

Cultural Differences in the Effects of Contextual Factors and Privacy Concerns on Users' Privacy Decision on Social Networking Sites

Yao Li (corresponding author):

Affiliation: School of Modeling, Simulation and Training, University of Central Florida

E-mail: yao.li@ucf.edu

Eugenia Ha Rim Rho

Affiliation: Department of Informatics, University of California, Irvine

E-mail: hrrho@uci.edu

Alfred Kobsa

Affiliation: Department of Informatics, University of California, Irvine

E-mail: kobsa@uci.edu

Abstract: Many social network sites (SNSs) have become available around the world and users' online social networks increasingly include contacts from different cultures. However, there is lack of investigation into the concrete cultural differences in the effects of contextual factors and privacy concerns on users' privacy decisions on social network sites (SNSs). The goal of this paper is to understand how contextual factors and privacy concerns cast different impact on privacy decisions, such as friend request decisions, information disclosure and perceived risk, in different countries. We performed a quantitative study through a large-scale online survey across the US, Korea and China to model the relationships between contextual factors, privacy concerns and privacy decisions. We find that the contextual influence and focus of privacy concerns vary between the individualistic and collectivistic countries in our sample. We suggest that multinational SNS service providers should consider different contextual factors and focus of privacy concerns in different countries and customize privacy designs and friend recommendation algorithms in SNSs in different countries.

KEYWORDS: Culture; privacy concern; context; information disclosure; social network sites

1 INTRODUCTION

Privacy is a global phenomenon. People in different cultures are universally aware and capable of regulating interpersonal privacy, but their specific perceptions and behaviors vary from culture to culture (Altman, 1975). Culture is about the "collective programming of the mind that distinguishes the members of one group from others" (Hofstede et al., 2010). People residing in the same cultures are guided by similar norms and legal systems embedded in shared beliefs, values and interests, which in return influence their perception and behavior. Thus, people's privacy behaviors are also deeply rooted within beliefs and values that are culturally distinct.

Today, a major focal point of privacy tensions is social networking sites (SNS). Billions of users share an enormous amount of personal information on SNSs to facilitate their online social interaction. This however threatens their privacy, as it makes users more accessible, visible and identifiable (Boyd & Ellison, 2007;

Gross & Acquisti, 2005). In reaction to this, users need to adjust their privacy decisions from time to time to keep certain personal information private (Strater & Lipford, 2008). Researchers have found that many users alter their privacy decisions based on the contextual factors, which describe the social settings where the information sharing happens, such as whom users share information with and what information is shared (Fogues et al., 2017; Nissenbaum, 2009). Users' privacy decisions are also influenced by their privacy concerns (Min, 2015; Min & Kim, 2014). When users find that information sharing does not conform to the prevailing context-specific norms, or become concerned with the risks of information sharing, they feel less comfortable disclosing information.

Many SNSs like Facebook, Twitter, and Instagram have become available worldwide since last decade. For example, as of April of 2019, Facebook has 300 million users in India, making it the leading country in Facebook use over the US, and another 100 million users spread in Brazil, Indonesia, Mexico, Philippines, Vietnam, Thailand, Turkey, UK and so on (*Facebook Users by Country / Statistic*, n.d.). Since many SNSs now can reach users worldwide and impact the social lives of large and diverse populations from different parts of the world, and since individual users' social networks increasingly include contacts from different cultures, an investigation of cultural differences in users' privacy decisions in SNSs is most warranted. First, most studies about the effects of contextual factors and privacy concerns on privacy decision are conducted in a single country and mostly in Western countries. It is unknown whether such contextual factors and privacy concerns play a role in countries with different cultures. Second, most previous cross-cultural privacy research focuses on in which culture users have higher levels of privacy concerns (H. Cho et al., 2009; Krasnova & Veltri, 2010; Milberg et al., 2000), or larger amount of information disclosure (S. E. Cho & Park, 2013; Miltgen & Peyrat-Guillard, 2014; Posey et al., 2010; Tsoi & Chen, 2011). Few has considered the contextual impact on privacy decisions, nor investigated the cultural differences in contextual impact on privacy decisions. Users in different cultures may respond differently to the same contextual factors due to different cultural norms and practices. Thus, it remains unexplored how users' privacy decision-making differs in the specific context in different countries with different cultural backgrounds. Third, as privacy concerns in SNSs involves multiple social aspects, such as the interactional and psychological aspects, in addition to informational aspect, it is still an open question whether users in different countries focus on different types of privacy concerns or not.

To fill these research gaps, our study aims to answer three research questions: 1) How does the contextual impact on privacy decisions in SNSs differ in different countries? 2) How does the impact of privacy concerns on privacy decisions in SNSs differ in different countries? 3) Are SNS users in different countries concerned with different aspects of privacy in online social interaction? Answers to these research questions are important as they enhance our understanding about the cultural differences that exist in users' privacy attitudes and behaviors. It will also inform the privacy design that would challenge the "one-size-fits-all" privacy support (Wilkinson et al., 2018) in contemporary SNSs like Facebook, a platform that is largely universal across countries.

We perform a large online survey across three countries – US, South Korea (short for Korea for the rest of the paper) and China. Based on the survey data, we build a model using factor analysis and multi-group Structural Equation Modeling to explore the country differences in contextual impact, different aspects of privacy concerns in online social interactions, and their effects on different types of privacy decisions. Our findings show that contextual factors indeed cast different effects on privacy decisions across the three countries, and that users in different countries focus on different aspects of privacy concerns, and thus have different preferences in privacy decisions in SNSs. We finally discuss the theoretical and design implications of our findings.

The paper is structured as following. In Section 2, we review the related literature in privacy decisions, contextual factors, privacy concern and cross-cultural privacy research. In Section 3, we propose a hypothesized model and specify each hypothesis in detail with theoretical justification. Section 4 describes how we deploy the cross-country survey study and how we analyze the survey data to test out model. In Section 5, we report the model testing results. We discuss the theoretical and design implications and the limitations of this study in Section 6-8. We conclude this study in Section 9.

2 LITERATURE REVIEW

2.1 Privacy Decisions

The rapid development of information technologies forces users to deal with an increasing number of privacy decisions in their daily online activities. Privacy decision refers to how users attempt to control information flows (Acquisti, 2012). It describes users' behavioral reactions in information sharing. In the use of SNSs, such decisions can range from configuring visibility of posts, accepting friend requests, self-censoring posts, to sharing personal details via messages. Substantial previous privacy studies have focused on information disclosure (Smith et al., 2011), which is one of the most frequent type of privacy decisions in the use of SNSs (Gross & Acquisti, 2005). For example, users maintain, expand and interact with their online social relationships through sharing personal information (Boyd & Ellison, 2007), particularly by creating online profiles, updating their status, sharing photos and videos, chatting with other SNS users, and commenting on information shared by others. When they encounter unwanted online social relationships or find the information too sensitive, they adjust their information disclosure to protect their privacy. Thus, users' privacy decisions change all the time and are subject to the impact of a number of personal and environmental factors (Acquisti et al., 2016; Alashoor et al., 2016).

2.1.1 Contextual Impact on Privacy Decisions

One privacy research stream suggests that privacy decisions are highly dependent on the context (Fogues et al., 2017; Nissenbaum, 2009). One of the most widely used theoretical work in this research stream is Nissenbaum's contextual integrity. According to the framework of Nissenbaum's contextual integrity (Nissenbaum, 2009), contextual integrity exists if the information flows according to the information norms governing the specific context. Context refers to "the structured social settings characterized by the activities, roles, relationships, structures, norms, rules, and internal values (goals, ends, purposes)". For instance, we

move in and out of distinct contexts in our daily life, such as from home to workplace, and from one social event to another social event. Context can be conceptualized by three parameters, actors (subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows). When these parameters change, the context changes. The information norms describe what types or nature of information sharing is appropriate, allowable or expected. In other word, the information norms regulate how certain type of information flows from actor(s) to actor(s). Information norms are context-specific, meaning that if the context changes, the information norms change. Information flow that is appropriate in one context may become inappropriate in another context. For example, it may be appropriate to share photos of one's social life with one's friends on Facebook, but not with one's employers (Hull et al., 2011). In this example, the information recipient changes from friends to employers. Thus, the norms of sharing medical information change.

Contextual integrity has been heavily discussed in prior studies that investigate the role of context in users' privacy attitude and behaviors on SNSs. A large number of these studies examine how concrete elements of context impact users' privacy decisions. Such elements of context operationalize the three context parameters in contextual integrity. They include the person or entity to be shared with, the type of information, sensitivity of the information and motivation of information sharing. For example, users are more likely to disclose information to close ties than to distant ties (Consolvo et al., 2005). Personal information, such as activity data (Bilogrevic et al., 2013), locations (i.e., bank, hotel, etc.) (Dong et al., 2015), and inappropriate content (i.e., drinking alcohol) (Fogues et al., 2017) are less shared on SNSs. Users are more likely to share their true information if they are driven by specific purposes, such as coordination and planning, than by random purposes, such as sharing for fun (Tang et al., 2010). Another majority of past studies has demonstrated the way social media collapse multiple contexts and bring together commonly distinct audiences by examining the context-relative information norms. For example, Lipford et al. (Lipford et al., 2009) reported that SNS users expected themselves to share their profiles, newsfeeds, and photos in one context, i.e., with close friends, when they were actually sharing in a more public context. Shklovski et al. (Shklovski et al., 2014) found that users perceived Facebook apps as simple consumer services that outfit their personal space, but these apps collected personal information to intentionally leak out of their personal space, i.e., to third-party entities.

2.1.2 Privacy Concern as a Predictor of Privacy Decisions

Besides contextual factors, privacy concern is also shown to be a primary predictor of privacy decisions (Min, 2015; Min & Kim, 2014). Privacy concern describes users' attitudes and beliefs about information privacy. It drives users to be more cautious in information sharing. For example, privacy concern negatively predicts users' information disclosure (Jiang et al., 2013; Min, 2015; Min & Kim, 2014; Son & Kim, 2008; Stewart & Segars, 2002), and positively influences how the person perceives risk in a specific situation (Malhotra et al., 2004). However, researchers also found that users' privacy concern is sometimes only a weak predictor of privacy decisions (Acquisti & Gross, 2006; Tufekci, 2008). Users' privacy behavior may not be in line with their stated privacy concerns (Acquisti & Gross, 2006).

