



# Impact of privacy concern in social networking web sites

Privacy in social  
networking  
web sites

Xin Tan and Li Qin

*Department of Information Systems and Decision Sciences,  
Fairleigh Dickinson University, Teaneck, New Jersey, USA, and*

Yongbeom Kim and Jeffrey Hsu

*Department of Information Systems and Decision Sciences,  
Fairleigh Dickinson University, Madison, New Jersey, USA*

211

Received 14 January 2011

Revised 11 July 2011

19 October 2011

Accepted 20 October 2011

## Abstract

**Purpose** – This study aims to understand the impact of users' privacy concerns on their acceptance of social networking web sites (SNWs).

**Design/methodology/approach** – This paper develops two research models, with privacy concern conceptualized either as an antecedent of acceptance intention, or as a moderator of the relationships in the technology acceptance model (TAM). Using a survey questionnaire, empirical data were collected from 428 undergraduate college students. Structured equation modeling was used to test the validity of the proposed research models.

**Findings** – The privacy concerns of the research respondents were found to be statistically significant. However, they did not directly affect users' acceptance of social networking web sites. Instead, privacy concerns did moderate the effects of perceived usefulness, and perceived ease of use, on users' intention to continue to use SNWs.

**Research limitations/implications** – The study identifies the theoretical foundations of privacy and privacy concerns in the context of SNWs. This empirical study, based on an established theoretical foundation, will help the research community to gain a deeper understanding of the impacts of privacy concern in the context of social networking.

**Practical implications** – The findings of this study can provide SNW operators with useful strategies and tactics to enhance users' acceptance depending on their level of privacy concern.

**Originality/value** – With the worldwide rapid growth of SNWs, there have been ongoing concerns about how users' private information is viewed or used by others. This study provides much needed empirical evidence about the impact of privacy concerns on users' acceptance of SNWs.

**Keywords** Social networking sites, Privacy, Technology acceptance, User studies, Attitudes

**Paper type** Research paper

## 1. Introduction

In the Internet Age, we have witnessed the rapid growth of social network web sites (SNWs) such as Facebook, MySpace, LinkedIn, and Orkut, in recent years (Zhou, 2011). Users across the world have signed up for accounts on SNWs in order to discover other people with similar interests or experience, to share personal information with both friends and strangers, or to establish business contacts. With millions of registered users visiting SNWs on a daily basis, the potential business value of SNWs has become too great to be ignored by either marketers or application developers. Today, both major and emerging consumer brands, such as Coca Cola, BMW, Gap, Netflix, and ZipCar, have established their presence on various SNWs. At the same time, application developers have created many popular gadgets (mini apps running within



SNWs pages) like FarmVille, Mafia War, and iLike, to keep users engaged on SNWs for hours every day.

In addition to displaying contextual advertisements to visitors, SNW operators have partnered with marketers to provide additional features by utilizing social connections for viral marketing. Facebook Beacon, for example, was such an experiment. On November 6, 2007, Facebook launched a social advertising program called Beacon. Through this program, Facebook users would share with their friends on Facebook information about their online purchases on 44 partner Web sites, such as eBay, Fandango, and Overstock (Facebook, 2007). However, only days after the launch, Facebook encountered strong backlash from users over concerns about privacy invasion. As a result, Facebook was forced to change from an “opt-out” option to an “opt-in” option (Story and Stone, 2007). This highly publicized event highlights the sensitive nature of privacy concern in SNWs.

In the relatively short history of Facebook, the Beacon program is not the only incident that has triggered users’ protest over privacy issues. In fact, almost every time Facebook rolled out a major new feature, it made member information more accessible, rather than less (Jaroslovsky, 2010). If there was any outcry from users, the strategy usually was to scale back or reverse the action later. To explain Facebook’s ever changing privacy policy and privacy control during a speech, Facebook founder Mark Zuckerberg said, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time” (B. Johnson, 2010). Should other SNWs operators and marketers follow Facebook’s way of handling users’ privacy? This is an important question to answer in order to effectively manage this relatively new form of media and the business opportunities within it.

For SNW users, theoretically, there are many privacy issues that deserve serious consideration. First, the information posted in public or semi-public user profiles can lead to such risks as identity theft, sexual exploitation, online stalking, and cyber harassment (Gross and Acquisti, 2005). Second, the posting of personal and private information in SNW opens up a user to public scrutiny, possibly creating permanent records that can affect the user negatively in the future (Rosenblum, 2007). Third, the viral feature of news feed makes personal information far more accessible and visible, posing a disruption of privacy (Boyd, 2008). Despite some anecdotal evidence (Barnes, 2006; Boyd, 2008), however, the level of privacy concern and its impact on the usage pattern in SNWs are largely unknown.

