Information & Management 54 (2017) 851–865

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use

Tabitha L. James[a,*], Linda Wallace[b], Merrill Warkentin[c], Byung Cho Kim[d], Stéphane E. Collignon[e]

[a] Department of Business Information Technology, Pamplin College of Business, Virginia Tech, 1007 Pamplin Hall, Blacksburg, VA 24061, USA
[b] Department of Accounting and Information Systems, Pamplin College of Business, Virginia Tech, 1007 Pamplin Hall, Blacksburg, VA 24061, USA
[c] Department of Management and Information Systems, College of Business, Mississippi State University, Mississippi State, MS 39762, USA
[d] Department of Logistics, Service & Operations Management, College of Business, Korea University, Anam-dong, Seongbuk-gu, Seoul 136-701, Republic of Korea
[e] Department of Management Information Systems, College of Business and Economics, West Virginia University, 1601 University Ave., PO Box 6025, Morgantown, WV 26506-6025, USA

ARTICLE INFO

Article history:
Received 23 October 2015
Received in revised form 26 October 2016
Accepted 4 January 2017
Available online 10 January 2017

Keywords:
Online social networks
Facebook
Perceived shared risk
Information exposure
Privacy concern
Cross-cultural analysis

ABSTRACT

People using online social networks (OSNs) exchange information through posts of multimedia content, which may contain others' information. Our study contributes to the privacy literature by examining individuals' perceptions of the risk their OSN activity poses to others' information. We introduce the concept "*perceived shared risk*," which includes OSN users' perceived *severity* and *susceptibility* of exposing others' information. Results indicate culture, concerns regarding one's own information, and Facebook information disclosure self-efficacy influence both risk components. We also identify a correlation between perceived shared risk and the use of OSN privacy controls.

1. Introduction

Online social networks (OSNs) have gained widespread acceptance across the globe as a platform for online socialization. One consequence of socializing (through online and offline) is that other people are often referenced as they are frequently a part of our daily activities and important events. When we talk about, or show pictures of, events in our lives, we often discuss the participation of others in those activities or show group pictures from the events. Consequently, while relating our life events, we share information about others. For example, an individual may take a picture of his or her child and the child's friend at a birthday party and post it on Facebook. In so doing, that individual is exposing the information related to both his or her own child (e.g., image) and the other child (e.g., the identity of the other child). In this scenario, the individual is also exposing some of his or her own information (e.g., the identity of his or her child) and similar information related to the parents of the other child. Of interest in the present study is whether the person who shares information through an OSN is considering the risk that he or she poses to others whose information is being shared through the user's OSN activity.

Posting a picture of one's child and the child's friend at a birthday party on an OSN is a common practice in today's society. However, this example illustrates the concept of co-owned information from the theory of Communication Privacy Management (CPM) [1]. For example, the photographer parent who took the picture regards the image as his or her property. The child of the photographer is also a stakeholder of the image because it is an image of the child. The child's friend would have a similar interest in the image. In addition, the other parents may feel ownership of the photo because it also depicts their child. Finally, the individuals holding the birthday party may feel that they also deserve ownership of the photo. Thus, the photo is co-owned information, and its sharing may impact each of the owners. Although concern over the exposure and use of one's own information has been

* Corresponding author.
E-mail addresses: tajames@vt.edu, stephane@vt.edu (T.L. James), wallacel@vt.edu (L. Wallace), m.warkentin@msstate.edu (M. Warkentin), bkim@korea.ac.kr (B.C. Kim), stephane.collignon@mail.wvu.edu (S.E. Collignon).

http://dx.doi.org/10.1016/j.im.2017.01.001
0378-7206/

frequently studied, individuals' perceptions of the risk their OSN activity poses to others' information has not been well studied. The latter is an important first step in studying the intricacies of information disclosure decisions in situations where information is co-owned.

In the case of co-owned information, there are many possible undesirable consequences of information disclosure to individuals with an ownership stake. The consequences can be exacerbated in an online environment in ways that are often difficult for users to envision. Suggested consequences include "inadvertent disclosure of personal information, damaged reputation due to rumors and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft" [2,p. 84]. Thus, it is crucial to understand individuals' perceptions of the risk their OSN activity poses to others' information, what influences that perception of risk, and how the perception of that risk affects the privacy mechanisms that may protect co-owned information.

Privacy research in the information systems (IS) literature has evolved from investigations of individual privacy concerns regarding the way companies handle one's information to a more diverse array of concerns, such as how peers handle one's information, as OSN use has become mainstream. Early privacy research in the IS literature focused on individuals' concerns over specific collection and mishandling of their own personal information by companies. For example, individuals' concerns over collection of personal information, unauthorized secondary use, improper access, and handling errors by companies were analyzed by Smith et al. [3]. Later studies explored concerns over collection, control, and awareness in the context of personal information disclosure to companies and suggested that these Internet users' information privacy concerns positively influence *risk beliefs,* which are defined as "the expectation that a high potential for loss is associated with the release of personal information to the firm" [4,p. 341]. Dinev and Hart [5] explored how individuals' risk beliefs influenced their willingness to disclose their information to e-commerce companies. They categorized two constructs under the category "risk beliefs" (Internet privacy concerns and perceived Internet privacy risk) and suggested that Internet privacy concerns comprised an individual's concern that his or her personal information might be misused, which was modeled as being influenced by perceived Internet privacy risk that was defined as general concerns about a company misusing collected personal information [5]. The authors took a similar modeling approach to explore cross-cultural differences in personal information disclosure to e-commerce companies [5]. More recent research has modeled perceived risk as "a function of perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations" and measured it by looking primarily at perceived access or loss of personal information [6,p. 302]. Dinev et al. [6]'s model also suggested that individuals' perceived privacy was influenced by perceived information control and perceived risk. This brief review illustrates that privacy studies in IS have primarily focused on individuals' concern over the disclosure and handling of their own information by companies online. Only recently have IS studies begun to consider a wider swath of information disclosure considerations. For example, noting the importance of co-owned information and the uniqueness of information disclosure decisions on OSNs, Chen et al. [7] explore individuals' concern over their personal information being disclosed by their peers. Our study contributes to this body of literature by focusing on the exploration of individuals' perceptions of the risk that their own OSN activity will pose to others. We provide a unique perspective because our study examines individuals' perception of how their own OSN behavior impacts other people rather than how the actions of other people or organizations affect their own privacy. Further, we provide insight into how the consideration of others affects one's OSN use decisions.

We introduce the interpersonal concept of *perceived shared risk of exposing others' information* and conceptualize it as having two components typically associated with risk: (1) the perceived *severity* of exposing others' information as a result of a user's OSN use and (2) the perceived *susceptibility* of others to information exposure as a result of a user's OSN use. Previous literature [8] has explored privacy with the theoretical lens of the protection motivation theory (PMT), suggesting that the motivation to protect oneself from harm (e.g., privacy invasion) stems from an assessment of both the perceived susceptibility of the entity to the risk and the perceived severity of realization of the risk (e.g., information exposure). The assessment of the severity and susceptibility of the risk (in our case, severity and susceptibility of others' information exposure through a user's OSN use) may influence whether behaviors to mitigate the perceived risk are enacted (e.g., privacy controls).

Furthermore, we examine several antecedents and covariates that have been noted in the literature as having an influence on how risk and privacy are managed. First, we collect data in both the United States and South Korea to explore the relationship between culture and perceived shared risk. Previous studies have suggested cultural distinctions in how privacy, risk, and decision-making for others are considered [1,9–15]. Second, we examine the relationship between perceived shared risk and the commonly measured "concern for information privacy" (CFIP), which measures individual perceptions of the sharing and use of one's own information. Previous work on risk has suggested that people consider social values, norms, and training when making decisions for others [10,16]; thus, we explore the relationship between an individual's concern for their own information and the perception of how their OSN activity may impact others' information. Third, we examine the relationship between Facebook information disclosure self-efficacy, which addresses the perceived competency of the user regarding information disclosure on Facebook, and perceived shared risk. Previous research has suggested that users with a higher self-efficacy in different types of OSN use are likely to have increased socialization and information disclosure (e.g., have more friends, share more information about themselves), be exposed to more risk from their use, and be considerate of outcomes in evaluating their competency [8,17–20]. Therefore, we explore if individuals' perceived competency with actions of sharing information on OSNs will influence how they see the risk of those actions to others. In addition, we test several covariates that have been associated with personal privacy and risk in previous research. Finally, we test the influence of perceived shared risk on the use of Facebook privacy controls that could be leveraged to protect others' information.

By many measures, socialization using online platforms has become extremely popular. Facebook, in particular, has experienced unparalleled popularity. A recent Nielsen survey found that Americans spend more time on Facebook than on any other website [21]. As of December 2015, Facebook claims 1.04 and 1.59 billion active daily and monthly users, respectively (http://newsroom.fb.com/Key-Facts). A recent Pew Internet report on Facebook usage found that the highest usage activities on Facebook were those that involved other people's content, such as commenting on someone else's post or photo or "Liking" content another user posted [22], which points to a trend of using Facebook in an increasingly public and interactive style. In fact, it has been suggested that "mass adoption of social-networking websites of all shapes and sizes points to a larger movement, an evolution in human social interaction" [23]. Thus, individuals must adapt to the

emerging peculiarities of socialization over the Internet, one component of which is the determination of how to consider others while interacting socially online. Because Facebook is one of the most popular and frequently investigated OSNs in the literature, we chose to focus our efforts on how Facebook users perceive their own activities as affecting the privacy of others.

It has become increasingly challenging to monitor the information about oneself that is broadcast online, resulting in online reputational concerns plaguing individuals and companies [24]. The possibility of the permanence and broad dissemination of shared information are suggested as distinguishing characteristics that change the nature of communication in an online environment [25]. Because tools to control the spread of one's information are limited, individuals must often rely on the good judgment of others to protect their information from broad public exposure. Thus, it is extremely important to measure an interpersonal perception of shared risk—the perception of one's own culpability in exposing others' information. Our study takes one of the first steps toward examining this phenomenon.

The remaining paper is organized as follows. In Section 2, we establish the theoretical foundation for our hypotheses. The methodology and the analysis of the theoretical model are presented in Section 3. A discussion of the results and their implications are provided in Section 4, followed by contributions, limitations, and ideas for future research in Section 5 and concluding remarks in Section 6.