Previous studies have also shown that privacy concerns in SNSs should not be limited to informational privacy, but extended to various aspects of online social interactions, such as interactional and psychological privacy (Karr-Wisniewski et al., 2011; Zhang et al., 2011). This is mostly because the privacy management in SNSs involve a significant amount of interpersonal boundary regulation, which is more complex than the privacy issues a business transaction could entail. In e-commerce use, privacy is mostly about managing factual personal information disclosure to organizations. Factual information privacy refers to one's ability to control identifiable personal information about oneself (Smith et al., 2011). However, SNS privacy is largely interpersonal, extending beyond factual information disclosure. For instance, users may be willing to share their identifiable information on SNSs, but may not want to be contacted by unwanted people. Such privacy issue is related with people's ability to control their interpersonal boundary with others, which is defined in Altman's boundary regulation theory (Altman, 1975) and Petronio's Communication Privacy Management theory (CPM) (Petronio, 2002) as interpersonal boundary regulation that requires people to coordinate and negotiate to optimally regulate each other's social interactions. Thus, SNS privacy concern is not limited to factual privacy, but also involves other aspects of online social interactions.

There has been an increasing amount of efforts in recent years to expand the conceptualization of privacy concerns in the context of SNSs. Generally, researchers have proposed interactional and psychological privacy in addition to factual privacy to describe users' privacy concerns in the use of SNSs. Interactional privacy is about users' ability to control their encounters with others (Burgoon et al., 1989). For instance, users may feel compelled by or uncomfortable with online social interaction with certain people. They may disable or limit interruptions from such people (Wisniewski et al., 2012). Such control meets their security, affiliation and intimacy needs, as well as avoids unwanted contact or involvement (Burgoon et al., 1989). Psychological privacy protects users from intrusions upon their thoughts, feelings, attitudes, and values (Burgoon et al., 1989). It includes one's freedom to express their views and to hide themselves from interference of others. For instance, users may want to be free from by others' interference when they share their thoughts, feelings, and values on SNSs (Zhang et al., 2011). Psychological privacy enables people to develop autonomy and self-identity (Burgoon et al., 1989).

The interactional and psychological privacy are crucial in the context of SNSs because SNSs remove the physical constrains of interpersonal information sharing and enrich the way one can be reached by and exposed to others (Zhang et al., 2011). For example, SNS users can be contacted through instant message, emails, search engines and friend recommendations by others on SNSs. Their thoughts, feelings, and values can be viewed by vast audience. This greatly increases the chance of unwanted contact and undesired influence of others. Interactional and psychological privacy have been captured in several conceptualizations of SNS privacy concerns. For example, Zhang et al. proposed a four-dimensional conceptualization of SNS privacy concerns, including interactional and psychological privacy in addition to factual information privacy (Zhang et al., 2011). Wisniewski et al. proposed five boundary types to conceptualize interpersonal privacy preferences in SNS, including interactional and disclosure privacy (P. Wisniewski et al., 2016). Dienlin and

Trepte applied three dimensions of privacy concern, including informational, social, and psychological privacy (Dienlin & Trepte, 2015).

2.3 National Culture and Privacy Decisions

In the recent decades, a growing body of privacy research has examined the relationships between national culture and privacy decisions. Culture is defined as the "collective programming of the mind that distinguishes the members of one group from others" (Hofstede et al., 2010). It is a collective concept, thus commonly used for tribes, nations and organizations. Cultural differences at nation level have been a highly popular research topic, as they highlight the differences between national populations (Hofstede et al., 2010; House et al., 2004; Schwartz, 1994). Despite there are considerable variances between individuals in the same countries, research has shown that people in the same national cultures exhibit certain differences when compared with other nations (Hofstede, 2011; Harry Charalambos Triandis, 1995).

Among the various country-level cultural differences that contrast national cultures, the majority relates the dichotomy of individualism versus collectivism (Oyserman et al., 2002; Schimmack et al., 2005; Harry C. Triandis et al., 1988). Collectivistic cultures emphasize that groups (i.e., family, tribe, country) bind and mutually obligate individuals, whereas individualistic cultures assume that individuals are independent of one another (Oyserman et al., 2002; Harry Charalambos Triandis, 1995). Researchers find that individualism is more prevalent in industrialized Western countries, whereas collectivism prevails in East Asian countries (Yamagishi & Yamagishi, 1994). Although researchers have also discovered other dimensions that can describe country-level cultural differences, such as uncertainty avoidance (Hofstede et al., 2010), harmony (Schwartz, 1994) and assertiveness (House et al., 2004), the majority of cross-cultural studies has been focusing on individualism versus collectivism.

In privacy research, researchers have argued that while people in different cultures are universally capable of regulating their social boundaries, their specific attitudes, behaviors and decisions may be quite different from culture to culture (Altman, 1977). For example, users in individualistic countries exhibit relatively higher levels of privacy concerns than those in collectivistic countries (H. Cho et al., 2009; Krasnova & Veltri, 2010; Wang, Norcie, et al., 2011), and are less likely to disclose personal information (S. E. Cho & Park, 2013; Posey et al., 2010; Tsoi & Chen, 2011), while more likely to adopt privacy management behaviors (Rui & Stefanone, 2013; Steenkamp & Geyskens, 2006). Additionally, people in collectivistic countries primarily use SNS to maintain their current relationships (Kim et al., 2011; Wang et al., 2015), and have more SNS friends who are either close ties (Tsoi & Chen, 2011) or offline connections belonging to the same social groups (S. E. Cho & Park, 2013). Users in individualistic countries are less likely to trust the SNS service providers (Wang, Norice, et al., 2011). They usually have a wider variety of social networks to find new friends with similar interests (Kim et al., 2011). They adopt more protective self-presentation (Rui & Stefanone, 2013), and generally feel more in control over disclosure (Krasnova & Veltri, 2010).

2.4 Research Gap

Based on the literature review, prior studies have shown that users' privacy decisions can be influenced by the contextual factors and their privacy concerns. However, the majority of these studies are conducted in a single country, and mostly in Western countries. It remains an open question whether the contextual factors and users' privacy concerns would similarly influence users' privacy decisions in different countries.

Additionally, research has shown that there exist significant cultural differences in users' privacy attitudes and behaviors. However, most of these studies focus on comparing levels of privacy concerns (Krasnova & Veltri, 2010) or amount of information disclosure (S. E. Cho & Park, 2013; Tsoi & Chen, 2011) across countries without paying attention to the specific information sharing context. As privacy decisions are highly sensitive to the prevailing contextual factors, it is unknown whether such contextual impact differs in different countries. For instance, people with different cultures may respond differently to the same contextual factors due to different cultural norms and practices. These issues remained unexplored in previous cross-cultural work.

Lastly, previous cross-cultural privacy studies mostly examine informational privacy concern, namely concerns about factual information sharing. However, as we reviewed, privacy concerns in SNSs move beyond factual information disclosure and should reflect the interpersonal nature of social interactions, such as the interactional and psychological aspects (Karr-Wisniewski et al., 2011; Zhang et al., 2011). Likewise, SNS information disclosure also covers a variety of aspects of social life and interpersonal interaction in addition to factual information about users. Thus, it is necessary to include these various aspects in cross-cultural privacy research.

To fill these research gaps, our study aims to answer three research questions:

RQ1: How does the contextual impact on privacy decisions in SNSs differ in different countries?

RQ2: How does the impact of privacy concerns on privacy decisions in SNSs differ in different countries?

RQ3: Are SNS users in different countries concerned with different aspects of privacy in online social interaction?

To answer these research questions, we propose a hypothesized model to test, which will be described in the next section.

3 HYPOTHESES DEVELOPMENT

In this section, we discuss how we develop our hypotheses and research model based on previous theories and frameworks. Figure 1 depicts the research model and hypotheses. We describe each hypothesis in more detail in the following subsections.

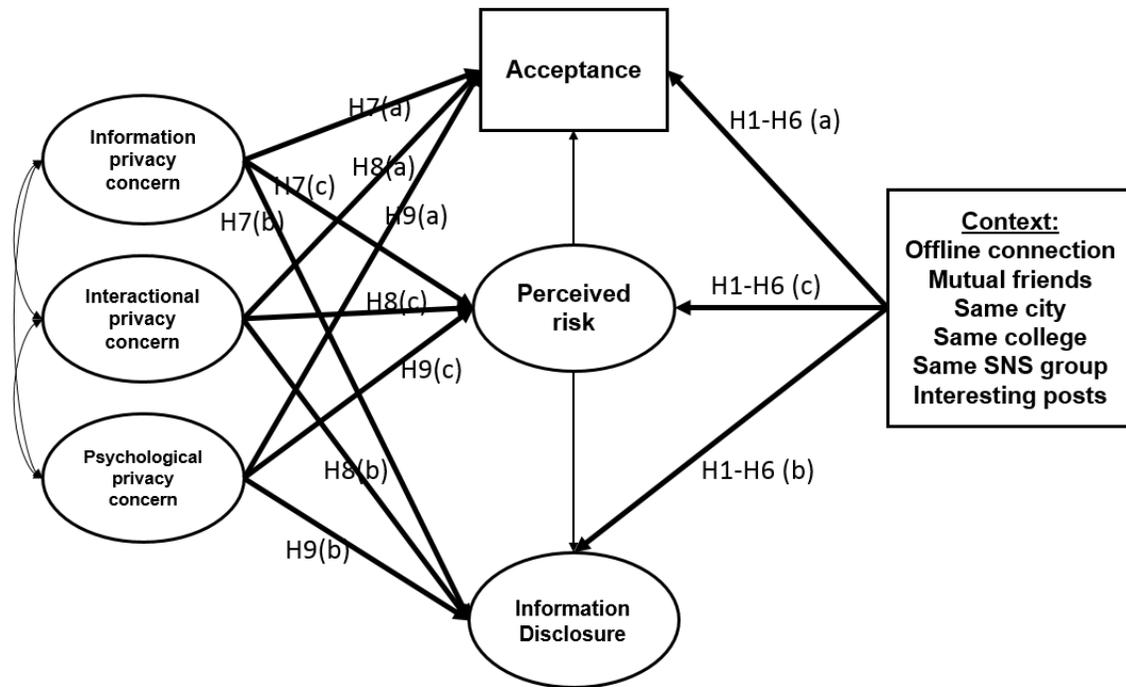


Figure 1. Hypothesized model. Bold paths are hypothesized to differ across different countries (H10-H21).

3.1 Privacy Decisions

In the present study, we examine two contextualized privacy decisions: *acceptance of friend requests and information disclosure*. “Friend requests” are one of the most common SNS activities. Accepting friend requests is a direct way to grant access to one’s personal information in many SNSs and to allow online encounter with others, thus has been considered as a way to manage privacy (Dong et al., 2015). Information disclosure, as we reviewed earlier, has been intensively used in privacy research. These two actions, acceptance of friend requests and information disclosure sufficiently describe users’ privacy decisions in SNSs. We thus include them as outcome variables in our model.