The present study is an investigation into privacy concern in the context of SNW. A survey of actual SNW users was used to collect data for answering two related research questions:

*RQ1.* Are there significant privacy concerns among SNW users?

*RQ2.* What is the impact of privacy concern on users’ acceptance of SNW?

The findings from this research provide empirical evidence to SNW operators, marketers, application developers, and other parties in managing their businesses in the context of SNW.

The remainder of this paper is organized as follows. The first section introduces related literature on SNW, privacy, and prior studies on privacy concern in social networking settings. The second section reports on the development of our research

---

models and associated hypotheses. The third section presents the details of the survey study, and discusses the findings of the data analysis. The conclusion section addresses the implications of this study for research and practice, points out the limitations, and highlights the directions for future research.

## 2. Related literature

In this section, we first introduce the basic concepts related to social networking web sites. Then we review the existing literature on the concepts of privacy and privacy concern. In the end, we survey the existing studies on privacy concern in the context of SNW.

### 2.1 Social networking web sites

A Social Networking Web site (SNW) provides users with web-based services that allow individuals to:

- construct a public or semi-public profile within a bounded system;
- articulate a list of other users with who they share a connection; and
- view and traverse their list of connections and those made by others within the system (Boyd and Ellison, 2007).

Based on these features, the origin of SNW may be traced back to as early as 1997 when a web site called SixDegrees.com was founded (Boyd and Ellison, 2007).

Today, Facebook and MySpace are the two most well-known social networking web sites in the United States, each boasting hundreds-of-millions of users. Even though exact numbers are too dynamic to track, some statistics of unique visitors and page views have shown a growing user base of SNWs. In January 2010, Facebook is ranked as the second most visited web site in the whole world, only behind Google (Alexa, 2010). With registered members surpassing 500 million mark in 2010, Facebook aims at reaching 1 billion users soon (Sweeney, 2010).

Businesses increasingly see SNWs as an important medium for public relations, communications and marketing. The business value of SNW for various companies is derived primarily from two sources: first, the public or semi-public profiles of SNW users may serve as consumer demographic information, on which consumer behavior analysis can be done and targeted marketing campaigns can be based; second, the social connections embedded in SNWs may serve as the foundation for effective viral marketing. One viral feature found in most SNWs is the Feed (or news feed), pioneered by Facebook (Boyd, 2008). Feeds provide a timely update on the activities of people with who a SNW user has a connection. For example, a SNW user will receive notifications when someone in his or her network (friends list) makes a new friend, joins a club, becomes a fan, posts a comment on other user's wall, shares a new picture, or installs a widget. Recent acquisitions have showcased the high valuation of SNWs. For instance, in 2005 News Corporation acquired Intermix Media, owner of the then two-year-old Myspace.com, for \$580 million (Siklos, 2005). More recently, Bebo.com was bought by AOL in 2008 for \$850 million (McCarthy, 2008). With regard to the current top SNW, Facebook, it has been valued up to 15 billion dollars based on an equity investment by Microsoft in 2007 (Sloane, 2007).

While more and more users have joined various SNWs, many high profile incidents (as profiled earlier) have hinted that SNW users are concerned about their privacy. On the other hand, we also witnessed the dynamic and changing nature of privacy concern

over time. When Facebook initially launched the News Feed feature in 2006, hundreds of thousands of Facebook users participated in a Facebook petition to protest against this public broadcast of their online activities (Schmidt, 2006). Nowadays, Feed is a popular feature found in most SNWs (Gallaughar, 2010). To study such privacy related issues in SNWs, a clear understanding about the concepts of privacy and privacy concern are needed.

### *2.2 Concept of privacy*

The concept of privacy is not new, with definitions and studies on the issue spanning the fields of philosophy, anthropology, psychology, law, and management. As early as in the nineteenth century, Warren and Brandeis (1890) articulated that privacy referred to “the right to be left alone.” However, even today privacy is a concept that lacks a consistent definition. There are some scholars who advocate privacy as a unitary concept (Introna and Pouloudi, 1999; Johnson, 1989; Westin, 1967). For example, Johnson (Johnson, 1989) defined the function of privacy as “to isolate certain limited and culturally defined aspects of the individual’s life as being morally and legally protected from the evaluative judgment of others.” Karyda *et al.* (2009) discussed privacy in ubiquitous environments as an individual’s privacy including bodily privacy, territorial privacy, privacy of communications, information privacy, and location privacy, and how privacy can be preserved by enforcing “fair information practices”, which define how personal information should be collected and treated in a “fair way”.