2. Theoretical foundation and hypotheses development

Fig. 1 provides a high-level overview of our research model. Our primary contribution is to introduce the concept of perceived shared risk of information exposure and better understand its implications in an OSN environment (i.e., Facebook). In the next section, on the basis of previous literature, we conceptualize perceived shared risk of information exposure as having two components: the susceptibility of others to information exposure by one's own Facebook activity and the severity of the possible exposure. Ideally, it would be valuable to determine if perceived shared risk will influence behaviors that could protect privacy. However, we take an initial step toward this goal by examining whether others' considerations influence the decision to use Facebook privacy controls. This behavior could be leveraged to protect others' information; that is, one could limit others' information exposure through the application of Facebook privacy controls.

We examine the factors that may influence perceived shared risk of information exposure. Specifically, we examine (1) collectivistic/individualistic cultural orientation, (2) individual CFIP, and (3) Facebook information disclosure self-efficacy. We develop the argument for these relationships in the following sections. In addition, we examine several covariates commonly associated with risk: gender, age, and experience duration. Our model provides a unique examination of the consideration of the exposure of others' information by Facebook users.

2.1. Introducing the concept of perceived shared risk and exploring its influence on privacy protection behaviors

In this study, we center our model on a conceptualization of perceived shared risk of information exposure that explores how an individual perceives the potential for his or her OSN activity to threaten the privacy of other individuals. Therefore, we provide a complementary view to those studies that have examined perceived privacy risk or privacy concern related to one's own

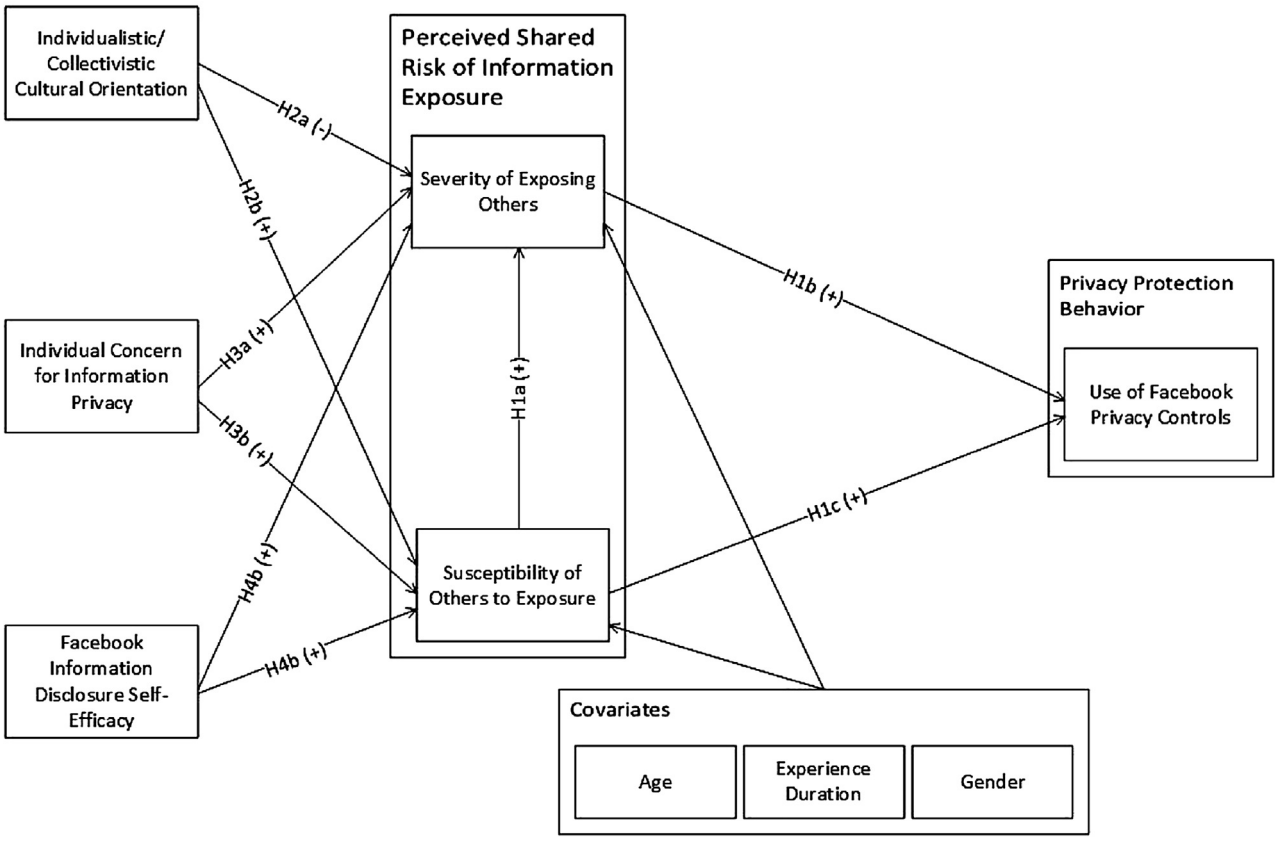

Fig. 1. Conceptual Model to Study Perceived Shared Risk of Information Exposure.

information [5,6,8,9,17,26–29] or individual privacy concern regarding peer disclosure of one's own information [7]. To formulate perceived shared risk, we draw on the PMT [30,31] description of risk as consisting of two components: susceptibility and severity. This approach has been previously used to study individual privacy by Youn [8,17] and Youn and Hall [28], and we assert that the threat landscape in the context of our focal phenomenon is consistent with the traditional threat landscapes evaluated through the theoretical lens of the PMT. Drawing on this foundation, we propose that for the OSN user to fully assess the risk of exposing others' information, he or she must consider both the *susceptibility* of the other party to unwanted exposure and the *severity* of the impact of the exposure. Perceived susceptibility refers to an individual's perception of the likelihood of an event happening to an individual. In the focal context, this means examining the Facebook user's perception of the susceptibility of other people to information exposure as a result of the user's Facebook activity. Perceived severity reflects the magnitude of the possible effect of the occurrence of an event. In our study, the event encompasses negative consequences resulting from a user exposing someone else's personal information through the user's activity on Facebook.

Most privacy studies in IS have been concerned with how individuals view issues related to the disclosure and use of their *own* personal information. Two concepts are common in the IS literature on individual privacy: perceived risk and concern for privacy [5,6,9,26,27,29]. Perceived risk revolves around an individual's perception of how personal information could be misused in general [5] or "the expectation that a high potential for loss is associated with the release of personal information to the firm" [4,p. 341]. For example, does the individual believe that any individual's information transmitted over the Internet could be misused or given to a third party without the owner's consent? Concern for privacy typically refers to individual's concerns about what will happen to his or her information once he or she has submitted that information online [5]. For example, is the individual worried about what will be done with the information he or she shares or whether someone else will be able to locate that information?

In other words, individual perceived risk in IS privacy studies often relates to individual perceptions of the likelihood of (usually unwanted) information exposure in general, whereas concern for privacy represents the individual's worry over unwanted exposure or misuse of his or her personal information in particular, thus providing a view of the importance that an individual attaches to privacy. These two concepts are theoretically aligned with susceptibility to information exposure, often labeled "perceived privacy risk" or "perceived vulnerability," and severity of information exposure, often labeled "privacy concern." In fact, perceived privacy risk and privacy concern have been categorized together under "risk beliefs" in past studies [5].[1]

[1] The IS literature has exhibited inconsistencies in the use of the terms "privacy concern" and "risk." We have relied on our references for our definitions of the constructs. For example, Dinev and Hart [5] introduced the "concern for privacy" scale that we adopted in the current study, and we retained their terminology. We explored individuals' perceptions of the risk or threat they pose to others' information by modeling risk as perceived susceptibility and severity, adapting scales developed for measuring these constructs in the context of protection motivation [8,28,32]. Our risk constructs explore individuals' perceptions of severity and susceptibility of disclosure of others' information resulting from the individual's OSN use, which distinguishes our constructs from any others in the IS literature with regard to the ownership considerations of the information being disclosed. Although this characteristic differentiates our study from previous work, it also illustrates a need for explicitly differentiating privacy concern and risk in the IS literature and opens the door for future research to further explore privacy perceptions with regard to various forms of co-owned information.

PMT describes motivation as a "positive linear function of the belief that an individual is susceptible to the perceived risk and the perceived risk is severe" [8,p. 92–93]. Youn [8] originally interpreted individual information disclosure risk as susceptibility and severity and suggested that both negatively impacted the intention to disclose personal information in her study of information disclosure by teenagers. Youn [8] also suggested, in accordance with PMT, that willingness to disclose individual information would negatively impact certain privacy protection behaviors in teenagers. Findings by Youn [8] suggest that although severity negatively impacted personal information disclosure, the relationship between susceptibility and personal information disclosure was not significant. Youn's [8] study also illustrated that as information disclosure willingness decreased, the teenagers' tendency toward behaviors such as providing inaccurate or incomplete information increased. These results influenced Youn's [17] later work, which was still grounded in PMT, where the conceptual model reflected the earlier findings to suggest that a "vulnerability to risks" directly impacted "levels of online privacy concerns." This relationship is consistent with many IS privacy studies that suggest perceived privacy risk [5,9] or perceived vulnerability [29] directly influence individual privacy concern. Youn [17] posited a direct relationship between privacy concern and privacy protection behaviors (e.g., information fabrication or seeking information from others to inform privacy decisions), and the empirical results of their study indicated that as levels of online privacy concern increased, the likelihood that respondents would seek information from others and refrain from information disclosure also increased.

Because individual privacy attitudes have previously been modeled as having the dimensions of susceptibility (i.e., perceived privacy risk or vulnerability) and severity of personal information exposure or misuse (i.e., privacy concern) [5,6,8,9,17,26,27,29], we follow a similar strategy to examine individuals' perception of the threat their OSN activity poses to others' information. Moreover, in previous studies, the relationship between susceptibility and severity has either been omitted [8] or typically modeled as susceptibility influencing severity [5,9,17,29]. We will propose the latter approach (H1a) and argue that heightened awareness of vulnerability to a threat often leads to increased perceptions of the severity of that threat. Therefore, we suggest that as individuals' perception of the susceptibility of exposing others' information through their own OSN use increases, the perceived severity of such information exposure will increase as well. In addition, prior research has suggested that susceptibility and severity may influence website use and privacy protection behaviors [5,8,9,17,27,28]. Similarly, we will examine the relationships between the perceived susceptibility and severity of exposing others' information through OSN use and the use of Facebook privacy controls.