In addition to friend request acceptance and information disclosure, we introduce the *situational perceived privacy risk* (shortened as perceived risk in the model) to describe users’ situational judgement or response regarding different friend requests. Perceived privacy risk is defined as one’s expectation of losses associated with information sharing (Malhotra et al., 2004). We include perceived privacy risk in our model because: 1) perceived privacy risk can change upon different situations and thus subject to the impact of contextual factors (Malhotra et al., 2004); 2) since many studies have demonstrated the weak relationship between privacy concerns and privacy decisions (Acquisti & Gross, 2006; Tufekci, 2008), perceived privacy risk can act as a mediator between privacy concerns and privacy decisions, which follows Malhotra et al.’s work. Malhotra et al. argue that perceived risk in a specific situation can be influenced by privacy concern which reflect one’s pre-disposition to worry about privacy, and can determine one’s consequent privacy behavior (Malhotra et al., 2004). Lo (Lo, 2010) and Krasnova et al (Krasnova et al., 2010) later supported Malhotra’s

model by verifying that perceived risk mediates the relationship between privacy concern and information disclosure in SNSs. Therefore, our model uses the situational perceived risk as a mediator between privacy concern and decisions.

3.2 Contextual Factors

We focus on information recipient to describe the context in friend requests. According to the framework of Nissenbaum's contextual integrity, context can be conceptualized by three parameters: actors (subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows) (Nissenbaum, 2009). Among these three context parameters, the majority of previous literature focuses on the information recipient as a primary contextual predictor of privacy decisions on SNSs (Bilogrevic et al., 2013; Fang & LeFevre, 2010; Lipford et al., 2009; Wiese et al., 2011). Regarding the operationalization of information recipient in SNSs, several studies examine the type of social relationships between the user and the information recipient. For example, users are more likely to accept known social relationships (Chen et al., 2009) or the relationships that they have offline interaction with (Strater & Lipford, 2008). In addition, users are more likely to disclose information to close ties, such as spouses (Consolvo et al., 2005) and close friends and family (Benisch et al., 2011; Sadeh et al., 2009), than to distant ties (Bilogrevic et al., 2013), such as strangers and merchants (Lederer et al., 2003) and co-workers (Consolvo et al., 2005). Another group of studies use commonalities to characterize information recipients. For instance, users tend to accept information recipients who share similar post content (Chen et al., 2009), location histories (Bao et al., 2015), mutual friends (Chen et al., 2009) and interests (Ben Sassi et al., 2017). When facing unknown online relationships, users alter their openness based on common friends, content (e.g., photos, lists, interests, etc.), indicated geographical locations (Brzozowski & Romero, 2011), and social clues in profiles (Wisniewski et al., 2012).

Based on these studies, we conclude that relationships and commonalities with information recipients are two major contextual factors to operationalize the "recipient" parameter. In friend requests, the information recipient is the requester who send the friend request, as once accepted, the requester will likely join the audience to one's information sharing and initiate online social encounter. As users can meet both known and unknown relationships in friend requests, we use *offline interaction*, *mutual friends*, *commonalities in location* and *commonalities in interests* as the contextual factors to characterize the information recipient:

H1: Having offline connection with the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

H2: Having mutual friends with the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

H3: Living in the same city with the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

H4: Going to the same college with the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

H5: Staying in the same SNS group with the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

H6: Interesting posts from the requester increases users' (a) friend request acceptance and (b) information disclosure with the requester, and reduces users' (c) perceived risk of the requester.

3.3 Privacy Concern

Most of the conceptualizations of privacy concern, such as the Concern for Information Privacy (CFIP) (Smith et al., 1996), were developed in the context of e-commerce that focusses on the disclosure of factual personal information. In SNSs, privacy concerns extend beyond factual information disclosure and are related with various aspects in social interactions, such as interactional and psychological privacy. Thus, the conceptualization of SNS privacy concerns should involve the dimensions that reflect the interpersonal nature of boundary regulation. One example of such conceptualization is Zhang et al.'s four-dimensional privacy concerns in online social network: virtual territory privacy, factual information privacy (shortened to information privacy for brevity), interactional privacy, and psychological privacy (Zhang et al., 2011). Among them, information privacy describes control over identifiable personal information; interactional privacy describes users' concern towards online encounters with others; psychological privacy is about the freedom to express one's views and the concern towards others' reactions to one's information disclosure. We thus use *information, interactional, and psychological privacy concerns* in our study to cover the comprehensive social aspects of online interpersonal privacy. Since privacy concern negatively predicts users' information disclosure (Jiang et al., 2013; Min, 2015; Min & Kim, 2014; Son & Kim, 2008; Stewart & Segars, 2002), and positively influences how the person perceives risk in a specific situation (Malhotra et al., 2004), we hypothesize:

H7: Information privacy concern negatively influences users' (a) friend request acceptance and (b) information disclosure with the requester, and positively influences users' (c) perceived risk of the requester.

H8: Interactional privacy concern negatively influences users' (a) friend request acceptance and (b) information disclosure with the requester, and positively influences users' (c) perceived risk of the requester.

H9: Psychological privacy concern negatively influences users' (a) friend request acceptance and (b) information disclosure with the requester, and positively influences users' (c) perceived risk of the requester.

3.4 Cultural Differences

3.4.1 Cultural Differences in Contextual Impact

To answer RQ1, we hypothesize that country moderates the effect of contextual factors on perceived risk and decisions. In order to hypothesize the concrete moderation effects, we review cross-cultural social-psychological literature. Research has found different norms of social interactions in different cultures (Oyserman et al., 2002; Schimmack et al., 2005; Harry C. Triandis et al., 1988). For example, in collectivistic cultures, people favor in-group relationships (family, friends, etc.) over out-group relationships (strangers) (Bond & Smith, 1996), and interact more frequently with in-group members (Gudykunst et al., 1992).

Collectivists tend to understand their self-identities based on social roles and endeavors; harmony in in-group relationships contributes to their life satisfaction (Kwan et al., 1997). These cultural differences are related with the contextual factors in our study, as our contextual factors describe the relationships with information recipients. Recipients with offline interaction, mutual friends, and in the same college can be considered as in-group relationships because such recipients are usually existing social relationships that people already interact with. Thus, we hypothesize that users in collectivistic countries are more willing to disclose to and interact with known online social relationships, their college friends, and friends of friends, as these relationships are more likely to be their in-group members:

H10: The effects of offline connection on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in Korea and China than in the U.S.

H11: The effects of mutual friends on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in Korea and China than in the U.S.

H12: The effects of same college on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in Korea and China than in the U.S.

In individualistic cultures, people tend to define their identities through uniqueness and personal achievement rather than social roles (Oyserman et al., 2002). Though they also feel close to in-group members, they interact with more groups, and expect to have more freedom to decide which groups to belong to (Wheeler et al., 1989). They treat different in-group relationships in a similar manner (Hui et al., 1991), and have greater willingness to trust others—including strangers, and greater ease in the interaction with strangers (Yamagishi, 1988). Relating these cultural differences with our contextual factors that describe recipients' characteristics, recipients in the same city, SNS group and with interesting posts can be considered as out-group relationships because such recipients are usually weak social relationships. Therefore, we hypothesize that users in individualistic countries may feel comfortable to interact with strangers, such as people in the same city or same SNS groups, and people with interesting posts, because users in individualistic countries interact with more groups and have greater willingness to trust strangers and join more groups:

H13: The effects of same SNS group on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in the U.S. than in Korea and China.

H14: The effects of same city on (a) friend request acceptance, (b) information disclosure, (c) perceived risk are stronger in the U.S. than in Korea and China.

H15: The effects of interesting posts on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in the U.S. than in Korea and China.

3.4.2 Cultural Differences in Privacy Concerns

To answer RQ2 and RQ3, we examine how country moderates the effects of privacy concerns on perceived risk and decisions, and the main effect of country on privacy concerns.

Information Privacy Concern:

As we review early, most previous cross-cultural privacy studies focus on factual information disclosure and show that users in individualistic countries exhibit relatively higher levels of privacy concerns than those in collectivistic countries (H. Cho et al., 2009; Krasnova & Veltri, 2010; Wang, Norcie, et al., 2011), we thus hypothesize:

H16: Users' information privacy concern is higher in the U.S. than in Korea and China.

H17: The effects of information privacy concern on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in the U.S. than in Korea and China.

Interactional Privacy Concern:

Interactional privacy is about users' ability to control their encounters with others and to avoid unwanted contact or involvement (Burgoon et al., 1989). Because people in collectivistic cultures favor in-group relationships over out-group, and less frequently interact with people outside their social groups (Bond & Smith, 1996), they have more restrictions in managing their social encounter with others than people in individualistic cultures. It is possible that they focus on maintaining relationships with in-group members and avoiding contact from unwanted out-group people so as to satisfy their affiliation with social groups. We thus hypothesize:

H18: Users' interactional privacy concern is higher in Korea and China than in the U.S.

H19: The effects of interactional privacy concern on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in Korea and China than in the U.S.

Psychological Privacy Concern

Psychological privacy is about one's freedom to express their views and to maintain psychological independence from cognitive and affective interference of others (Burgoon et al., 1989). It allows people to develop autonomy and self-identity. A well-known characteristic of individualism is the focus on autonomy, independence and freedom. In countries with high individualism, such as US, the social norms encourage people to create a personal, private and unique self. People are comfortable if their opinions do not agree with others. However, in collectivistic countries, people tend to care about, and be influenced, by social norms and others' opinions, especially of those who are important social relationships (Harry C. Triandis et al., 1988). They are more likely to raise concerns if their opinions do not agree with others. Thus, we hypothesize:

H20: Users' psychological privacy concern is higher in Korea and China than in the U.S.

H21: The effects of psychological privacy concern on (a) friend request acceptance, (b) information disclosure, and (c) perceived risk are stronger in Korea and China than in the U.S.

4 METHODOLOGY

4.1 Survey Administration

We tested our research hypotheses using data collected from an online survey deployed on Qualtrics.com. We ran the survey simultaneously in three countries, the US, Korea and China, from September to November 2017. We chose these three countries because of their large populations of SNS users and well-established ICT infrastructures. Additionally, Korea and China have lower individualism scores than the US, according

to Hofstede’s cultural framework, which can help us contrast the country differences. The SNS platform of the survey was Facebook in US and Korea, and WeChat in China. The survey in the US was in English. We translated it into Korean and Simplified Chinese, using back-translation by native speakers to ensure semantic consistency. In the US, we ran the survey at the University of <anonymized> and on Amazon Mechanical Turk. At <anonymized>, we used convenience sampling by posting the survey link in departmental mailing lists and undergraduate and graduate student Facebook groups. 90 participants took our survey through this distribution. On Amazon Mechanical Turk, 400 participants took our survey, with a compensation of \$1. In Korea, 316 participants were recruited from an online panel by Qualtrics. The company ran regular benchmarking surveys to ensure their panelists are representative of the larger Internet population in Korea. In China, we collected 451 responses by posting the survey link on popular forums, such as Baidu Tieba, Tianya, Douban, etc. We compensated each participant with ¥ 1 for completing the survey. The compensation was delivered through the WeChat Red Packet¹. The average time to take the survey was about 10-20 minutes for participants across all three countries.