The study of privacy has been extended to critical applications in business, including consumer behavior, marketing, e-commerce, and Internet/ information technology use (Lanier and Saini, 2008; Phelps *et al.*, 2000). This is of importance because businesses need to collect personal and behavioral information on individual consumers to better understand them. Much attention has been paid to balancing marketers’ information needs and consumers’ right to privacy. In particular, much of the research on consumer privacy has been related to consumer’s willingness to share private information (Phelps *et al.*, 2000), information gathering and use contexts (Nowak and Phelps, 1995), as well as the many privacy-related tradeoffs that occur in marketing transactions (Milne and Gordon, 1993).

### *2.3 Concept of privacy concern*

Privacy concern is the main focus of the present study. Privacy concern is a person’s awareness and assessment of risks related to privacy violations. Prosser (Prosser, 1960) discussed four components (legal torts) which comprise privacy, including false light (i.e. false public portrayals), disclosure (i.e. publicly disclosing embarrassing private facts), appropriation (i.e. use of a person’s image or identity without permission), and intrusion (i.e. physically invading a person’s solitude or seclusion) (Prosser, 1960). This four-dimensional perspective on privacy has been embraced by most courts and has guided much federal and state legislation (McWhirter and Bible, 1992).

In the existing literature, privacy concern can be defined from a personal and consumer perspective as a “sense of anxiety regarding one’s personal privacy” (Lanier and Saini, 2008). Another definition describes it as being “a concern for controlling the acquisition and subsequent use of information [...] about him or her” (Westin, 1967). With privacy concern, the focus is on the concerns that individuals have about who have access to their private information and how such information will be used.

---

Certainly, with the increased use of the Internet, social networking, and other forms of information sharing, concerns over privacy continue to be a source of much research and discussion.

Some of the factors that affect privacy concern include information usage, awareness, information sensitivity, familiarity with the firm/organization, and compensation (Nowak and Phelps, 1992). According to Lanier and Saini (Lanier and Saini, 2008), there are three major categories of privacy concern that affect consumers:

- (1) Notification, as many consumers want to be informed about the collection and use of their personal information by firms.
- (2) Control, as consumers want to feel that they have some control over the collection of their personal information and the sharing of this information among firms.
- (3) Security, as most consumers want some assurance that the personal information they provide to firms, especially online, and the storage of this information is secure.

In general, it was found that individuals are more likely to be concerned about their privacy when information is used without one's permission or knowledge, or when the intended use of the information is not clearly stated (Phelps *et al.*, 2000). Another important privacy concern is related to secondary use of private information. In this case, firms may sell or provide their customers' information to others, without notifying the customers who is receiving this information and how it may ultimately be used (Nowak and Phelps, 1995; Phelps *et al.*, 2000).

In the field of information systems (IS), privacy and privacy concern also raised interest among researchers. A number of studies (George, 2002; Pavlou *et al.*, 2007; Rose *et al.*, 1999) have been done to investigate the impact of information privacy concern on consumers' online purchase intention and behaviors. With the growing popularity of SNWs, some researchers have started giving attention to the issue of privacy concern in the context of online social networking. In the following, we review the prior work on privacy concern in the context of SNW.

#### *2.4 Prior work on privacy concern in SNW*

Compared to other mature Web-based services, such as e-commerce and e-services, SNW is a relatively new phenomenon, hitting the mainstream after 2003 (Boyd and Ellison, 2007). As a new social media, various SNWs have launched new features to attract more users, many of which are followed by questions about privacy concerns. Throughout the early evolution of SNW, researchers have paid particular attention to privacy issues in SNWs (Fogel and Nehmad, 2009).

Some researchers have tried to describe the sources of privacy concern in SNWs. Boyd (2008) asserted that the sense of exposure and invasion is the primary source of privacy concern in the events associated with Facebook's News Feeds launch. Chew *et al.* (2008) identified three privacy-sensitive areas in SNWs:

- (1) A lack of control over activity streams, i.e. a user may not be aware of all the events that are fed into his/her activity stream and the entire audience who can see their activity stream.

- (2) Unwelcome linkages, i.e. the links available in SNWs reveal some information about an individual that he or she had not intended to reveal.
- (3) Deanonymization through the merging of social graphs, i.e. de-anonymizing users by comparing personally identifiable information across social networking sites, even if the information is partially disguised in each networking site.

Fogel and Nehmad (2009) studied the influence of gender on privacy and found that men generally have less privacy concern than their female counterparts, and thus tend to disclose more personal information on SNWs than female users.

Some other researchers have attempted to assess the effect of information revelation and privacy options of SNWs on users' privacy control. For instance, Gross and Acquisti (2005) conducted a survey among more than 4,000 college students (Facebook users) to study patterns of information revelation in online social networks and their privacy implications. The findings indicate that, despite the potential attacks on various aspects of their privacy, only a small percentage of students changed their privacy preferences. There were some explanations as to the lack of privacy control by SNW users. Preibusch *et al.* (2007) argued that the privacy options offered by SNWs do not provide users with the flexibility they need to handle conflicts with friends who have different conceptions of privacy. Acquisti and Gross (2006) claimed that there is often a disconnect between users' desire to protect privacy and their privacy control behaviors, a phenomenon known as the "privacy paradox" (Barnes, 2006).