Prior research has found mixed results between susceptibility, severity, and privacy protection mechanisms (unwillingness to disclose information, fabrication, privacy information seeking, etc.) [5,8,9,17,27,28]. Although previous research has explored the use of privacy protection mechanisms by OSN members, a common theme among these studies is that even if the users state that they are aware of the privacy risks associated with the OSN, they do not limit their OSN use [2,33,34]. Research has shown that individuals are often unaware that privacy-protecting mechanisms are available, and furthermore, even if they are aware, they often decline to use them [27,34,35]. Some of these contradictions could be attributed to the interesting incongruity in the use of privacy controls in an environment that counts on content generation as its major resource. Privacy controls restrict information flow through the OSN when widespread access by all members is important to the success of the platform [36]. Prior

studies do not show conclusive evidence for the use of privacy mechanisms even when considering the user's own protection [e.g.,37,38]. Therefore, it is unlikely that our study will provide strong support for the impact of perceived shared risk on the use of privacy protection mechanisms. However, for the sake of completeness and following similar argumentation from past studies, we suggest that those with a higher perceived shared risk of information exposure will be more likely to use Facebook's privacy controls because such a mechanism would at least reduce the size of the audience to which other's information was disclosed (i.e., the scope of the information disclosure) (H1b and H1c).

Following the logic in the previous discussion, we propose the following hypotheses:

H1a: An individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity is positively associated with the perceived severity of such an exposure.

H1b: An individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's personal information is positively associated with that individual's use of the Facebook privacy controls.

H1c: An individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity is positively associated with that individual's use of the Facebook privacy controls.

2.2. Antecedents of perceived shared risk

Many factors have been associated with individual privacy concern, perceived privacy risk, or privacy rule development [1,8,9,12,17,28,39,40]. Commonly included factors can be loosely categorized into personal characteristics (e.g., cultural orientation, gender, age, and personality traits) and contextual elements (e.g., domain knowledge, self-efficacy, privacy knowledge or awareness, perceived benefits, and experience duration). There are many differences in the form these constructs take, how they are operationalized in the models, and which relationships are proposed.

The primary contribution of our study is to introduce the concept of perceived shared risk and to develop an instrument to measure it. However, we also illustrate its use in the previous section by exploring the association of perceived shared risk to the use of Facebook privacy controls; similarly, in this section, we provide an initial investigation into the drivers of perceived shared risk. Although we leave more comprehensive examinations to future work, choosing in this paper to concentrate on the development of perceived shared risk, we begin an investigation into the determinants of perceived shared risk by exploring in detail one personal characteristic (cultural orientation) and one contextual element (Facebook information disclosure self-efficacy) frequently associated with individual privacy. In addition, we test gender, age, and experience duration as covariates in our empirical model below. Furthermore, because we introduce perceptions of the risk of exposing others' information, we explore the relationship between an individual's privacy concern for his or her own information and perceived shared risk.

Thus, in what follows, we consider three antecedents to perceived shared risk: individualistic/collectivistic cultural orientation, concern for the privacy of one's own information, and Facebook information disclosure self-efficacy. These antecedents and their associated hypotheses are described in the following sections.

2.2.1. Individualistic/collectivistic cultural orientation

Culture has often been associated with privacy. For example, in CPM, Petronio [1] argues that culture plays an important role in developing privacy rules. Altman [41] suggests that the mechanisms to regulate privacy may differ among cultures but that privacy itself may occur as a process in all cultures. Similarly, Laufer and Wolfe [11] propose that culture is an important environmental element that influences privacy perceptions. Several IS studies have incorporated culture into examinations of privacy or self-disclosure in technology environments [9,12–15,42]. Likewise, studies on risk have also explored the role of culture [43,44]. Well-known cultural distinctions exist between Eastern and Western cultures, and it has been suggested that a promising area of study is to determine "how cultural differences in the way that we view our social circles impact our willingness to share information online" [45,p. 233]. Thus, our study examines the relationship between individualistic/collectivistic cultural orientation and perceived shared risk, which extends the exploration of culture and privacy to encompass the considerations of others' information. The individualistic/collectivistic cultural distinction is particularly relevant to our study because collectivists tend to focus on others and consider themselves a representative of their in-group [46]. This is contrasted with the individualist's focus on the self and behavior that tends to place the self before others [46]. This contrast in the espoused values held by OSN users is naturally expected to be reflected in the perspectives on the impact of information disclosure on others.

One of the most noted cultural differences is the importance of independence or autonomy. Western cultures are described as individualistic, whereas Eastern cultures are often referred to as collectivistic. Individualistic cultures emphasize the importance of maintaining one's autonomy or independence from the group. In individualistic cultures, individual success and being able to accomplish things without other peoples' help are often considered positive. However, in collectivistic cultures, the good of the group is given preference over the needs of an individual [47]. Research has indicated that collectivists tend to define themselves as an "aspect or representative" of the group and "tend to establish more intimate, and long-lasting relationships than do individualists" [46,p. 368–369]. The view of the individual's place in the world and his or her connection to the rest of society can vary dramatically between cultures. This view is likely to influence how an individual interacts with others and what elements of that interaction are most crucial with respect to their own interests. Cultural characteristics influence the ways in which individuals consider outcomes and react in situations. In Eastern cultures, "the symbolic boundary between the self and other such selves is blurred and constantly negotiated through social interaction" [48, p. 225]. Given this view of Eastern people as being embedded within a collective, we argue that they will consider information exposure differently than people in Western cultures.

Miltgen and Peyrat-Guillard [12] found that individuals from cultures defined as collectivistic are more trusting and more likely to self-disclose. In other words, collectivistic individuals share information more readily with others; a collectivist may view himself or herself as more likely to expose others' information because he or she is simply looser with information in general. Furthermore, because collectivists tend to tie their self-definition to the group and form more intimate relationships with others, frequent information disclosure within a chosen group of friends may be viewed as typical interaction. The interpretation would be that the collectivist would perceive a high likelihood that his or her Facebook activity would expose others' information (H2b).

Following similar logic because the collectivist views others as an extension of himself or herself (i.e., his or her self-concept is grounded in the group), we argue that sharing information with others may not be perceived as a privacy violation. In fact, Bellman et al. [49,p. 315] suggest that collectivistic cultures "have a greater acceptance that groups, including organizations, can intrude on

the private life of the individual," so it could be argued that collectivists may not consider the exposure of others' information to be a negative event but rather a condition of living. Furthermore, the literature on culture and risk has suggested that collectivists have different perceptions of risk [43,44]. Specifically, research has found that collectivists are more likely to receive help if something goes wrong and are therefore less risk-adverse [43]. Subsequent work suggested that collectivists did not necessarily have different attitudes toward risk than individualists but rather that the collectivists' perception of the risk of the situation was different [44]. In other words, collectivists may view a situation as risky but not attach as much severity to the risk presented because they believe the group will lend support should something go wrong. Therefore, we argue that individuals with collectivistic tendencies will be less likely to view their Facebook activity exposing others' information to be severe (H2a).

2.2.2. Individual concern for privacy

A substantial body of research has studied online privacy [e.g.,6,42,50]. One popular stream of research in the IS literature is to examine antecedents to an individual's concern for privacy. For a valuable overview of this research, including a history of privacy and technology, see Junglas et al. [40], Smith et al. [42], and Bélanger and Crossler [50]. Much of this work has focused on the users' perceptions of how their information is treated by companies or organizations [e.g.,3,4]. Thus, the components of privacy concern are often related to the organization's handling of the information and privacy concern is used as an indicator to examine why people may or may not participate in online activities. For example, Smith et al. [3] proposed a multidimensional scale to measure CFIP, which was later confirmed by Stewart and Segars [51], and has been subsequently widely used in the IS research to examine behavioral intent (e.g., intent to transact) and privacy actions [50]. Dinev and Hart [5] developed an Internet privacy concerns construct based upon CFIP [3,52] to further examine online transactions. In the present study, we use a modified version of this scale to examine the respondents' (Facebook users') concern for their own privacy on Facebook.

Rather than exploring factors influencing the formation of an individual's concern for his or her own privacy, we posit that OSN users' concern for their own information privacy will influence their perception of the role that their activities have in posing a risk to others' information. Privacy concern has frequently been modeled as both a dependent and independent variable in IS research into various phenomena [42]. We suggest that people with a high concern for their own privacy (a "private person") will naturally transfer that concern to others because they possess a strong *a priori* privacy orientation. Because OSN use requires one to share information that is typically considered personal, it is likely that a private person would consider Facebook to be a privacy-violating technology and would be concerned for his or her own privacy on this platform. Previous studies of risk suggest that when making decisions for others, people will consider social values, norms, and training [10,16]. For example, one study found that financial planners were more cautious regarding their client's money than their own and suggested this may be due in part to training [16]. Thus, individuals who value their own privacy, possibly as a result of viewing privacy as a social value, norm, or as a result of training about consequences of information exposure, may apply similar importance to the information of others. Therefore, we hypothesize that an individual's concern for his or her own privacy will have a positive impact on the perceived susceptibility of others to information exposure as a result of the user's Facebook activity (H3b) and a positive impact on the perceived severity of another person's personal information being exposed as a result of that activity (H3a).

2.2.3. Facebook information disclosure self-efficacy

Self-efficacy is defined as "people's beliefs about their capabilities to produce designated levels of performance that exercise influence over events that affect their lives" [53,p. 71]. Furthermore, Bandura [53,p. 71] suggests that "self-efficacy beliefs determine how people feel, think, motivate themselves and behave." Similarly, we suggest that individuals' confidence with respect to operating in the environment (i.e., Facebook) in which they are making information disclosure decisions will impact their perceptions of the risk their Facebook activity poses to others' information. Specifically, we suggest that individuals' perceived competency with actions of sharing information on the OSN will influence how they see the risk of those actions to others. We define Facebook information disclosure self-efficacy as the user's self-reported competency to perform information disclosure tasks on the OSN.

Several forms of self-efficacy have been investigated in the IS literature. One of the most widely applied constructs is computer self-efficacy [54]. Internet self-efficacy has also been examined in previous work [55,56]. Notably, Gangadharbatla [56] examined the influence of Internet self-efficacy on the attitude toward social networking sites. Thus, self-efficacy is measured in relation to the environmental tasks of relevance. It has been recommended that to examine self-efficacy, the tasks of most importance should be carefully identified [57]. To this end, we consulted with domain experts and previous surveys of Facebook usage to determine common information disclosure tasks [22,58]. We incorporated tasks that (1) involve information disclosure, (2) involve socialization with others on the OSN, (3) are frequently performed, and (4) have different levels of difficulty [59]. To measure self-efficacy, our items were based upon those found in Bélanger et al. [60].