We used questions to screen out participants younger than 18 or non-Facebook users (for US and Korea) or non-WeChat users (for China). We also restricted their nationalities to these three countries. We eliminated responses that failed attention check questions embedded in the survey and those from repeated IP addresses. A total of 1159 valid survey responses (US: 443, Korea: 305, and China: 411) was collected. Table A.1 in the Appendix shows the demographics of the respondents.

The survey consisted of three parts. We first asked participants about their demographics, such as gender, age, income, and education background. We also asked about their general self-disclosure amount on SNSs. It was measured by 6 items using a seven-point Likert scale from the General Disclosiveness Scale (Wheless & Grotz, 1976), and adapted to the domain of SNS use. Its items can be found in the “General self-disclosure amount” section in Table A.2 in the Appendix.

In the second part, we asked a set of items that measured SNS privacy concerns, using a seven-point Likert scale. We took three dimensions of online social network privacy concerns from (Zhang et al., 2011): 4 items on information privacy concern, 3 items on interactional privacy concern, and 4 items on psychological privacy concern. All the privacy concern items can be found in the “Privacy concern” section in Table A.2 in Appendix.

The third part contained scenario-based questions. Since we could not access participants’ actual Facebook friend request decisions, we developed scenarios that were visually similar to the friend requests on Facebook and WeChat. We randomly presented each participant with 3 different scenarios describing 3 friend requests. Each scenario contained a combination of 6 contextual variables. Table 1 lists the 6 contextual variables.

Contextual Variable	Name
Does the participant know the requester offline?	Know
Is the participant in the same Facebook group as the requester?	Group
Does the participant live in the same city as the requester?	City
Does the participant have mutual friends with the requester?	Friends

¹ WeChat Red Packet is a popular feature in WeChat that allows transfer of money as a gift.

Is the participant from the same college/school as the requester?	College
Does the participant find the requester's Facebook posts interesting?	Post

Table 1. Contextual variables and their names.

We created a total of 63 scenarios after verifying that their combinations of contextual factors made sense. An example scenario is:

“You get a new friend request on Facebook. You know this person offline. The person is in the same city and college with you, but not in the same Facebook group. You don't have any mutual friends. The person's Facebook posts are not interesting to you.”

For each scenario, participants were asked to indicate their perceived risk, their decision on the friend request, and their information disclosure to the requester. The perceived risk was measured by a 7-point Likert scale on 4 items taken from (Jarvenpaa et al., 1999). It gauged how risky participants perceived the requester in the specific scenario. Risk perception was thus situational rather than general. The decision on the friend request was binary, indicating whether participants accepted or declined the friend request in the scenario. The information disclosure construct contained 17 different items of personal information that were usually shared on Facebook, partially taken from (Gross & Acquisti, 2005; Knijnenburg et al., 2013), such as real name, gender, age, photo, etc. Participants could select any number of information items including none. By selecting an item, participants indicated that they were willing to disclose this item to the requester. Thus, the response to each item of information disclosure was binary. All items of perceived risk and information disclosure can be found in Table A.2 in the Appendix.

4.2 Data Analysis

We used Mplus to build models. We combined the data from the three countries with a country indicator. We first subjected the 17 items of information disclosure to an Exploratory Factor Analysis (EFA) to test whether they are subject to one factor, as they are not pre-established measurement for information disclosure. We used a robust weighted least-square estimator (WLSMV) and an oblique Geomin rotation method. The WLSMV estimator provides a better option for modelling categorical or ordered data as it does not assume normally distributed variables. Surprisingly, there were two dimensions underlying these 17 items. We considered the meaningfulness of the factors together with model fit indices (i.e., RMSEA, CFI, TLI, eigenvalues, etc.) to find out the optimal solution. A RMSEA smaller than 0.08 and CFI and TLI greater than 0.9 indicate an acceptable model fit. Low factor loadings (<0.4) with the parent factors, or high cross-loadings (>0.4 or >1/2 of parent loadings) with other factors will be removed.

After testing the dimensionality of information disclosure, we subjected all items to a Confirmatory Factor Analysis (CFA) to build a measurement model. Items for self-disclosure amount, privacy concerns and perceived risk were ordinal, while items for information disclosure were binary. We used again the WLSMV estimator. Convergent validity is supported when indicators load significantly on their respective factors (standardized factor loadings exceed 0.6) and also the Average Variance Extracted (AVE) is higher than 0.5. Discriminant validity is supported when the correlation between latent factors is lower than .85, and smaller than the square root of the AVE of each factor. Based on the CFA results, we eliminated items with factor

loadings less than 0.6, or with significantly higher modification indices. We also checked the measurement invariance across the three countries by comparing configural, metric and scalar measurement models (see Cho et al. (H. Cho et al., 2018) for its importance in multi-cultural privacy research). If the metric or scalar model is not significantly worse than the configural model in terms of model fit, we can claim that we have metric invariance for comparing path coefficients across groups, or scalar invariance for comparing means. If any non-invariance exists, checking the estimations with large modification indices will help us locate the source of the non-invariance.

Next, we examined the main effects of country on all the factors to compare the levels of factors across the three countries. We especially examined how levels of three different privacy concerns vary across the three countries in order to test H16, H18 and H20. We made the US as the baseline in this step. After this, we subjected all factors and observed variables to Structural Equation Modeling (SEM) to test H1-H9, using the WLSMV estimator. We modeled the relationships as shown in the hypothesized model in Figure 1. We allowed residual correlations among different types of privacy concerns, and between friend request decision, information disclosure and perceived risk. We controlled general SNS self-disclosure amount, gender, age, education and income. Since a participant's responses to the 3 scenarios presented in the survey might be associated, we used two-level SEM. Two-level modeling allows within/between level modeling by introducing the random slope/intercept that varies across clusters in hierarchical data. In our two-level SEM, we allowed random intercept at subject level. The contextual variables in each scenario are within-level predictors, while the privacy concerns, general self-disclosure amount, and controlled demographic variables are between-level. We also computed the intra-class correlations (ICC) of dependent variables. The ICC is a measure of the relatedness of clustered data by comparing the variance within clusters with the variance between clusters.

Finally, to compare the effects across the three countries (H10-15, H17, H19, and H21), we used multi-group analysis. The grouping variable was country. In Step 1, we fit identical models (with intercepts and path coefficients to be the same) for each country. In Step 2, we fit the same model for each group, but allowed one path, i.e., from “known offline” to “perceived risk”, to be free (i.e., different among the three countries), while other estimations were identical. In Step 3, we compared the models in Step 1 and 2 through a Wald test to see if freeing the path significantly improved the model fit. We performed this process one by one for the paths from context variables to perceived risk, friend request acceptance, and information disclosure. If the model comparison showed a statistically significant result, we claimed a country difference to that effect. Because the computation of the multi-group two-level SEM is very time-consuming when indicators of latent variables are categorical, we used the factor scores of the latent factors.

5 RESULTS

5.1 Dimensionality of Information Disclosure.

The EFA results show that there were two dimensions underlying these 17 items. the information disclosure items into two dimensions: demographic and social information disclosure (Table 2). The model fit indices

for the two-factor solution are: $\chi^2=855.131$, $df=103$, $p<0.05$, $RMSEA = 0.079$, $CFI = 0.924$, $TLI = 0.900$. The demographic information disclosure has 5 items, while the social information disclosure has 8. The two-factor solution leaves 4 items with large cross-loadings, which are removed in later analysis. The three-factor solution makes a better model fit, but has one factor with only two items. We thus adopt the two-factor solution due to its meaningful factors and better parsimony.

Information Disclosure Items	1	2
Gender	0.789*	-0.011
Age	0.867*	0.005
My e-mail address	0.587*	0.123
My mailing address	0.768*	0.034
My phone number	0.787*	-0.100
Photo with my image	0.071	0.674*
Political views	0.048	0.803*
My educational background	0.159*	0.788*
Name of my college	0.141*	0.706*
My friend list	0.003	0.772*
Interests (favorite movies, books, etc.)	-0.069	0.865*
Status updates	-0.067	0.862*
Shared links	-0.195*	0.944*
Occupation	0.507*	0.375*
Hometown	0.350*	0.472*
Workplace	0.407*	0.439*
My current location	0.313*	0.532*

Table 2. EFA results of information disclosure items (* $p<0.05$)

5.2 Measurement Model.

The results from CFA show that the measurement model has acceptable fit indices ($\chi^2= 1762.267$, $df = 506$, $p<.001$; $RMSEA = 0.046 < 0.05$, 90% CI: [0.044, 0.049], $CFI = 0.977 > 0.9$, $TLI = 0.974 > 0.9$). A chi-square test with a p-value greater than 0.05 usually indicates good model fit. However, it is sensitive to sample size. We thus use other criteria, such as RMSEA, CFI and TLI together to describe the goodness-of-fit of our measurement model. All standardized factor loadings are above the recommended 0.6 level (see Table A.2 in the Appendix). Each latent variable's Average Variance Extracted (AVE) is greater than 0.5, indicating adequate convergent validity (Table A.2 in the Appendix). The square root of each latent variable's AVE is greater than its correlations with other latent variables, indicating adequate discriminant validity (Table 3). We conducted two measurement invariance tests². One is solely for demographic and social information disclosure, and one is for other factors. This is because information disclosure has binary items while the other factors have 7-category items. The results of the measurement invariance test (Table A.3 in the Appendix) show that demographic and social information disclosure achieve partial scalar invariance, with four items that should be freed in their intercepts in the US sample. Other factors (general self-disclosure amount, privacy concerns, and perceived risk) achieve partial metric invariance, with one information privacy concern item in the Korean sample, and one psychological privacy concern item and one general self-

² Since the chi-square test is sensitive to sample size, we conducted the measurement invariance test on a random subset (N=390) of our data.

disclosure amount item in the Chinese sample that should be freed in their factor loadings. As invariance in up to 20% of parameters is acceptable when conducting multiple group comparisons (Byrne, 1989), our measurement model can be used for comparing path coefficients between countries.

