Cooperative Work*. ACM, New York, NY, doi:10.1145/2145204.2145320

[105] Frederic Stutzman, Jessica Vitak, Nicole B. Ellison, Rebecca Gray, and Cliff Lampe. 2012. Privacy in interaction: Exploring disclosure and social capital in Facebook. In *Proceedings of the 6th International AAAI Conference on Weblogs and Social Media*. AAAI Press, Palo Alto, CA, 330–337.

[106] Stefano Taddei and Bastianina Contena. 2013. Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior* 29, 3 (May 2013), 821–826. doi:10.1016/j.chb.2012.11.022

[107] Jim C. Tam. 2000. Personal data privacy in the Asia pacific: A real possibility. In *Proceedings of the 10th Conference on Computers, Freedom and Privacy: Challenging the Assumptions*. ACM, New York, NY, 259–262. doi: 10.1145/332186.332296

[108] Sabine Trepte and Leonard Reinecke (Eds.). 2011. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer-Verlag, Berlin.

[109] Harry C. Triandis, Robert Bontempo, Hector Betancourt, Michael Bond, Kwok Leung, Abelando Brenes, James Georgas, C. Harry Hui, Gerardo Marin, Bernadette Setiadi, Jai B. P. Sinha, Jyoti Verma, John Spangenberg, Hubert Touzard, and Germaine de Montmollin. 1986. The measurement of the etic aspects of individualism and collectivism across cultures. *Australian Journal of Psychology* 38, 3 (May 1986), 257–267. doi:10.1080/00049538608259013

[110] Harry Charalambos Triandis, Robert Bontempo, Marcelo J. Villareal, Masaaki Asai, and Nydia Lucca. 1988. Individualism and collectivism: Cross-cultural perspectives on self-ingroup relationships. *Journal of Personality and Social Psychology* 54, 2 (February 1988), 323–338. doi:10.1037/0022-3514.54.2.323

[111] Harry Charalambos Triandis. 1995. *Individualism & Collectivism*. Westview Press, Boulder, Colorado.

[112] Mina Tsay-Vogel, James Shanahan, and Nancy Signorielli. 2016. Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society* 20, 1 (August 2016), 1–21. doi:10.1177/1461444816660731

[113] Jessica Vitak. 2012. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* 56, 4 (October 2012), 451–470. doi:10.1080/08838151.2012.732140

[114] Jessica Vitak, Pamela Wisniewski, Xinru Page, Airi Lampinen, Eden Litt, Ralf De Wolf, Patrick Gage Kelley, and Manya Sleeper. 2015. The future of networked privacy: Challenges and opportunities. In *Proceedings of the 18th ACM Conference Companion on Computer-Supported Cooperative Work & Social Computing*. ACM, New York, NY, doi:10.1145/2685553.2685554

[115] Jichuan Wang and Xiaoqian Wang. 2012. *Structural Equation Modeling: Applications Using Mplus*. John Wiley & Sons, Higher Education Press, Hoboken, New Jersey.

[116] Samuel D. Warren and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4, 5 (December 1890), 193–220. doi:10.2307/1321160

[117] Neil D. Weinstein. 1989. Optimistic biases about personal risks. *Science* 246, 4935 (December 1989), 1232–1233. doi:10.1126/science.2686031

[118] Alan F. Westin. 1967. *Privacy and Freedom*. Atheneum, New York.

[119] Lawrence R. Wheeless and Jams Grotz. 1976. Conceptualization and measurement of reported self-disclosure. *Human Communication Research* 2, 4 (June 1976), 338–346 doi:10.1111/j.1468-2958.1976.tb00494.x

[120] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98, 1 (February 2017), 95–108. doi:10.1016/j.ijhcs.2016.09.006

[121] Pamela Wisniewski, Bart P. Knijnenburg, and H. Richter Lipford. 2014. Profiling Facebook users' privacy behaviors. In *SOUPS2014 Workshop on Privacy Personas and Segmentation*, 1–6

[122] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 609–618. doi:10.1145/2207676.2207761

[123] Heng Xu. 2012. Reframing privacy 2.0 in online social network. *University of Pennsylvania Journal of Constitutional Law* 14, 4 (March 2012), 1077–1102.

[124] Lili Nemec Zlatolas, Tatjana Welzer, Marjan Heričko, and Marko Hölbl. 2015. Privacy antecedents for SNS self-disclosure: The case of facebook. *Computers in Human Behavior* 45, 1 (April 2015), 158–167. doi:10.1016/j.chb.2014.12.012

Received March 2017; revised January 2018; accepted March 2018