Youn [8,17] included a concept called "persuasion knowledge" in her examination of individual risk following a PMT conceptualization of susceptibility and severity. In these studies, Youn [8,17] suggests that persuasion knowledge measures individuals' confidence in their ability to understand and cope with tactics employed by marketers. She argues that such knowledge would influence how teenagers perceive and cope with marketers' data collection and use practices. Similarly, we suggest that perceived competency with information disclosure methods on Facebook would influence how users perceive the risk to others that is associated with their Facebook activity. Hsu et al. [18] argue that self-efficacy is positively related to personal and community outcome expectations in a study on knowledge sharing. They suggest that individuals anticipate outcomes from the performance of a task while evaluating their competency in performing that task. Livingstone and Helsper [19], contrary to expectations, found that online skills and Internet self-efficacy were associated with more online risks being encountered rather than fewer. Another study explored self-presentation self-efficacy on an OSN and found those with a higher self-presentation self-efficacy had more friends, completed more details in their profile, and had more group memberships [20]. These studies indicate that as competency with the platform increases, it is possible that more activity or socialization occurs, leading to the possibility of exposure to more risks. Thus, we argue that increased perceived competency with information disclosure activities on Facebook should correspond with the user having a better understanding of the ways information could be exposed and the consequences of the sharing.

Therefore, we expect that those users who report a high Facebook information disclosure self-efficacy perceive a higher susceptibility of others to information exposure as a result of their Facebook activity (H4b) and attach a higher severity to the occurrence (H4a). This is based upon previous research that has suggested that users with a higher self-efficacy in different types of OSN use are likely to have increased socialization and information

disclosure (e.g., have more friends, share more information about themselves), be exposed to more risk from their use, and be considerate of outcomes in evaluating their competency.

3. Method and analysis

3.1. Scale development and survey administration

The survey instrument was developed by predominantly using items adapted from existing IS literature (see Table 1). However, it was necessary to fully develop one of the scales because the construct had not previously been rigorously measured. We followed recognized procedural methods to develop and adapt the measurement scales [61,62]. To ensure that the questions reflected the intent of the study, expert panels were consulted. The expert panels consisted of individuals from two large US universities and one Korean university. Both subject matter experts and experts on survey development were recruited to participate in the panels. The resulting three panels included undergraduate and Masters students who were experienced Facebook users, and PhD students and faculty members from multiple departments who conduct academic research relying on instrument development. We gave these experts the instrument and an explanation of the study; we then asked them to comment on the phrasing and the appropriateness of items for the intended purpose. The resulting suggestions were cataloged and considered, with most being adopted. The expert panel's advice resulted in the reformulation of several items, benefiting from multiple perspectives, a practice which should ameliorate common method bias [63,64].

Following the consultation of the expert panels, the resulting instrument was pilot-tested using respondents from two large US universities. A total of 84 responses were collected, of which 74 were usable. On the basis of the exploratory factor analysis (EFA), several items were rephrased and a few items were dropped or added. A second pilot of the survey was performed at one US location. A useable sample of 72 responses resulted from the 92 surveys administered. The EFA indicated an acceptable factor structure for this pilot. The data for both pilots were collected using Qualtrics (http://www.qualtrics.com), an online survey provider.

The full data collection was conducted in both the USA and South Korea. The instrument resulting from the expert panels and the pilot studies was used. Again, Qualtrics was used to develop and administer the survey online. Participation in the study was voluntary, and respondents were recruited from two large southeastern universities in the USA and three universities in Korea. To recruit the participants, multiple instructors were asked to provide their students with the link to the survey; links were posted on class websites or were emailed to students. Anonymity was ensured to all participants; this discourages participants from answering what they consider is expected from them (social desirability bias or acquiescence bias) and consequently ameliorates common method variance [63]. The Korean sample was surveyed either in English or Korean depending on the primary language used in classroom instruction at the university. The Korean students who were surveyed in English were sufficiently proficient to attend part of their academic program in that language. Because the survey items were adopted from papers published in English-language scholarly journals, we translated our instrument into Korean following the accepted procedures to ensure translation quality; moreover, a back-translation procedure was also used to verify the acceptability and cross-cultural equivalence of the translation [66]. Those students whose classroom instruction was in Korean were administered the Korean version of the survey. We surveyed students because they are very active Facebook users, our target demographic. The use of students is appropriate if the students are familiar with the context and phenomenon under investigation [67,68] and is especially appropriate for this study because the demographics of Facebook users matches our sampling frame [69,70]. It was necessary to have only respondents who were active Facebook users participate in the study; therefore, a filter question was posed at the beginning of the survey asking if the respondents had logged into their Facebook account several times in the last month. If they answered negatively, they were thanked for their time and excluded from further participation. The construct measurement items were randomized using Qualtrics to reduce common method variance [63]. In addition, attention trap questions were added to the online instrument to allow for the removal of participants who may not have been actively and cognitively engaged in taking the survey [71]. The attention trap questions asked the participants to choose a specific multiple-choice answer from the selection. Any participant's response that did not correctly address the attention trap questions was expelled from the sample.

We obtained 912 responses from the USA and 573 responses from Korea. Of the 912 US responses, 58 were eliminated because the subjects were infrequent Facebook users. From the Korean data, 122 responses were unusable because of infrequent Facebook use. The manipulation check excluded 93 responses from the Korean collection and 57 from the US collection. Responses in which an answer to a construct item was left blank were also omitted, resulting in the exclusion of 34 more responses (24 from Korea and 10 from the USA). After the data were cleaned, the number of usable responses from the USA equaled 787 and from Korea equaled 334. This resulted in a final combined sample size of n = 1121.

Demographic information was collected from the respondents and is reported in Table 2. Although a little over half the sample was male, this demographic category was relatively evenly split. The majority of the respondents were college-aged students (18–25 years). Most of the sample was either Caucasian or Asian-Korean. Although some respondents reported some level of employment, the majority of the sample was made of full-time students.

Information regarding the respondents' technical exposure was also collected. In particular, the respondents were asked to provide an opinion regarding their technical skill. The majority of the respondents classified themselves as either intermediate or advanced computer users. We were also interested in more explicitly observing the extent of their Facebook use. The

Table 1
Sources for Survey Items.

Constructs:	Items Adapted From:
Individualistic/Collectivistic Cultural Orientation (CULTURE)	Hofstede [65], Srite and Karahanna [47]
Individual Concern for Information Privacy (PRIV)	Dinev and Hart [5]
Facebook Self-efficacy (SEFF)	Bélanger et al. [60]
Severity of Exposing Others (SEV)	Johnston and Warkentin [32]
Susceptibility of Others to Exposure (SUS)	Johnston and Warkentin [32]
Use of Facebook Privacy Controls (UPC)	Scale developed by authors

Table 2
Sample Demographic Information.

Gender		Age (years)		Ethnicity		Employment Status	
Male	573	18–20	623	Caucasian/White	629	Employed full-time	31
Female	548	21–25	434	African American/Black	86	Full-time student	955
		26–30	38	Latino/Hispanic (White, Black)	18	Employed part time or looking for full-time work	12
		31–35	14	Pacific Islander	1	Work part time and go to school part time	73
		36–54	11	Native American/Indian	4	Unemployed, not looking for work	20
		55 or Older	1	Middle-Eastern	3	Other	28
				Mixed Race	11		
				Other	6		
				Asian-Korean	334		
				Asian-Not Korean	27		

respondents were asked to report the number of years they had been on Facebook (i.e., experience duration) and how many Facebook friends they had. The response indicates that the target demographic was obtained because the majority of respondents reported being on Facebook for 2 or more years and having more than 100 friends. This indicates significant exposure to Facebook and relatively large online social circles. This information is detailed in Table 3.

The final items in the instrument, along with the mean and standard deviation of each item resulting from the final data collection, are provided in Table 4. Regarding the perceived shared risk constructs, i.e., severity and susceptibility, the descriptive statistics illustrated an interesting trend. The means for perceived severity ranged from 3.7 to 4, which is close to "Agree," and the standard deviations were some of the lowest for the scale. This indicates that the respondents consider that the consequences would be severe if another person's information was compromised because of the respondent's activity on Facebook. However, the items for perceived susceptibility were noticeably lower, and the standard deviations were higher. Thus, although the respondents feel that sharing another person's information through their use of Facebook could have severe consequences, they do not strongly feel that their use of Facebook is likely to result in such a sharing (mean approximately 3 = "neutral" for susceptibility items). The standard deviations for the perceived susceptibility items were high, indicating some variation in opinion.

The means for the items regarding the privacy controls were all between 3.8 and 3.9, which is close to "Agree." In other words, the respondents tended to agree that they use Facebook's privacy controls. However, the standard deviations for this set of items were large. This implies that there is some use of the privacy controls among the sample but that it is not consistent.

The antecedents to perceived shared risk in the model were individual concern for privacy, individualistic/collectivistic cultural orientation, and Facebook information disclosure self-efficacy. The means for the culture items were between "disagree" and "neutral," which implied a sample that overall was more individualistic than collectivistic. The responses from the USA outnumbered the responses from Korea, but the means from solely the Korean respondents indicated that they were not highly collectivistic either. Our sample from Korea was young and the survey included many English-speaking Koreans, both of which could imply Western influence. The privacy items showed that the respondents were concerned about the sharing or inappropriate use of their own information (means between "neutral" and "agree"). The Facebook information disclosure self-efficacy items showed the highest means of the instrument, all between 4.4 and 4.5, and the lowest standard deviations. This indicates that the respondents are confident in their ability to perform information disclosure tasks on Facebook. In other words, they report a high information disclosure self-efficacy with regard to Facebook.

3.2. Convergent validity, reliability, and discriminant validity

We ran our model in SmartPLS v. 3.2.1 and examined the output for indications of convergent validity. One of the culture items (CULTURE6) had a low factor loading (<0.30), and was therefore removed from further analysis to improve the reliability of the scale. Table 5 shows that all remaining items loaded cleanly on the appropriate factors. Factor loadings greater than 0.7 are recommended; however, with our sample size, loadings above 0.3 are respectable [72]. All our loadings eclipsed the cutoff value.

The factor loadings largely confirm convergent validity, which requires that all items within a factor be correlated with one another. There were also no substantial cross-loadings (i.e. the difference between any two cross-loadings is greater than 0.1, indicating that an item loads higher on the relevant factor) [73]. Table 6 gives the construct correlations, which are all less than 0.4. The low factor correlations, along with the absence of significant cross-loadings, confirm discriminant validity. A second check for discriminant validity can be conducted by examining the square root of the average variance extracted (AVE), given in Table 6 on the diagonal of the correlation matrix (i.e., the underlined value). It is suggested that discriminant validity is indicated if the square root of the AVE is greater than the correlations below it in the correlation table for that construct [74], which is the case for all of

Table 3
Technical Exposure of Sample.