Amount	0.845						
Information	0.018	0.790					
Interactional	0.215	0.24	0.819				
Psychological	0.211	0.455	0.532	0.862			
Perceived risk	0.099	0.346	0.308	0.334	0.893		
Demographic	0.137	-0.129	-0.092	-0.019	-0.227	0.728	
Social	0.069	-0.043	-0.283	-0.076	-0.509	0.533	0.745
	Amount	Info.	Inter.	Psycho.	Risk	Demo.	Social

Table 3. Factor correlations (the diagonal shows the square root of the AVEs).

5.3 Country Main Effects.

We model the main effects of country on all the factors and friend request decision in Table 4 to show an overall comparison across the three countries. We set the US as the baseline. The overall comparison shows that Korean and Chinese SNS users exhibit a higher general self-disclosure amount than US users. They perceived more risk towards the requesters in the scenarios, and also disclosed more demographic information but less social information. They are more concerned than US users about their control over online encounters with others (interactional privacy concern) and about their freedom to express views (psychological privacy concern). **H18 and H20 are supported.** Korean users, but not Chinese users, have significantly lower information privacy concerns than US users, which **partially supports H16.**

Factors	US	KR	CN
General self-disclosure amount	Baseline	0.307***	0.665***
Information privacy concern		-0.165***	-0.086
Interactional privacy concern		0.877***	0.407***
Psychological privacy concern		0.510***	0.440***
Perceived risk		0.235***	0.566***
Demographic information disclosure		0.428***	0.182***
Social information disclosure		-0.379***	-0.333***

Table 4. Main effects of country on factors (***p<.001).

5.4 Multi-group SEM.

Before conducting the multi-group SEM, we computed the intra-class correlations (ICC) for outcome variables (Table 5). The average cluster size is 3, as all the 1159 participants responded to 3 random scenarios. The ICCs show significant interclass correlations so that the use of multilevel modeling is called for.

Variable	ICC
Acceptance	0.373
Perceived Risk	0.523
Demographic Info. Disclosure	0.583
Social Info. Disclosure	0.532

Table 5. ICCs of dependent variables.

We present the multi-group SEM model and path coefficients in Figure 2. In the multi-group SEM model, we free the path coefficients across the three countries. The multi-group SEM has good model fit: $\chi^2=$

116.396, $df = 48$, $p < .001$; $RMSEA = 0.035 < 0.05$, $CFI = 0.991 > 0.9$, $TLI = 0.949 > 0.9$. We mark out in bold the path coefficients that are significantly different across the three countries, and report the respective change of Chi-square and its significance in the results from multi-group analysis shown in Figure 2.

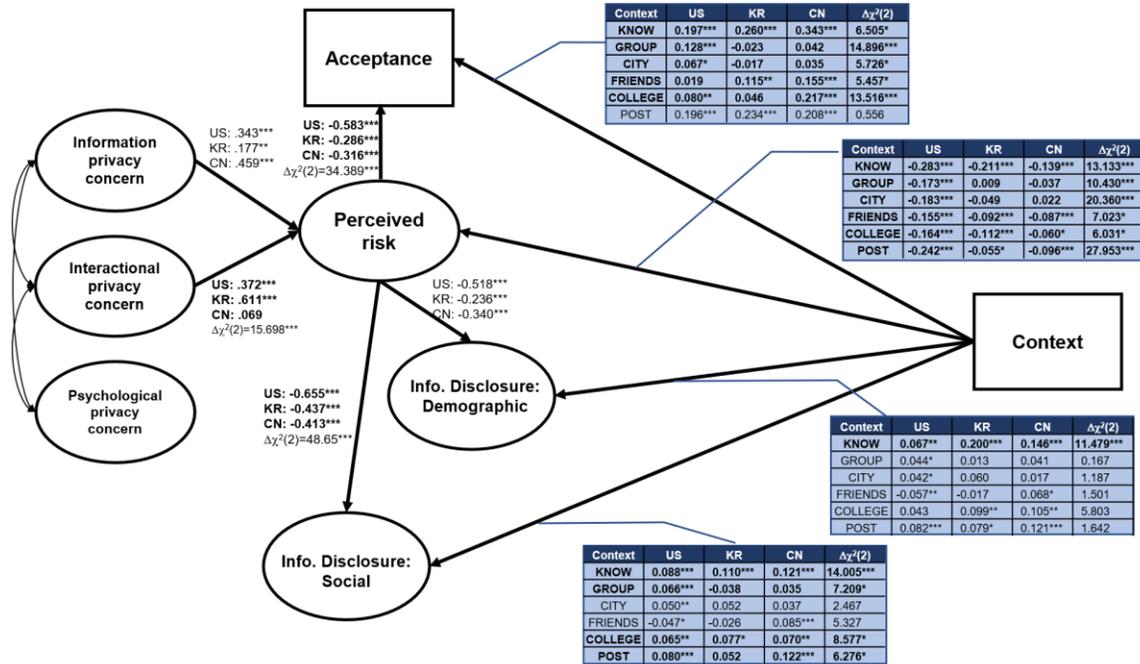


Figure 2. Path coefficients comparison across the three countries (* $p < .05$, ** $p < .01$, *** $p < .001$). Note non-significant paths are not included in the graph.

5.5 Effects of Contextual Factors

The contextual effects on privacy decisions are overall significant in US (except for the effect of mutual friends on friend request acceptance and the effect of same college on demographic information disclosure), whereas the contextual effects in Korea and China are not as significant as in US in certain cases. This suggests that previous findings about contextual factors that were based on US samples cannot necessarily be generalized to other countries.

Particularly, offline connection and interesting posts significantly increase the acceptance of friend requests in three countries, thus **H1(a) and H6(a) are fully supported**. Requesters in the same SNS group or city are not well accepted in Korea and China. **H3(a) and H5(a) are only partially supported**. Americans' friend request decisions are not significantly influenced by mutual friends, thus **H2(a) is partially supported**. Same college does not have significant effect on acceptance in Korea, thus **H4(a) is partially supported**. Comparing the three countries, the effects of known offline and mutual friends on friend request acceptance are significantly stronger in Korea and China than the US. By contrast, the effects of same SNS group and city are significantly stronger in the US than the two Asian countries. **H10(a), H11(a), H13(a) and H14(a) are supported**. **H12(a) is partially supported**, as effect of same college is significantly stronger in China

than the US, but not for Korea. **H15(a) is not supported**, as there is no significant difference in the effects of interesting posts across the three countries.

The contextual variables do not consistently increase both demographic and social information disclosure in all the three countries. Only offline connection and interesting posts significantly increase information disclosure across three countries. Hence, **H1(b) and H6(b) are supported. H2(b)-H5(b) are only partially supported** as the context effects are only significant in one or two countries. Compared with the contextual effects across the three countries, the effect of known requester is significantly stronger in Korea and China. **H10(b) is supported**. The effects of same SNS group on social information disclosure are stronger in US, and the effect of same college are stronger in Korea and China. However, the same does not apply to demographic information disclosure. Thus, **H12(b) and H13(b) are partially supported**. The effects of interesting posts on social information disclosure are stronger in China, and those on demographic information disclosure do not significantly differ across the three countries. Thus, **H15(b) is rejected**. The effects of mutual friends and same city also do not significantly differ across three countries. **H11(b) and H14(b) are rejected**. Comparing the effect size of contextual factors on two types of information disclosure, the contextual factors drive users in the US to make more social than demographic disclosures. In Korea and China, contextual factors drive users to make more demographic than social disclosures, except same group, city and mutual friends which do not significantly influence any information disclosure.

The contextual variables, offline connection, mutual friends, same college and interesting posts significantly reduce perceived risk in three countries, thus **H1(c), H2(c), H4(c), and H6(c) are supported**. The effects of same SNS group and same city are not consistently significant across three countries, **thus H3(c) and H5(c) are partially supported**. The contextual effects on perceived risk vary significantly across the three countries. In the US, all the contextual variables diminish the perceived risk significantly. In Korea and China, only offline connection, mutual friends, same college, and interesting posts will significantly reduce users' perceived risk. All the contextual effects are significantly weaker in Korea and China than in the US. Thus, **H13(c), H14(c) and H15(c) are supported, while H10(c), H11(c) and H12(c) are rejected**.

5.6 Effects of Privacy Concerns.

Information privacy concern positively influences perceived risk in the three countries (H7c is supported). Interactional privacy concern only positively influences perceived risk in US and Korea (H8c is partially supported). However, both information and interactional privacy concerns do not directly and significantly influence friend request acceptance and information disclosure, thus **H7(a)(b) and H8(a)(b) are not supported**. Psychological privacy concern does not significantly influence any privacy decision in three countries. **H9 is and H20 are rejected**. The effects of information privacy concern do not significantly differ across the three countries. Thus, **H17 is rejected**. The effects of interactional privacy concern significantly vary across the three countries. They are significantly larger in Korea than in US than in China. **H19(c) is partially supported**.

5.7 Summary of Results

We summarize the hypotheses testing results in Table 6:

#		Hypothesized Effects	Result
H1	a-c	Known offline→(+) acceptance(+) information disclosure(-) perceived risk	Full support
H2	a-b	Mutual friends→(+) acceptance(+) information disclosure	Partial support
	c	Mutual friends→(-) perceived risk	Full support
H3	a-c	Same city→(+) acceptance(+) information disclosure(-) perceived risk	Partial support
H4	a-b	Same college →(+) acceptance (+) information disclosure	Partial support
	c	Same college →(-) perceived risk	Full support
H5	a-c	Same SNS group→(+) acceptance(+) information disclosure(-) perceived risk	Partial support
H6	a-c	Interesting posts→(+) acceptance(+) information disclosure(-) perceived risk	Full support
H7	a-b	Information privacy concern →(-) acceptance(-) information disclosure	No support
	c	Information privacy concern →(+) perceived risk	Full support
H8	a-b	Interactional privacy concern →(-) acceptance(-) information disclosure	No support
	c	Interactional privacy concern →(+) perceived risk	Partial support
H9	a-c	Psychological privacy concern→(+) acceptance(+) information disclosure(-) perceived risk	No support
H10	a-b	Known offline×country→ acceptance, information disclosure: KR, CN > US	Full support
	c	Known offline×country→ perceived risk: KR, CN > US	No support
H11	a	Mutual friends×country→ acceptance: KR, CN > US	Full support
	b-c	Mutual friends×country→ information disclosure, perceived risk: KR, CN > US	No support
H12	a-b	Same college×country→ acceptance, information disclosure: KR, CN > US	Partial support
	c	Same college×country→ perceived risk: KR, CN > US	No support
H13	a, c	Same SNS group ×country→ acceptance, perceived risk: US > KR, CN	Full support
	b	Same SNS group ×country→ information disclosure: US > KR, CN	Partial support
H14	a	Same city ×country→ acceptance: US > KR, CN	Full support
	b	Same city ×country→ information disclosure: US > KR, CN	No support
	c	Same city ×country→ perceived risk: US > KR, CN	Full support
H15	a-b	Interesting posts×country→ acceptance, information disclosure: US > KR, CN	No support
	c	Interesting posts×country→ perceived risk: US > KR, CN	Full support
H16		Information privacy concern: US > KR, CN	Partial support
H17	a-c	Information privacy concern×country→ acceptance, information disclosure, perceived risk: US > KR, CN	No support
H18		Interactional privacy concern: KR, CN > US	Full support
H19	a-b	Interactional privacy concern×country→ acceptance, information disclosure: KR, CN > US	No support
	c	Interactional privacy concern×country→ perceived risk: KR, CN > US	Partial support
H20		Psychological privacy concern: KR, CN > US	Full support
H21	a-c	Psychological privacy concern×country→ acceptance, information disclosure, perceived risk: KR, CN > US	No support

Table 6. Hypothesis testing results.

In sum, the testing results answer the three research questions. Regarding RQ1 (how does the contextual impact on privacy decisions in SNSs differ in different countries?), we find the effects of contextual factors on privacy decisions vary in different countries:

- The effect of offline connection on privacy decisions is stronger in Korea and China than the US.
- The effect of mutual friends on friend request acceptance is stronger in Korea and China than the US.
- The effect of same college on privacy decisions is stronger in China than the US.
- The effect of same SNS group on privacy decisions is stronger in the US than Korea and China.
- The effect of same city on friend request acceptance is stronger in the US than Korea and China.
- The effects of interesting posts on perceived risk is stronger in the US than Korea and China.

Regarding RQ2 (how does the impact of privacy concerns on privacy decisions in SNSs differ in different countries?), we find that privacy concerns do not have direct effect on privacy decisions and the effects of privacy concerns on perceived risk partially vary in different countries:

- The effects of information privacy concern on perceived risk do not significantly differ across the three countries.
- The effects of interactional privacy concern on perceived risk significantly vary across the three countries.
- Psychological privacy concern does not significantly influence any privacy decision in three countries.

Regarding RQ3 (are SNS users in different countries concerned with different aspects of privacy in online social interaction?), we find SNS users in the three countries focus on different aspects of privacy:

- Korean users, but not Chinese users, have significantly lower information privacy concerns than US users.
- Korean and Chinese SNS users exhibit more interactional privacy concern than US users.
- Korean and Chinese SNS users exhibit more psychological privacy concern than US users.

6 DISCUSSION

The goal of this paper is to understand how contextual factors and privacy concerns cast different impact on privacy decisions in different countries. We performed a quantitative study in three countries, the US, Korea and China, to model the relationships between contextual factors, privacy concerns and privacy decisions. Our findings show that contextual impact indeed vary across the three countries, and that users in different countries focus on different aspects in the formation of privacy concerns, and thus have different decisions in information disclosure in SNSs. We discuss the implications in this section.

6.1 Country Differences in Contextual Information Norms

We find significant country differences in contextual impact between the US, Korea and China. First, our findings demonstrate that the primary contextual factors that shape SNS privacy decisions vary across the three countries. For American users, almost all six contextual factors significantly influence friend

acceptance, information disclosure and perceived risk. In contrast, the privacy decisions of Korean and Chinese users are not significantly affected if the requester is in the same SNS group or city. The positive effects of a known requester on friend acceptance and information disclosure is much stronger in Korea and China than in the US, indicating that existing connection is more important for Korean and Chinese users. This suggests that the contextual factors found in previous work based on surveys conducted only in the US may not be equally impactful in other countries like Korea and China. Future cross-country privacy research should therefore look at different sets of contextual factors, in accordance with the respective cultures. Moreover, these findings echo previous results (Kim et al., 2011) which assert that users from collectivistic countries are motivated to use SNSs to maintain existing relationships, while individualists tend to expand their social networks. In collectivistic countries like Korea and China, people favor in-group over out-group relationships. Interactions with in-group relations are more predictable and comfortable than those with out-group relations. Thus, they are more likely to accept and to disclose to known requesters, rather than requesters in the same SNS group or city. In individualistic countries like the US, people are instead willing to interact with more groups (Wheeler et al., 1989) and engage with different groups and strangers (Yamagishi, 1988). Thus, in addition to known requesters, American users in our survey also find it easy to accept requesters who are merely in the same SNS groups or city, or who publish interesting posts, as this will help them expand their online social networks. Hence, we recommend that privacy researchers take cultural differences in contextual information norms into consideration when examining privacy decisions on SNS.

Another country difference in the contextual impact relates to the two common types of information disclosure, namely demographic and social information disclosure. Most prior cross-cultural privacy studies examined general information disclosure in SNSs without distinguishing between different categories of SNS information disclosure. Our findings show that Koreans and Chinese disclose more demographic information while Americans more social information (Table 4), suggesting that future research should specify the type of information disclosure when examining cross-cultural differences. Furthermore, the SEM model reveals that contextual factors drive users in different countries to disclose different types of information: in the US, the same contextual factors drive users to make more social than demographic disclosures, while in Korea and China it is the opposite (disregarding the factors of same group, city and mutual friends, which do not significantly influence information disclosure). Demographic disclosure refers to gender, age, contact information, etc., while social disclosure is about photos, views, interests, etc. Collectivistic users disclose more demographic information, perhaps because they want to be identified as ingroup members and trust other ingroup members to protect their identifiable information. Individualistic users more likely aim to find new friends with similar interests (Kim et al., 2011), and thus disclose more social information. We suggest that future work pay attention to these cultural differences in users' preferences for information types in SNS disclosure.

Third, the negative contextual effects on perceived risk is significantly stronger in the US than in Korea and China. Given a requester with the same contextual factors, the perceived risk is more reduced for American

users than for Korean and Chinese users. This seems somewhat contrary to the cultural differences that collectivistic countries as “high context” and people should be more sensitive to the social relationships, whereas individualistic countries are characterized as “low context” and people are more rule-based and autonomous (Hall, 1989). However, previous research had shown that users in collectivistic cultures perceive higher risk and are more risk-averse than in individualistic cultures (Dinev et al., 2006; Park & Jun, 2003). Individualists are more trusting of others, whereas collectivists are less likely to trust those beyond their in-groups (Hamamura, 2012). Since general trust of others serves as a lubricant for social interactions (Yamagishi & Yamagishi, 1994), this may partially explain why contextual factors are more likely to reduce risk perception in the US than in Korea and China and why Korean and Chinese users are less likely to mitigate their risk perception in different contexts.

6.2 Country Differences in Privacy Concerns

Our findings show that Korean and Chinese users are more concerned than US users about their control over online encounters with others (interactional privacy concern) and about their freedom to express opinions (psychological privacy concern). But both (especially the Korean users) have lower information privacy concerns than US users. Most prior SNS privacy literature examines only one type, namely information privacy concern. We find that American SNS users exhibit more information privacy concern while Korean and Chinese users exhibit more interactional and psychological privacy concerns. Psychological privacy is about one’s freedom to express their views and to maintain psychological independence from cognitive and affective interference of others (Burgoon et al., 1989). In other word, it is about one’s concern regarding others’ judgement on one’s information disclosure. Individuals in collectivistic cultures are known to likely more care about, and be influenced, by others’ opinions, especially of those who are important social relationships (Harry C. Triandis et al., 1988). People in individualistic cultures rather tend to value personal and unique feelings over others’ judgement and are thus less likely to have psychological privacy concerns. Interaction privacy concern is about the control over unwanted online encounters with others. Individualists prefer to join more in-groups, while collectivists stay with fewer but more stable in-groups. Thus, their concerns of unwanted contacts may vary. These findings may be useful for future cross-cultural privacy studies that should posit users’ privacy concerns as non-uniform, segmented into different types of online social interactions. Different types of privacy concerns may cast varying effects on privacy decisions based on cultural differences.

6.3 Who Discloses Less Information?

One of our unique contributions is that our model considers both individual privacy concerns and contextual factors to capture the cultural differences in privacy decision-making. The earlier discussion suggests that contextual factors reduce perceived risk more strongly in the US than in Korea and China. Hence one would assume that in the same context, American SNS users should disclose more personal information than Korean and Chinese users because they perceive less risk. This, however, is seemingly contrary to previous findings

that users in individualistic countries disclose less personal information in SNSs than in collectivistic countries (Posey et al., 2010). Our model incorporates privacy concerns and contextual factors in an integrated view of cultural differences in privacy decisions. The total effects of privacy concerns are negative and the total effects of contextual factors are positive. The effects of privacy concerns are relatively large in the US after mediated by perceived risk. This indicates that the positive contextual effects are countered by the negative effects of privacy concerns more strongly in the US than in Korea and China. Thus, American users still disclose less information than Korean and Chinese users. This suggests that future cross-cultural privacy research should consider individual privacy concerns and contextual influence together to accurately capture the cultural differences in privacy decisions. If only privacy concerns are accounted for, the cultural differences in privacy decisions may become exaggerated when culturally distinct contextual effects are not included. If solely contextual effects are considered, the results may be reversed as privacy concerns would counteract the contextual effects more strongly in individualistic than in collectivistic countries.

7 DESIGN IMPLICATIONS

Based on the country differences, we suggest several design implications for multinational SNS providers. First, our study shows that the primary contextual factors that shape SNS privacy decisions vary across the US, Korea and China. This suggest that friend recommendation algorithms in SNSs should consider different contextual factors in individualistic and collectivistic countries. For example, SNSs in Korea and China should focus on contextual factors such as offline connection and mutual friends when recommending friend requests, whereas in the US they should focus on commonalities in city and SNS groups. Other context-aware mechanisms in SNSs, such as contextualized privacy setting configurations, should also be differentiated. Contextual factors that do not reduce perceived risk in collectivistic countries (e.g., same city, college, or interests) should not be considered.

Second, when differentiating the contextual factors in different countries, SNS providers need to control the effects of individual privacy concerns, as our model shows that privacy concerns counter the contextual effects. Ignoring the effects of privacy concerns leads to inaccurate predictions for friend request acceptance and ineffectiveness of contextualized privacy support. Additionally, the different types of privacy concerns should be accounted for, as users' privacy concerns in individualistic and collectivistic countries are not uniform. Individualistic users focus on factual information, whereas collectivistic users focus on control over unwanted SNS contacts and judgement of others about their information sharing. Thus, SNS providers should design different strategies to facilitate users' privacy preferences. For example, in individualistic countries SNSs could employ mechanisms to protect factual information disclosure, and in collectivistic countries more features to filter or block unwanted social contact and online judgement.