Technical Proficiency		Length of Time on Facebook		Number of Friends on Facebook	
Novice	43	Less than 6 months	19	1–30	18
Intermediate	661	6 months–1 year	44	31–100	58
Advanced	412	1–2 years	184	101–300	222
		2–4 years	278	301–500	261
		4 or more years	596	501–1000	311
				1001+	251

Table 4
Descriptive Statistics for Survey Items.

Construct Indicator	Item	Mean	Std. Dev.
SEV1	The posting of somebody's personal information resulting from my Facebook activities could have severe consequences for that other person.	3.72	0.915
SEV2	If I shared somebody's personal information through Facebook, it could be harmful for that other person.	3.97	0.870
SEV3	If another person's personal information was exposed by my use of Facebook, this could be significant for that person.	3.90	0.837
SEV4	It could be unfortunate for a person if his or her personal information was spread by my Facebook activity.	4.01	0.848
SUS1	It is possible that other people's personal information may be shared by my use of Facebook.	3.50	1.036
SUS2	If I use Facebook, it is likely that the personal information of some other people may be posted.	3.30	1.059
SUS3	Others may experience leaks of personal information because of what I do on Facebook.	2.99	1.085
SUS4	By using Facebook, I risk exposing others' personal information.	3.44	0.996
UPC1	I use the privacy controls provided by Facebook.	3.91	1.144
UPC2	I control how I connect with people by managing the privacy settings provided by Facebook.	3.85	1.107
UPC3	I edit privacy settings provided by Facebook to control the viewership of the content I post.	3.80	1.148
CULTURE1	Being accepted as a member of a group is more important than having autonomy and independence.	2.64	0.911
CULTURE2	Being accepted as a member of a group is more important than being independent.	2.68	0.927
CULTURE3	Group success is more important than individual success.	2.98	0.908
CULTURE4	Being loyal to a group is more important than individual gain.	3.15	0.967
CULTURE5	Individual rewards are not as important as group welfare.	2.75	0.914
CULTURE6	It is more important for a manager to encourage loyalty and a sense of duty in subordinates than it is to encourage individual initiative.	3.20	0.923
PRIV1	I am concerned that information I submit on Facebook could be misused.	3.60	1.005
PRIV2	I am concerned because information I transmit on Facebook can be intercepted by third parties.	3.61	0.945
PRIV3	I am concerned about submitting personal information on Facebook because of what others might do with it.	3.65	0.961
PRIV4	I am concerned about submitting personal information on Facebook because it could be used in a way I did not foresee.	3.75	0.923
SEFF1	I know how to post pictures on Facebook.	4.48	0.710
SEFF2	I know how to update my status.	4.52	0.650
SEFF3	I know how to tag people on Facebook.	4.40	0.802
SEFF4	I know how to post something to a friend's wall.	4.49	0.708

(5-Point Likert Scale: 1 = Strongly Disagree to 5 = Strongly Agree).

our constructs. Thus, both tests confirm discriminant validity, which indicates that the factors are distinct.

SmartPLS provides several statistics that can be used to examine the reliability of the instruments: Cronbach's alpha, composite reliability (CR), and the AVE. These statistics indicate how reliable the instruments may be over time [75]. A Cronbach's alpha of greater than 0.7 is indicative of good reliability [76,77]. A CR of greater than 0.7 is also suggestive of good reliability, and it is recommended that the CR be greater than the AVE [72]. It is also suggested that the AVE should be greater than 0.5 [72,74]. All our scales have Cronbach's alphas and CRs of greater than 0.70, which is indicative of reliability. Furthermore, in each case, the CR is greater than the AVE. However, although the AVEs for all other scales are greater than 0.5, the culture scale has an AVE of less than 0.5 (0.434); although the other reliability statistics hold for the culture scale, the low AVE could indicate reliability issues with the culture scale. However, this scale is very widely used in IS research [47,65], and most of the reliability statistics are acceptable, so we used it to examine culture in our study. Future work should explore alternatives to this scale.

3.3. Cross-cultural equivalence

Because we used respondents from two different countries, a brief discussion of cross-cultural equivalence is necessary. Specifically, it is necessary to check for construct bias, method bias, or items bias [13]. First, to address construct bias, a factor analysis was performed separately on each country's data to determine if the results were similar. The same factor structure was obtained for both subsamples of the data, which indicates that our constructs were interpreted similarly in both countries (a lack of construct bias).

Table 5
Cross-loadings Table.

	Factor					
	1	2	3	4	5	6
UPC1	−0.102	0.206	0.212	0.153	−0.047	0.928
UPC2	−0.094	0.196	0.217	0.139	−0.015	0.932
UPC3	−0.088	0.210	0.188	0.166	−0.024	0.941
SEV1	−0.035	0.329	0.123	0.767	0.327	0.134
SEV2	−0.071	0.270	0.176	0.777	0.220	0.131
SEV3	−0.046	0.295	0.223	0.792	0.306	0.118
SEV4	−0.034	0.290	0.227	0.760	0.230	0.128
SUS1	0.053	0.221	0.138	0.278	0.811	−0.018
SUS2	0.097	0.207	0.064	0.198	0.747	−0.035
SUS3	0.134	0.259	0.013	0.216	0.778	−0.058
SUS4	0.080	0.278	0.121	0.369	0.755	0.006
SEFF1	−0.020	0.120	0.877	0.217	0.117	0.183
SEFF2	−0.060	0.153	0.901	0.241	0.091	0.199
SEFF3	−0.060	0.078	0.852	0.168	0.080	0.215
SEFF4	−0.055	0.148	0.889	0.214	0.103	0.181
CULTURE1	0.919	0.059	−0.070	−0.071	0.103	−0.071
CULTURE2	0.921	0.029	−0.036	−0.047	0.118	−0.132
CULTURE3	0.475	0.029	0.002	0.015	0.030	0.023
CULTURE4	0.392	0.041	0.032	0.005	0.008	0.081
CULTURE5	0.318	0.032	−0.051	0.009	0.006	0.024
PRIV1	0.060	0.782	0.101	0.264	0.348	0.123
PRIV2	0.079	0.827	0.107	0.297	0.299	0.195
PRIV3	0.015	0.827	0.121	0.335	0.176	0.207
PRIV4	0.001	0.834	0.146	0.363	0.197	0.195

To prevent method bias, we administered the survey on the same platform with the same instructions for both countries (Qualtrics). We surveyed respondents from both countries who were familiar with social networking and filtered out those who did not use Facebook. In addition, we surveyed college students in both countries to minimize the difference in demographics. Furthermore, we statistically examined the demographic differences between the two groups. We found that age with a $t(1120) = -17.445$ ($p < 0.001$) and number of Facebook friends with a $t(1124) = 22.219$ ($p < 0.001$) had statistically significant differences. Considering the means, the US respondents on average were slightly younger and had more Facebook friends. We computed the Cohen's d to determine the effect size. The Cohen's d for age was −1.05 ($r = 0.46$) and 1.46 ($r = 0.59$) for several Facebook friends. To account for this, we tested models including both variables as covariates to our model. Number of Facebook friends did not prove to have an impact on the independent variables, so this variable was not included in the model. Age was included as a covariate, as shown in Fig. 2.

Item bias can be introduced through translation problems and complex wordings of items. To reduce item bias, we administered the survey to both subsets of respondents in English (using South Koreans that took college courses in English, which suggests fluency), where possible, and used a back-translation procedure to verify the Korean language survey. We also used existing scales, where possible, and panel tested our survey items with content and method experts from both countries.

3.4. Structural model

The sample size for the present study was n = 1121. The model consisted of six latent variables. The structural model was tested in SmartPLS Version 3.2.1 (http://www.smartpls.de). This software tests the model using partial least squares (PLS) regression, which allows the relationships among multiple independent and dependent constructs to be modeled simultaneously [78,79]. Path coefficients, t-statistics, and p-values were generated using SmartPLS. PLS also provides an R-squared value for the endogenous variables. These statistics for the model considered in the present study are given in Fig. 2.

All paths in Fig. 2 are significant at the $p < 0.05$ level. H1c was significant, but the relationship was reversed from what we expected. The R-squared values for perceived severity and perceived susceptibility were quite reasonable. The R-squared value for the use of privacy controls was low, which is not unexpected because we tested only the influence of perceived shared risk on this behavior and not any of the other variables that have been shown to affect the use of privacy controls. We discuss the implications of these results in the next sections.

4. Discussion

Table 7 shows the results from testing our model, including the path coefficient and significance of each hypothesis. An examination of Fig. 2 and Table 7 illustrates that our antecedents explained a noteworthy amount of the variance for the perceived severity and perceived susceptibility. Furthermore, our results yield some important contributions to the field.

We explored the relationship between perceived susceptibility of others' information being exposed as a result of the user's Facebook activity and the severity of that occurring (H1a). A significant positive relationship (0.260, $p < 0.001$) was found between susceptibility and severity. This reinforces the previous findings that suggest that perceptions of vulnerability/susceptibility are positively associated with increased concern of privacy violations [5,9,17,29]. The result indicates that individuals who consider that it is likely that another person's information will be exposed through their Facebook activity are more likely to believe that such an information exposure is severe. Facebook is a social tool, and therefore, personal information is likely to be shared frequently because that is what people visit the OSN to see. Those individuals that perceive others to be vulnerable to information exposure through their OSN activity are cognizant that their socialization exposes others. Our findings indicate this understanding of the general vulnerability of exposing others' information leads to higher levels of severity being assigned to such an exposure. One interpretation of this may be that people who deem something as unlikely to happen may have trouble assigning severity to it (i.e., they contemplate the repercussions less because they do not believe their OSN activity is exposing others' information). In contrast, those who consider the likelihood of others' information being exposed as a result of their Facebook use to be high may attach severity to it more easily.

Table 6
Validity and Reliability.