8 LIMITATIONS

The study has several limitations. First, our findings are based on measures of self-reported perception and behavioral intent in response to fictitious scenarios instead of actual reactions to real friend requests. We did not have access to actual Facebook data, nor could we capture some of the factors without asking, such as

situational perceived risk. In privacy, behavioral intentions may diverge from actual disclosure behavior (Norberg et al., 2007). However, we provided a specific context for a friend request in each scenario that was close to real-world situations. This also enabled us to randomize the contextual factors and draw causal inferences, which is hard to achieve using actual behavioral data. The contextual influence is in line with previous research based on actual behavior data (Dong et al., 2015). We thus believe that our results are useful. We suggest that future studies enhance our findings by capturing actual behaviors.

We use country-level comparison and propose that the cultural differences between individualism and collectivism may explain the country differences we found. This must be viewed with some caution though. First, the three countries in our study may not holistically represent the contrasting aspects between individualism and collectivism. We choose these three countries because they are considered the most representative countries for individualism and collectivism to our best knowledge. Our results do not deviate significantly from cross-cultural privacy studies in other countries, e.g., France vs. UK (Posey et al., 2010) or a multi-national comparison (Li et al., 2017). Second, the levels of individualism and collectivism may be variant within a nation, especially in multiethnic and immigrant societies. Admitting the variations within a nation, we still find significant country effects, indicating that even if not all the residents in a nation are individualistic or collectivistic, the majority of them will exhibit the nature of the national cultures. But we suggest future studies use valid individual-level individualism/collectivism measurements to explain the cultural differences. Third, there may be other country factors that lead to country differences in contextual information norms, such as other cultural dimensions, demographics, legal and political systems, economic factors, etc. There may also be some cross-country differences observed in this study that may not necessarily be related to individualism/collectivism. For example, the insignificant effect of same city on friend request acceptance may be due to the fact the almost $\frac{1}{4}$ of the South Korean population lives in Seoul, thus whether the request is from someone who lives in the same city does not matter much for Korean users. We suggest that future research consider additional country differences in examining the relationship between culture and privacy behavior.

Third, we only focus on predictors that are related to our research questions. We may miss other important factors, such as the benefit from information sharing, which is considered a critical predictor in privacy calculus models and common compared with perceived risk (Xu et al., 2009). However, due to the scope of the study and the space limit in the survey, we did not include all the important predictors of privacy decisions. To build a more comprehensive model, we will consider it in future work.

Finally, we use different recruitment methods in the three countries, which may influence the country effects we find. Most American participants were recruited from Amazon Mechanical Turk (AMT). AMT workers are considered more technology savvy than the general population. We tried to reduce this effect by incorporating participants from our campus. The differences in our recruitment methods were due to the time, accessibility and cost of our study. Collecting large amount of cross-country data is a difficult and costly task. We suggest future research use more efficient cross-country data collection methods. The measurement invariance in privacy-related concepts is another difficulty in cross-country research. Despite several rounds

of back-translation with native speakers, we still have a small number of measurement non-invariance in our constructs. It is still unclear whether the non-invariance is caused by translation or by country differences in privacy conceptualization. We call for future work on this topic.

9 CONCLUSION

The goal of this paper is to understand how effects of contextual factors and users' privacy concerns on privacy decisions differ in different countries. We conduct a survey-based study in three countries, the US, Korea and China, and model the relationships between contextual factors, privacy concerns and privacy decisions. We find that the impact of contextual factors and privacy concerns on privacy decisions vary across the three countries, and that users in different countries focus on different aspects of privacy concerns, which may explain why they have different decisions on information sharing, friend request and perceived risk in SNSs. We suggest strategies for multinational SNS providers to customize their privacy design and the considered context characteristics in different cultures.

10 REFERENCES

- Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. *Digital Enlightenment Yearbook 2012*, 193–197.
- Acquisti, A., Adjerid, I., Balebako, R. H., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2016). *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online* (SSRN Scholarly Paper ID 2859227). Social Science Research Network. <https://papers.ssrn.com/abstract=2859227>
- Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (pp. 36–58). Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/11957454_3
- Alashoor, T., Lambert, L., & Farivar, S. (2016). *A Review of Measures of Disclosure Outcomes in the IS Privacy Literature*. AMCIS 2016 Proceedings. <http://aisel.aisnet.org/amcis2016/ISSec/Presentations/20>
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company, Monterey, California 93940 (\$6.95 cloth).
- Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33(3), 66–84. <https://doi.org/10.1111/j.1540-4560.1977.tb01883.x>
- Bao, J., Zheng, Y., Wilkie, D., & Mokbel, M. (2015). Recommendations in location-based social networks: A survey. *GeoInformatica*, 19(3), 525–565. <https://doi.org/10.1007/s10707-014-0220-8>

- Ben Sassi, I., Mellouli, S., & Ben Yahia, S. (2017). Context-aware recommender systems in mobile environment: On the road of future research. *Information Systems*, 72, 27–61. <https://doi.org/10.1016/j.is.2017.09.001>
- Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, 15(7), 679–694. <https://doi.org/10.1007/s00779-010-0346-0>
- Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., & Hubaux, J.-P. (2013). Adaptive Information-sharing for Privacy-aware Mobile Social Networks. *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 657–666. <https://doi.org/10.1145/2493432.2493510>
- Bond, R., & Smith, P. B. (1996). Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological Bulletin*, 119(1), 111–137. <https://doi.org/10.1037/0033-2909.119.1.111>
- Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Brzozowski, M. J., & Romero, D. M. (2011). Who Should I Follow? Recommending People in Directed Social Networks. *Fifth International AAI Conference on Weblogs and Social Media*. Fifth International AAI Conference on Weblogs and Social Media. <http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewPaper/2867>
- Burgoon et al. (1989). Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, 6(2), 131–158. <https://doi.org/10.1177/026540758900600201>
- Byrne, B. M. (1989). Multigroup comparisons and the assumption of equivalent construct validity across groups: Methodological and substantive issues. *Multivariate Behavioral Research*, 24(4), 503–523.
- Chen, J., Geyer, W., Dugan, C., Muller, M., & Guy, I. (2009). Make New Friends, but Keep the Old: Recommending People on Social Networking Sites. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 201–210. <https://doi.org/10.1145/1518701.1518735>

- Cho, H., Knijnenburg, B., Kobsa, A., & Li, Y. (2018). Collective Privacy Management in Social Media: A Cross-Cultural Validation. *ACM Trans. Comput.-Hum. Interact.*, 25(3), 17:1–17:33. <https://doi.org/10.1145/3193120>
- Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3), 395–416. <https://doi.org/10.1177/1461444808101618>
- Cho, S. E., & Park, H. W. (2013). A qualitative analysis of cross-cultural new media research: SNS use in Asia and the West. *Quality & Quantity*, 47(4), 2319–2330. <https://doi.org/10.1007/s11135-011-9658-z>
- Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: Why, when, & what people want to share. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 81–90. ACM. <https://doi.org/10.1145/1054972.1054985>
- Dienlin, T., & Trepte, S. (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), 285–297.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389–402. <https://doi.org/10.1057/palgrave.ejis.3000590>
- Dong, C., Jin, H., & Knijnenburg, B. P. (2015). Predicting Privacy Behavior on Online Social Networks. *Ninth International AAAI Conference on Web and Social Media*, 91–100. <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10554>
- Facebook users by country | Statistic.* (n.d.). Statista. Retrieved May 24, 2019, from <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>
- Fang, L., & LeFevre, K. (2010). Privacy Wizards for Social Networking Sites. *Proceedings of the 19th International Conference on World Wide Web*, 351–360. <https://doi.org/10.1145/1772690.1772727>
- Fogues, R. L., Murukannaiah, P. K., Such, J. M., & Singh, M. P. (2017). Sharing Policies in Multiuser Privacy Scenarios: Incorporating Context, Preferences, and Arguments in Decision Making. *ACM Trans. Comput.-Hum. Interact.*, 24(1), 5:1–5:29. <https://doi.org/10.1145/3038920>

- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. <https://doi.org/10.1145/1102199.1102214>
- Gudykunst, W. B., Gao, G., Schmidt, K. L., Nishida, T., Bond, M. H., Leung, K., Wang, G., & Barraclough, R. A. (1992). The Influence of Individualism Collectivism, Self-Monitoring, and Predicted-Outcome Value on Communication in Ingroup and Outgroup Relationships. *Journal of Cross-Cultural Psychology*, 23(2), 196–213. <https://doi.org/10.1177/0022022192232005>
- Hall, E. T. (1989). *Beyond Culture*. Anchor Books.
- Hamamura, T. (2012). Are Cultures Becoming Individualistic? A Cross-Temporal Comparison of Individualism–Collectivism in the United States and Japan. *Personality and Social Psychology Review*, 16(1), 3–24. <https://doi.org/10.1177/1088868311411587>
- Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1). <https://doi.org/10.9707/2307-0919.1014>
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and Organizations: Software of the Mind, Third Edition*. McGraw Hill Professional.
- House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*. SAGE Publications.
- Hui, C. H., Triandis, H. C., & Yee, C. (1991). Cultural differences in reward allocation: Is collectivism the explanation? *British Journal of Social Psychology*, 30(2), 145–157. <https://doi.org/10.1111/j.2044-8309.1991.tb00931.x>
- Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology*, 13(4), 289–302. <https://doi.org/10.1007/s10676-010-9224-8>
- Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, 5(2), 0–0. <https://doi.org/10.1111/j.1083-6101.1999.tb00337.x>
- Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, 24(3), 579–595. <https://doi.org/10.1287/isre.1120.0441>

- Karr-Wisniewski, P., Wilson, D. C., & Richter-Lipford, H. (2011). A New Social Order: Mechanisms for Social Network Site Boundary Regulation. *AMCIS 2011 Proceedings*, Paper 101. http://aisel.aisnet.org/amcis2011_submissions/101
- Kim, Y., Sohn, D., & Choi, S. M. (2011). Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior*, 27(1), 365–372. <https://doi.org/10.1016/j.chb.2010.08.015>
- Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, 71(12), 1144–1162. <https://doi.org/10.1016/j.ijhcs.2013.06.003>
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109–125. <https://doi.org/10.1057/jit.2010.6>
- Krasnova, H., & Veltri, N. F. (2010). Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. *2010 43rd Hawaii International Conference on System Sciences (HICSS)*, 1–10. <https://doi.org/10.1109/HICSS.2010.307>
- Kwan, V. S., Bond, M. H., & Singelis, T. M. (1997). Pancultural explanations for life satisfaction: Adding relationship harmony to self-esteem. *Journal of Personality and Social Psychology*, 73(5), 1038–1051.
- Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who wants to know what when? Privacy preference determinants in ubiquitous computing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 724–725. <https://doi.org/10.1145/765891.765952>
- Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M.-H. C. (2017). Cross-Cultural Privacy Prediction. *Proceedings on Privacy Enhancing Technologies*, 3(2).
- Lipford, H. R., Hull, G., Latulipe, C., Besmer, A., & Watson, J. (2009). Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. *Computational Science and Engineering, 2009. CSE'09. International Conference On*, 4, 985–989. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5283751