Factor	Cronbach's Alpha	CR	AVE	CULTURE	PRIV	SEFF	SEV	SUS	UPC
CULTURE	0.770	0.764	0.434	0.659					
PRIV	0.835	0.890	0.669	0.049	0.818				
SEFF	0.903	0.932	0.774	−0.054	0.145	0.880			
SEV	0.777	0.857	0.599	−0.060	0.384	0.242	0.774		
SUS	0.778	0.856	0.598	0.117	0.316	0.112	0.353	0.773	
UPC	0.927	0.953	0.872	−0.101	0.219	0.219	0.165	−0.032	0.934

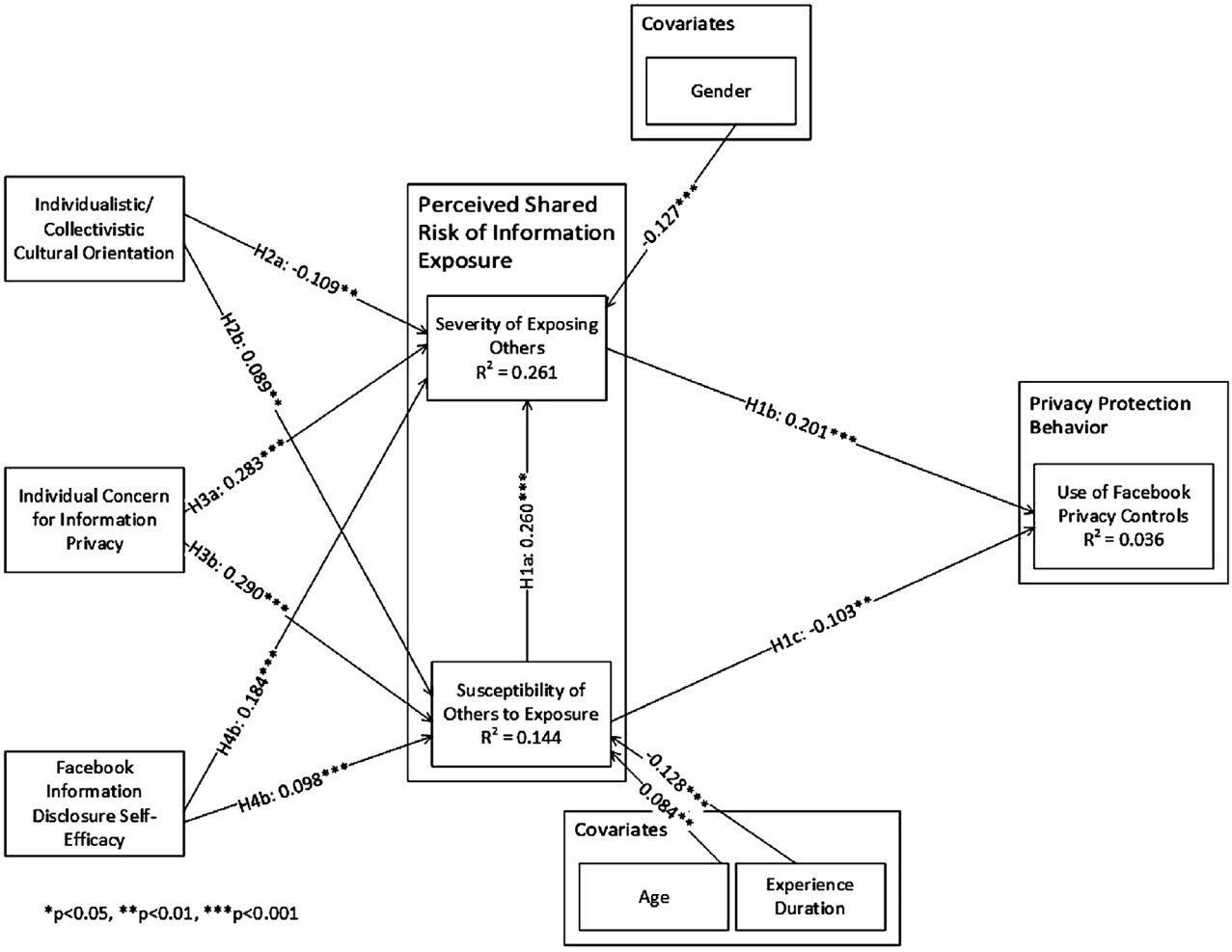

Fig. 2. Structural Model.

Table 7
Summarized Results.

	Hypothesis	Indication	Coef.	P
H1a	An individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity is positively associated with the perceived severity of such an exposure.	Supported	0.260	<0.001
H1b	An individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's personal information is positively associated with that individual's use of the Facebook privacy controls.	Supported	0.201	<0.001
H1c	An individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity is positively associated with that individual's use of the Facebook privacy controls.	Reversed	−0.103	0.001
H2a	Collectivistic cultural leanings are negatively associated with an individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's personal information.	Supported	−0.109	0.001
H2b	Collectivistic cultural leanings are positively associated with an individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity.	Supported	0.089	0.004
H3a	An individual's concern for his or her own information privacy is positively associated with an individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's personal information.	Supported	0.283	<0.001
H3b	An individual's concern for his or her own information privacy is positively associated with an individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity.	Supported	0.290	<0.001
H4a	Facebook self-efficacy is positively associated with an individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's personal information.	Supported	0.184	<0.001
H4b	Facebook self-efficacy is positively associated with an individual's perception of the susceptibility of others to personal information exposure as a result of his or her Facebook activity.	Supported	0.098	<0.001

We examined the influence of both elements of perceived shared risk of information exposure (susceptibility and severity) on the use of the privacy controls on Facebook. Perceived severity had a positive influence on the use of privacy controls (H1b: 0.201, $p < 0.001$), but perceived susceptibility had a negative influence (H1c: −0.103, $p < 0.01$). That is, users who thought that exposing others' information as a result of their Facebook use was severe were more likely to use the privacy controls. This relationship was as expected; as the severity of exposing others' information increased, the use of privacy controls increased. However, users who considered it likely that others' information would be exposed as a result of their Facebook use were less likely to use the privacy controls. This indicates that only if consequence (i.e., negative connotation) is associated with sharing others' information do users adopt this particular privacy behavior. One interpretation of this result is that understanding one's OSN activity exposes others' information is not enough to spur protective behavior; rather, the exposure of others' information has to be viewed as a negative outcome. Previous research has shown inconclusive evidence for the use of privacy mechanisms even when considering the user's own protection [e.g.,37,38], and our findings also show this to be the case regarding others' information. On a positive note, that the severity of exposing others' information is associated with higher use of OSN privacy controls suggests that if a user can be convinced that exposing others' information has a negative outcome, it is possible to convince them to use privacy protecting mechanisms that reduce that outcome.

We examined three antecedents (individualistic/collectivistic cultural orientation, individual CFIP, and Facebook information disclosure self-efficacy) to perceived shared risk that reveal some interesting insights. Individuals with collectivistic cultural leanings perceive others to be highly susceptible to information exposure as a result of their Facebook use but consider this exposure not to be severe. Individuals who have a high concern for their personal privacy and report high Facebook information disclosure self-efficacy tend to perceive others to be highly susceptible to information exposure as a result of the users' Facebook activity, and they perceive this exposure to be severe.

We measured espoused individualistic/collectivistic cultural orientation and identified a significant negative influence (H2a: −0.109, $p < 0.01$) on the perception of the severity of others' information being exposed, as hypothesized. That is, collectivistic cultural leanings suggest a lowered perception of severity, and individualistic cultural leanings suggest a higher perception of severity. A collectivistic culture encourages societal participation: members are expected to share with each other and to take care of each other. Collectivistic cultures place less emphasis on individual gain and emphasize doing things for the good of the collective (group). In this study, we suggested that collectivistic people see the exposure of others' information as less severe than individualistic people do. Collectivistic cultures are more open (less secretive) and place great importance on their interaction with others [48], so sharing information may be more common. In collectivistic cultures, people interact with each other to a greater extent and at a more personal level than in Western cultures, implying that privacy is viewed with a different lens [11] and may be tied to the scope of the shared information. In other words, exposing others' information may not be considered as severe as long as it is exposed within the intimate in-group. A weak positive relationship (H2b: 0.089, $p < 0.01$) was discovered between individualistic/collectivistic cultural orientation and perceived susceptibility of another person's information being exposed because of the Facebook action of the user. This indicates that users with a collectivistic cultural orientation are more likely to perceive others as being susceptible to information exposure as a result of their own Facebook activity. This aligns with collectivistic cultures being viewed as more open and likely to share more information. Thus, collectivists are more likely to expose others' information but consider that the exposure is not severe.

We hypothesized that individual privacy concern would positively impact an individual's perception of the severity of his or her Facebook activity leading to the exposure of another person's information and the perception of susceptibility of others to such an exposure. Privacy concern relates to the concern an individual has over his or her own information being exposed or misused. We argued that a person who was concerned with the handling and spread of his or her own information would transfer that concern to the treatment of other peoples' information. Therefore, a person with a high level of privacy concern will perceive the exposure of others' information by something he or she did on Facebook to be severe and also expect an exposure to be more likely to occur as a result of his or her activity on Facebook. We found substantial positive support for both relationships (H3a: 0.283, $p < 0.001$ and H3b: 0.290, $p < 0.001$). As expected, an individual with strong privacy concern would consider it severe if his or her own information was exposed, and therefore, he or she feels the same about the exposure of someone else's information. One interpretation of this finding is that because maintaining privacy is important to privacy-conscious individuals, they view the severity to be high if they were the reason that someone else's information was exposed. Similarly, we argue that a highly privacy-conscious person would regard it likely that someone else's information could be exposed through his or her Facebook activity because a highly private person tends to view Facebook as lacking privacy, given that its sole purpose is to encourage information exchange and interaction. Therefore, to a private individual, any activity at all on Facebook is likely to be viewed as capable of exposing someone's information.

Facebook information disclosure self-efficacy had a strong positive relationship (H4b: 0.185, $p < 0.001$) with an individual's perceived severity of others' information being exposed through his or her Facebook activity and a weak positive relationship (H4b: 0.097, $p < 0.01$) with perceived susceptibility of others to information exposure. This indicates that as users' confidence in their ability to use Facebook for information disclosure tasks grows, so does the perception of the severity of exposing others' information through their activity and susceptibility of others to information exposure. We based these hypotheses upon previous research that suggested that users with a higher self-efficacy in different types of OSN use are likely to have increased socialization and information disclosure (e.g., have more friends, share more information about themselves) [20], be exposed to more risk from their use [19], and be considerate of outcomes in evaluating their competency [18]. One interpretation of these results are that high levels of Facebook information disclosure self-efficacy are associated with a greater understanding of how information can be exposed on an OSN and deeper consideration of the outcomes of such exposure.

We also tested several covariates to perceived shared risk of information exposure: experience duration, number of Facebook friends, gender, and age. Youn [8] tested correlations between gender, age, and Internet use duration with individual risk (susceptibility and severity), finding negative correlations between gender and severity and susceptibility. Positive correlations were discovered between age and Internet use duration and severity and susceptibility. In our study, the number of Facebook friends was not found to have a significant relationship with either perceived shared risk component. Age was found to have a weakly significant positive relationship (0.083, $p < 0.01$) only with susceptibility of others to exposure. This suggests that the older the respondent, the more likely he or she is to perceive others to be susceptible to information exposure through his or her Facebook activity. As

experience duration (i.e., the length of time the user reports having a Facebook account) increases, the perception of susceptibility of others to information exposure decreases. No relationship was found between experience duration and severity of exposing others' information. This may indicate that the longer the users stay on Facebook, the more complacent they become in relation to harmful outcomes. Another explanation may be that, over time, Facebook users become less active on the platform, leading to decreased perceptions of susceptibility. Gender had a positive relationship with severity of exposing others' information, indicating that females tend to perceive exposing others' information through their OSN activity as less severe than males. No relationship was found between gender and susceptibility of others to exposure.

5. Contributions, limitations, and future research

In this study, we contribute to the information privacy literature by examining users' perceptions of the risk their OSN activity poses to others' information. This is an under-studied perspective on information disclosure because most studies concentrate on individual perceptions of privacy concern related to one's own information (e.g., organizational or peer use of one's personal information). Our contribution provides a step in the direction of exploring information disclosure decisions for co-owned information; that is, when the information one wants to share on an OSN involves not only one's own personal information but other people's information as well.

Our findings indicate that making a user more aware of the severity of exposing others could increase the use of OSN privacy controls, which are a privacy protection mechanism that does not severely limit the use of the platform. Thus, one suggestion for practice from our results would be to encourage people to make their friends aware of how they feel with regard to exposure of their personal information. It may be possible that simply telling friends that you would negatively view them posting a picture or talking about you on social media may be enough to encourage some limited protection behaviors. Future studies can consider the impact of such training or awareness on Facebook use in general and use of privacy protection mechanisms specifically.

Our study examined several antecedents to perceived shared risk of information exposure. Culture is commonly associated with privacy and risk beliefs, and our study illustrated that there is indeed a difference in perspectives between collectivists and individualists with respect to consideration of others' information exposure. We also found that our Korean participants had a lower collectivistic cultural orientation than expected. Interesting future research could include investigations of perceived shared risk in countries that may report stronger collectivistic leanings (e.g., China). In this study, we examined only the individualistic/collectivistic element of culture. Future studies can consider more granular examinations of culture and perceived shared risk. The present study explored the relationships between individual privacy concern and perceived shared risk of information exposure. However, as CFIP illustrates [3,51], individual privacy concern can be a function of granular information handling concerns. Furthermore, privacy studies have studied elements of privacy, such as awareness and control [4,6], that may have interesting implications for co-owned information. Future studies can explore variations on this theme by deepening the examination of both individual privacy-related antecedents to perceived shared risk (e.g., dispositional privacy, privacy awareness, privacy self-efficacy) and considering an expansion of the conceptualization of perceived shared risk following the roadmap laid out for individual privacy concern. One important extension of the present study relating to this suggestion is to include the benefits of OSN use in the perceived shared risk model that are tailored to perceived shared risk. Though the focus of the present study was to develop the notion of perceived shared risk, benefits that may counteract the risk are an important element of the privacy calculus [1,5,42,80].

The ideal way to protect other people's information is simply not to disclose anything the other individuals may want to remain confidential. However, information disclosure is the central driver of OSN functionality, and this stimulates further disclosure, especially for information that may drive interaction. The desire to participate may increase the likelihood of undesired information exposure. Therefore, the decision to share information becomes a part of a tradeoff between a desire to participate versus a desire to protect confidentiality [5,11]. The user's conundrum is either to violate the privacy of the other person or to restrict his or her participation on the platform, similar to classic gossip behavior.

There is also a potential conflict between what the OSN user considers private information and what the other person would want kept confidential. Deciding whether to disclose another's information relies on the judgment of the individual, and the societal norms of what is considered private. Therefore, users may feel that exposing someone's private information would have severe consequences but consider very little information to be private. The exploration of the privacy tradeoff and shifting attitudes on what is considered private are rich areas for future research, and our findings indicate that such exploration is necessary to increase the awareness of the impact a person's OSN use may have on others. There are many opportunities to further the examination of privacy from an interpersonal and co-owned information perspective. Developing new constructs that are contextualized to the consideration of others during information disclosure decisions would be interesting future research. For example, constructs or scales that explicitly examine privacy protection behaviors with respect to others' information could be developed.

6. Conclusion

This study considers privacy from a novel perspective—individual perceptions of the exposure of others' personal information through one's own OSN activity. Specifically, we introduce the concept of perceived shared risk as being composed of two components: severity of exposing others' information and susceptibility of others to information exposure from the user's OSN activity.

We also explore three antecedents that influence the consideration of the risk to others' information. We find that people with an individualistic cultural orientation, a high level of concern for their own privacy, and high Facebook information disclosure self-efficacy view exposing another person's personal information through their Facebook activity to be severe. Collectivistic cultural orientation, individual privacy concern, and Facebook information disclosure self-efficacy have significant positive relationships with perceived susceptibility.

Furthermore, we present findings that explore the impact of perceived shared risk on the use of Facebook privacy controls. Contrary to expectations, we found that those with a higher perceived susceptibility reported being less likely to use privacy controls. However, those with a higher perceived severity of exposing others' information were more likely to use Facebook's privacy controls. We suggest that the latter finding could reflect the view that the use of privacy controls would at least reduce the audience size to which other's information was disclosed (i.e., the scope of the information disclosure).

Although our study has developed the concept of perceived shared risk and provided an initial exploration of its use, we

believe that there are many interesting avenues that future research could explore with regard to consideration of others and co-owned information. Our study serves to introduce the concept of perceived shared risk, provides a rich examination of its drivers, and explores its influence on the use of Facebook privacy controls.

References

[1] S. Petronio, Boundaries of Privacy, State University of New York Press, Albany, NY, 2002.
[2] B. Debatin, J.P. Lovejoy, A.K. Horn, B.N. Hughes, Facebook and online privacy: attitudes, behaviors, and unintended consequences, J. Comput.-Mediat. Commun. 15 (2009) 83–108.
[3] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20 (1996) 167–196.
[4] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Inf. Syst. Res. 15 (2004) 336–355.
[5] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 17 (2006) 61–80.
[6] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inf. Syst. 22 (2013) 295–316.
[7] J. Chen, J.W. Ping, Y.C. Xu, B.C. Tan, Information privacy concern about peer disclosure in online social networks, IEEE Trans. Eng. Manag. 62 (2015) 311–324.
[8] S. Youn, Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach, J. Broadcast. Electron. Media 49 (2005) 86–110.
[9] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti, Privacy calculus model in e-commerce – a study of Italy and the United States, Eur. J. Inf. Syst. 15 (2006) 389–402.
[10] E.R. Stone, L. Allgaier, A social values analysis of self–other differences in decision making involving risk, Basic Appl. Soc. Psychol. 30 (2008) 114–129.
[11] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional developmental theory, J. Soc. Issues 33 (1977) 22–42.
[12] C.L. Miltgen, D. Peyrat-Guillard, Cultural and generational influence on privacy concerns: a qualitative study in seven European countries, Eur. J. Inf. Syst. 23 (2014) 103–125.
[13] C. Posey, P. Lowry, T. Roberts, T.S. Ellis, Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities, Eur. J. Inf. Syst. 19 (2010) 181–195.
[14] Y.-C. Ku, R. Chen, H. Zhang, Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan, Inf. Manag. 50 (2013) 571–581.
[15] K. Li, Z. Lin, X. Wang, An empirical analysis of users' privacy disclosure behaviors on social network sites, Inf. Manag. 52 (2015) 882–891.
[16] M.J. Roszkowski, G.E. Snelbecker, Effects of framing on measures of risk tolerance: financial planners are not immune, J. Behav. Econ. 19 (1990) 237–246.
[17] S. Youn, Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents, J. Consum. Aff. 43 (2009) 389–418.
[18] M.-H. Hsu, T.L. Ju, C.-H. Yen, C.-M. Chang, Knowledge sharing behavior in virtual communities: the relationship between trust, self-efficacy, and outcome expectations, Int. J. Hum. Comput. Stud. 65 (2007) 153–169.
[19] S. Livingstone, E. Helsper, Balancing opportunities and risks in teenagers' use of the internet: the role of online skills and internet self-efficacy, N. Media Soc. 12 (2009) 309–329.
[20] N.C. Krämer, S. Winter, Impression management 2.0: the relationship of self-esteem, extraversion, self-efficacy, and self-presentation within social networking sites, J. Media Psychol. 20 (2008) 106–116.
[21] Nielsen, Social Media Report Spending Time, Money, and Going Mobile, (2011) .
[22] K. Hampton, L.S. Goulet, L. Rainie, K. Purcell, in: P.I.R. Report (Ed.), Social Networking Sites and Our Lives, 2011.
[23] A.C. Weaver, B.B. Morrison, Social networking, Computer 41 (2008) 97–100.
[24] M.A. Fuller, M.A. Serva, J. Benamati, Seeing is believing: the transitory influence of reputation information on e-commerce trust and decision making, Decis. Sci. 38 (2007) 675–699.
[25] D. Rosenblum, What anyone can know: the privacy risks of social networking sites, IEEE Secur. Priv. 5 (2007) 40–49.
[26] H. Xu, H.-H. Teo, B. Tan, Predicting the adoption of location-based services: the role of trust and perceived privacy risk, ICIS 2005 Proceedings, Las Vegas, NV, 2005.
[27] M.J. Keith, S.C. Thompson, J. Hale, P.B. Lowry, C. Greer, Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior, Int. J. Hum. Comput. Stud. 71 (2013) 1163–1173.
[28] S. Youn, K. Hall, Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors, Cyberpsychol. Behav. 11 (2008) 763–765.
[29] T. Dinev, P. Hart, Internet privacy concerns and their antecedents-measurement validity and a regression model, Behav. Inf. Technol. 23 (2004) 413–422.
[30] R.W. Rogers, A protection motivation theory of fear appeals and attitude change, J. Psychol. 91 (1975) 93–114.
[31] R. Rogers, Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation, in: J. Cacioppo, R. Petty (Eds.), Social Psycho-Physicology, 1983, pp. 153–176 Guilford, New York.
[32] A.C. Johnston, M. Warkentin, Fear appeals and information security behaviors: an empirical study, MIS Q. 34 (2010) 549–566.
[33] E. Christofides, A. Muise, S. Desmarais, Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? CyberPsychol. Behav. 12 (2009) 341–345.
[34] A. Acquisti, R. Gross, Imagined communities: awareness, information sharing, and privacy on the Facebook, in: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies, Springer, Berlin, Heidelberg, 2006, pp. 36–58.
[35] R. Gross, A. Acquisti, Information revelation and privacy in online social networks, Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, ACM, Alexandria, VA, 2005, pp. 71–80.
[36] G.C. Kane, M. Alavi, G.J. Labianca, S.P. Borgatti, What's different about social media networks? A framework and research agenda, MIS Q. 38 (2013) 275–304.
[37] T. Govani, H. Pashley, Student Awareness of the Privacy Implications when Using Facebook, vol. 9(2005) , pp. 1–17 Unpublished paper presented at the Privacy Poster Fair at the Carnegie Mellon University School of Library and Information Science.
[38] H. Jones, J.H. Soltren, Facebook: threats to privacy, Project MAC: MIT Proj. Math. Comput. 1 (2005) 1–76.
[39] T. Dinev, J. Goo, Q. Hu, K. Nam, User behaviour towards protective information technologies: the role of national cultural differences, Inf. Syst. J. 19 (2009) 391–412.
[40] I.A. Junglas, N.A. Johnson, C. Spizmuller, Personality traits and concern for privacy: an empirical study in the context of location-based services, Eur. J. Inf. Syst. 17 (2008) 387–402.
[41] I. Altman, Privacy regulation: culturally universal or culturally specific? J. Soc. Issues 33 (1977) 66–84.
[42] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Q. 35 (2011) 989–1016.
[43] C.K. Hsee, E.U. Weber, Cross-national differences in risk preference and lay predictions, J. Behav. Decis. Mak. 12 (1999) 165–179.
[44] E.U. Weber, C. Hsee, Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk, Manag. Sci. 44 (1998) 1205–1217.
[45] M. Warkentin, B. Charles-Pauvers, P.Y.K. Chau, Cross-cultural IS research: perspectives from eastern and western traditions, Eur. J. Inf. Syst. 24 (2015) 229–233.
[46] H.C. Triandis, C. McCusker, H. Betancourt, S. Iwao, K. Leung, J.M. Salazar, B. Setiadi, J.B. Sinha, H. Touzard, Z. Zaleski, An etic-emic analysis of individualism and collectivism, J. Cross-Cult. Psychol. 24 (1993) 366–383.
[47] M. Srite, E. Karahanna, The role of espoused national cultural values in technology acceptance, MIS Q. 30 (2006) 679–704.
[48] Y. Uchida, V. Norasakkunkit, S. Kitayama, Cultural constructions of happiness: theory and emprical evidence, J. Happiness Stud. 5 (2004) 223–239.
[49] S. Bellman, E.J. Johnson, S.J. Kobrin, G.L. Lohse, International differences in information privacy concerns: a global survey of consumers, Inf. Soc. 20 (2004) 313–324.
[50] F. Bélanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Q. 35 (2011) 1017–1042.
[51] K.A. Stewart, A.H. Segars, An empirical examination of the concern for information privacy instrument, Inf. Syst. Res. 13 (2002) 36–49.
[52] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organ. Sci. 10 (1999) 104–115.
[53] A. Bandura, Self-efficacy, in: V.S. Ramachaudran (Ed.), Encyclopedia of Human Behavior, Academic Press, San Diego, 1994, pp. 71–81.
[54] D.R. Compeau, C.A. Higgins, Computer self-efficacy: development of a measure and initial test, MIS Q. 19 (1995) 189–211.
[55] M.-H. Hsu, C.-M. Chiu, Internet self-efficacy and electronic service acceptance, Decis. Support Syst. 38 (2004) 369–381.
[56] H. Gangadharbatla, Facebook me: collective self-esteem, need to belong, and Internet self-efficacy as predictors of the iGeneration's attitudes toward social networking sites, J. Interact. Advert. 8 (2008) 5–15.
[57] A. Burton-Jones, D.W. Straub, Reconceptualizing system usage: an approach and empirical test, Inf. Syst. Res. 17 (2006) 228–246.
[58] PRISM, Pamplin Social Media Research Report Presentation, Virginia Tech, 2011.
[59] G.M. Marakas, Y.Y. Mun, R.D. Johnson, The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research, Inf. Syst. Res. 9 (1998) 126–163.
[60] F. Bélanger, S. Collignon, K. Enget, E. Negangard, User resistance to the implementation of a mandatory security enhancement, the 2011 Dewald Roode Information Security Workshop, (2011) IFIP WG8. 11/WG11.
[61] G.A. Churchill Jr., A paradigm for developing better measures of marketing constructs, J. Mark. Res. 16 (1979) 64–73.