- Lo, J. (2010). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. *AMCIS 2010 Proceedings*.
<https://aisel.aisnet.org/amcis2010/110>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355.
<https://doi.org/10.1287/isre.1040.0032>
- Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, *11*(1), 35–57. <https://doi.org/10.1287/orsc.11.1.35.12567>
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125. <https://doi.org/10.1057/ejis.2013.17>
- Min, J. (2015). Personal information concerns and provision in social network sites: Interplay between secure preservation and true presentation. *Journal of the Association for Information Science and Technology*, n/a-n/a. <https://doi.org/10.1002/asi.23376>
- Min, J., & Kim, B. (2014). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, n/a-n/a. <https://doi.org/10.1002/asi.23206>
- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.
<https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Oyserman, D., Coon, H. M., & Kemmelmeier, M. (2002). Rethinking individualism and collectivism: Evaluation of theoretical assumptions and meta-analyses. *Psychological Bulletin*, *128*(1), 3–72.
<https://doi.org/10.1037/0033-2909.128.1.3>
- Park, C., & Jun, J.-K. (2003). A cross-cultural comparison of Internet buying behavior: Effects of Internet usage, perceived risks, and innovativeness. *International Marketing Review*, *20*(5), 534–553.
<https://doi.org/10.1108/02651330310498771>

- Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.
- Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems, 19*(2), 181–195. <https://doi.org/10.1057/ejis.2010.15>
- Rui, J., & Stefanone, M. A. (2013). Strategic Self-presentation Online: A Cross-cultural Study. *Comput. Hum. Behav., 29*(1), 110–118. <https://doi.org/10.1016/j.chb.2012.07.022>
- Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing, 13*(6), 401–412. <https://doi.org/10.1007/s00779-008-0214-3>
- Schimmack, U., Oishi, S., & Diener, E. (2005). Individualism: A Valid and Important Dimension of Cultural Differences Between Nations. *Personality and Social Psychology Review, 9*(1), 17–31. https://doi.org/10.1207/s15327957pspr0901_2
- Schwartz, S. H. (1994). Beyond individualism/collectivism: New cultural dimensions of values. In U. Kim, H. C. Triandis, Ç. Kâğıtçıbaşı, S. -C, & G. Yoon (Eds.), *Individualism and collectivism: Theory, method, and applications* (pp. 85–119). Sage Publications, Inc.
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, 2347–2356*. <https://doi.org/10.1145/2556288.2557421>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Q., 35*(4), 989–1016.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167–196. <https://doi.org/10.2307/249477>
- Son, J.-Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly, 32*(3), 503–529.
- Steenkamp, J.-B. E. M., & Geyskens, I. (2006). How Country Characteristics Affect the Perceived Value of Web Sites. *Journal of Marketing, 70*(3), 136–150. <https://doi.org/10.1509/jmkg.70.3.136>

- Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), 36–49. <https://doi.org/10.1287/isre.13.1.36.97>
- Strater, K., & Lipford, H. R. (2008). Strategies and Struggles with Privacy in an Online Social Networking Community. *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1*, 111–119. <http://dl.acm.org/citation.cfm?id=1531514.1531530>
- Tang, K., Lin, J., Hong, J., Siewiorek, D., & Sadeh, N. (2010). Rethinking location sharing: Exploring the implications of social-driven vs. Purpose-driven location sharing. *Proceedings of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing*, 85–94. <https://doi.org/10.1145/1864349.1864363>
- Triandis, Harry C., Bontempo, R., Villareal, M. J., Asai, M., & Lucca, N. (1988). Individualism and collectivism: Cross-cultural perspectives on self-ingroup relationships. *Journal of Personality and Social Psychology*, 54(2), 323.
- Triandis, Harry Charalambos. (1995). *Individualism & collectivism: Vol. xv*. Westview Press.
- Tsoi, H. K., & Chen, L. (2011). From Privacy Concern to Uses of Social Network Sites: A Cultural Comparison via User Survey. *Privacy, Security, Risk and Trust (Passat), 2011 Ieee Third International Conference on and 2011 Ieee Third International Conference on Social Computing (Socialcom)*, 457–464. <https://doi.org/10.1109/PASSAT/SocialCom.2011.71>
- Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36. <https://doi.org/10.1177/0270467607311484>
- Wang, Y., Li, Y., & Tang, J. (2015). Dwelling and Fleeting Encounters: Exploring Why People Use WeChat - A Mobile Instant Messenger. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, 1543–1548. <https://doi.org/10.1145/2702613.2732762>
- Wang, Y., Norcie, G., & Cranor, L. F. (2011). Who is Concerned About What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. *Proceedings of the 4th International*

- Conference on Trust and Trustworthy Computing*, 146–153.
<http://dl.acm.org/citation.cfm?id=2022245.2022260>
- Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. *International Conference on Trust and Trustworthy Computing*, 146–153. http://link.springer.com/10.1007%2F978-3-642-21599-5_11
- Wheeler, L., Reis, H. T., & Bond, M. H. (1989). Collectivism-individualism in everyday social life: The middle kingdom and the melting pot. *Journal of Personality and Social Psychology*, 57(1), 79–86.
<https://doi.org/10.1037/0022-3514.57.1.79>
- Wheless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, 2(4), 338–346.
- Wiese, J., Kelley, P. G., Cranor, L. F., Dabbish, L., Hong, J. I., & Zimmerman, J. (2011). Are you close with me? Are you nearby?: investigating social groups, closeness, and willingness to share. *Proc. UbiComp 2011*, 197–206. <https://doi.org/10.1145/2030112.2030140>
- Wilkinson, D., Namara, M., Badillo-Urquiola, K., Wisniewski, P. J., Knijnenburg, B. P., Page, X., Toch, E., & Romano-Bergstrom, J. (2018). Moving Beyond a “One-size Fits All”: Exploring Individual Differences in Privacy. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, W16:1–W16:8. <https://doi.org/10.1145/3170427.3170617>
- Wisniewski, P., Lipford, H., & Wilson, D. (2012). Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 609–618. <https://doi.org/10.1145/2207676.2207761>
- Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, 26(3), 135–174. <https://doi.org/10.2753/MIS0742-1222260305>
- Yamagishi, T. (1988). The Provision of a Sanctioning System in the United States and Japan. *Social Psychology Quarterly*, 51(3), 265–271. <https://doi.org/10.2307/2786924>
- Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*, 18(2), 129–166. <https://doi.org/10.1007/BF02249397>

APPENDIX

		Overall	US	KR	CN
Mean age		30	38	29	30
Gender (% of Male)		45.47	44.02	49.51	44.04
Education (%)	Primary School	0.78	0	2.3	0.49
	High School	20.45	24.83	28.52	9.73
	Associate or other 2-year degree	18.29	22.12	15.08	16.55
	Four-year college	43.49	40.18	44.59	46.23
	Graduate school	17	12.87	9.5	27

A.1 Demographic information of survey participants

Factors	Items	Loading
General Self-Disclosure Amount AVE = 0.714	I frequently talk about myself on Facebook.	0.879
	I often discuss my feelings on Facebook.	0.925
	I usually write about myself extensively on Facebook.	0.885
	I often express my personal beliefs and opinions on Facebook.	0.816
	I disclose my close relationships with other people on Facebook.	0.739
	I often disclose my concerns and fears on Facebook.	0.811
Information Privacy Concern AVE = 0.625	I believe that my information privacy is invaded when control is lost or unwillingly reduced.	0.661
	It bothers me if my friends on Facebook reveal the personal information I shared on Facebook to others.	0.814
	It is very important to me that I am aware and knowledgeable about how the information I shared will be used by my friends on Facebook.	0.847
	When my friends on Facebook want to use the information I shared on Facebook, they should let me know first.	0.827
Interactional Privacy Concern AVE = 0.675	It bothers me when my friends on Facebook “poke” (send a greeting message) me unexpectedly.	0.758
	It bothers me when my friends on Facebook start a conversation with me unexpectedly.	0.860
	It bothers me if I am interrupted by irrelevant messages or information from my friends on Facebook.	0.836
Psychological Privacy Concern AVE = 0.743	It bothers me if my friends on Facebook publicly dislike the contents I post.	0.763
	It bothers me if my friends on Facebook joke about the content I post.	0.843
	It bothers me if my friends on Facebook judge my mood or feelings I shared in my space.	0.927
	It bothers me if my friends on Facebook judge me about my opinions.	0.906
Perceived Risk AVE = 0.798	In general, it would be risky to share information on Facebook with this friend.	0.895
	There would be high potential for loss if I share the information on my Facebook with this friend.	0.894

	There would be too much uncertainty associated with sharing information on Facebook with this friend.	0.911
	Sharing information on Facebook with this friend would create many unexpected problems.	0.873
Demographic information disclosure AVE = 0.530	Gender	0.682
	Age	0.751
	My e-mail address	0.699
	My mailing address	0.773
	My phone number	0.731
Social information disclosure AVE = 0.555	Photo with my image	0.741
	Political views	0.755
	My educational background	0.807
	Name of my college	0.660
	My friend list	0.774
	Interests (favorite movies, books, etc.)	0.719
	Status updates	0.742
	Shared links	0.756

A.2. Item descriptions and factor loadings. Note: “Facebook” was replaced by “WeChat” in Chinese survey.

Model	Name	χ^2 (df)	$\Delta\chi^2$ (df)	CFI	TLI	RMSEA	Notes
Other Factors	Configural	1073.085 (537)***	-	0.902	0.886	0.088	Everything free
	Full metric	1136.757 (569)***	63.673 (32) p <.05	0.897	0.886	0.088	Equal factor loadings
	Partial metric	1114.815 (566)***	41.730 (29) p > .05 Compared with configural	0.900	0.889	0.086	3 factor loadings are freed: CONCERN3 in Korean PSYCHO3 in China AMOUNT3 in China
	Scalar	1344.205 (601)***	229.39 (35) p <.05 Compared with partial metric	0.865	0.858	0.098	Equal factor loadings and intercepts.
Disclosure Factors	Configural	414.954(192)	-	0.846	0.813	0.095	Everything free
	Partial scalar	426.597(206)	20.721(14) p>0.1 Compared with configural	0.848	0.827	0.091	4 intercepts are freed in US.
	Scalar	474.858(210)	72.405 (18) p <.05 Compared with configural	0.846	0.813	0.095	Equal factor loadings and intercepts.

A.3 Results of measurement invariance tests (**p<.001).