[62] S.B. MacKenzie, P.M. Podsakoff, N.P. Podsakoff, Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques, MIS Q. 35 (2011) 293–334.
[63] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (2003) 879–903.
[64] P.E. Spector, Method variance in organizational research truth or urban legend? Organ. Res. Methods 9 (2006) 221–232.
[65] G. Hofstede, Culture's Consequences: International Differences in Work-related Values, Sage Publications, Incorporated, 1980.
[66] R.W. Brislin, Back-translation for cross-cultural research, J. Cross-Cult. Psychol. 1 (1970) 185–216.
[67] M.E. Gordon, L.A. Slade, N. Schmitt, The science of the sophomore revisited: from conjecture to empiricism, Acad. Manag. Rev. 11 (1986) 191–207.
[68] D.R. Compeau, H.K. Marcolin, C.A. Higgins, Generalizability of information systems research using student subjects – a reflection on our practices and recommendations for future research, Inf. Syst. Res. 23 (2012) 1093–1109.
[69] R.E. Guadagno, N.L. Muscanell, D.E. Pollio, The homeless use Facebook?! Similarities of social network use between college students and homeless young adults, Comp. Hum. Behav. 29 (2013) 86–89.
[70] A.M. Kimbrough, R.E. Guadagno, N.L. Muscanell, J. Dill, Gender differences in mediated communication: women connect more than do men, Comput. Hum. Behav. 29 (2013) 896–900.
[71] D.M. Oppenheimer, T. Meyvis, N. Davidenko, Instructional manipulation checks: detecting satisficing to increase statistical power, J. Exp. Soc. Psychol. 45 (2009) 867–872.
[72] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Multivariate Data Analysis, Pearson Prentice Hall, Upper Saddle River, NJ, 2006.
[73] P.B. Lowry, J. Gaskin, Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it, IEEE Trans. Prof. Commun. 57 (2014) 123–146.
[74] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1981) 39–50.
[75] D.W. Straub, Validating instruments in MIS research, MIS Q. 13 (1989) 147–169.
[76] R.A. Peterson, A meta-analysis of Cronbach's coefficient alpha, J. Consum. Res. 21 (1994) 381–391.
[77] F.B. Davis, Educational Measurements and Their Interpretation, Wadsworth Publishing Company, Belmont, CA, 1964.
[78] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: a review and recommended two-step approach, Psychol. Bull. 103 (1988) 411–423.
[79] D. Gefen, D.W. Straub, M.-C. Boudreau, Structural equation modeling and regression: guidelines for research practice, Commun. Assoc. Inf. Syst. 1 (2000) 1–78.
[80] F. Kehr, T. Kowatsch, D. Wentzel, E. Fleisch, Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus, Inf. Syst. J. 25 (2015) 607–635.

Tabitha L. James is an Associate Professor in the Department of Business Information Technology at Virginia Tech. She received a BBA and a Ph.D. from the University of Mississippi. Her current research interests are in the areas of security and privacy in IS, social influences on technology adoption and use, combinatorial optimization, heuristics, and social networks. Her research has appeared in *IEEE Transactions on Evolutionary Computation*, *Information Technology and Management*, *Networks*, *Expert Systems with Applications*, *Decision Support Systems*, *European Journal of Operational Research*, *IEEE Intelligent Systems*, *Computers & Security, Information & Management*, and others. She has served as an AE for ICIS and a mini-track chair for AMCIS. She also serves on the board of editors of Engineering Applications of Artificial Intelligence.

Linda Wallace is an Associate Professor and the John & Angela Emery Junior Faculty Fellow at the Department of Accounting and Information Systems at Virginia Tech, where she is the Director of the Master's program in ACIS. She obtained her PhD in Computer Information Systems from Georgia State University in 1999. Her research interests include online communities, software project risk, information security, crowdfunding, and fitness technologies. Her research has been accepted for publication in *Decision Sciences*, *Communications of the ACM*, *Information & Management*, *IEEE Security & Privacy*, *Decision Support Systems*, *Journal of Systems and Software*, *Journal of Information Systems*, and others. She is an AE for *Decision Sciences* and *Information Systems Journal*.

Merrill Warkentin is a Professor of MIS and the Drew Allen Endowed Fellow at the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual, situational, and dispositional factors on individual user behaviors in the context of information security and privacy, addresses security policy compliance/violation and social media use and has appeared in *MIS Quarterly*, *Decision Sciences*, *Journal of the Association for Information Systems*,*European Journal of Information Systems*, *Decision Support Systems*, *Computers & Security*, *Information Systems Journal*, *Information & Management, Journal of Information Systems*, and others. He is the author or editor of seven books and has authored or coauthored over 250 published manuscripts, including over 70 peer-reviewed journal articles. He serves or has served as an Associate Editor of *MIS Quarterly, Information Systems Research, Decision Sciences, European Journal of Information Systems, Information & Management*, and other journals. He is a Senior Editor for *AIS Transactions on Replication Research*. He has held officer and other leadership positions at AIS, DSI, IFIP, and ACM. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He has chaired several international conferences and was the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS). Dr. Warkentin also served as a Distinguished Lecturer for the Association for Computing Machinery.

Byung Cho Kim is an Associate Professor at the Department of Logistics, Service & Operations Management at the Korea University Business School. He received his PhD in Industrial Administration from Carnegie Mellon University. His primary research interests include technology management, technology commercialization, and platform economics. Before joining Korea University, he served as an Assistant Professor of Business Information Technology at the Pamplin College of Business at Virginia Tech. His research has appeared in prestigious academic journals including *MIS Quarterly, Production and Operations Management, Decision Sciences, Marketing Letters, Decision Support Systems, International Journal of Electronic Commerce, Computational Economic,* and others.

Stéphane E. Collignon is a Teaching Assistant Professor at the Department of MIS in the College of Business and Economics at West Virginia University. He received a PhD in Business Information Technology from Virginia Tech, an MBA. from Duquesne University, and a BA in Entrepreneurship from Institut Commercial de Nancy, France. His two main current research interests are transportation procurement issues and privacy issues on social media. These topics are partially inspired from his experience in industry where Collignon worked for 7 years in logistics as an analyst and a project manager in two different French distribution companies. His research has appeared in *Information & Management, Information Technology Management*, and *Expert Systems with Applications*. He is a member of the Decision Sciences Institute and the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).