Despite the growing research interest in privacy and privacy concern in SNW context, there is a paucity of information and empirical evidence on how privacy concern affects acceptance of SNWs (Shin, 2010). A limited number of studies have been done to evaluate the impact of privacy concern on usage behavior in SNWs. For example, Dwyer *et al.* (2007) conducted a survey to compare perceptions of trust and privacy concern, along with users' willingness to share information and develop new relationships, among users of two popular SNWs, MySpace and Facebook. They found that members of both sites reported similar levels of privacy concern, but with different levels of trust and experience on the sites. The study demonstrates that online relationships can develop in sites where perceived trust and privacy safeguards are weak. In a recent study, Shin (2010) examined the impact of security and privacy perceptions on users' acceptance of SNW. The study found that the perceived security and privacy protections positively influence users' trust, attitude, and usage intention in SNW. In another study, Cha (2010) found that privacy concern is negatively correlated with the frequency of users using SNW, but not the time spent on SNW. While these studies provided insights to various aspect of privacy concern's influence in SNW context, their findings could not directly answer our research questions, i.e.

*RQ1.* Are there significant privacy concerns among SNW users?

*RQ2.* What is the impact of privacy concern on users' acceptance of SNW?

In particular, Shin's study (2010) examined the perceived privacy protection, which is a related, but a different construct as compared to privacy concern. In Cha's research (2010), the relative impact of privacy concern on SNW usage pattern is not measured through sophisticated statistical analysis.

---

Our study is an attempt to fill the void in the existing literature. A comprehensive understanding of the impact of privacy concern on users' acceptance of SNW may provide valuable insights for SNW operators and marketers to offer more effective services and applications to SNW users.

### 3. Development of research models

As mentioned in the introduction section, the research objective of the present study is to answer two related questions. First, are there significant privacy concerns among SNW users? Second, what is the impact of privacy concern on SNW users' usage behavior? While the first question can be answered by simply measuring and comparing the mean and standard deviation of privacy concerns among SNW users, the second question needs to be operationalized as research hypotheses derived from established theories.

SNWs represent an information-technology-driven platform that allows users to befriend and communicate with others who share similar interests or experiences, to reinforce existing social ties, or to establish business contacts. The concept of users' acceptance of SNW is a special case of technology acceptance. Therefore, the theoretical foundation of the research model should be the established theories in technology acceptance. In the IS field, the Technology Acceptance Model (TAM) by Davis (1989) has been extensively used to study the determinants of the adoption intention and usage behavior in different information technologies and systems, such as hardware (Igarria *et al.*, 1995), software (Rimenschneider and Hardgrave, 2001), e-service (Hu *et al.*, 1999), e-commerce (Gefen and Straub, 2000), and enterprise systems (Amoako-Gyampah and Salam, 2004). Several meta-analysis studies (e.g. King and He, 2006; Lee *et al.*, 2003) have found evidences that support "the parsimony of TAM, the robustness of its scales, and the strong generalizability of the model" (Venkatesh *et al.*, 2007). With the emergence of SNWs, researchers began to study their usage with TAM as the theoretical foundation. For instance, Willis (2008) applied TAM in a study of the acceptance of online social networking systems. Shin and Kim (2008) adapted TAM and Flow Theory to develop a framework for understanding attitudinal and behavioral patterns in a social networking site in South Korea. The findings of these studies support the general applicability of TAM in the context of SNWs. However, privacy concern in SNWs as a factor has not been studied in the framework of TAM.

In the following, we briefly report on the main and critical aspects of TAM, and then present our research models and associated hypotheses as an extension of the original TAM.

#### 3.1 Technology Acceptance Model (TAM)

As an adaptation of the Theory of Reasoned Action (TRA) (Ajzen and Fishbein, 1980), the TAM (Davis, 1989) has emerged as a powerful and parsimonious way to represent the antecedents of system usage through two beliefs: perceived ease of use (PEU) and perceived usefulness (PU) of an information system. The TAM theorizes that an individual's behavioral intention to use a system is determined by perceived usefulness, defined as "the extent to which a person believes that using the system will enhance his or her job performance", and perceived ease of use, defined as "the extent to which a person believes that using the system will be free of effort" (Davis, 1989).

Many empirical tests of TAM indicate that perceived usefulness is a strong determinant of behavioral intention (BI), while perceived ease of use is a relatively weak determinant of intention (Venkatesh and Davis, 2000). According to TAM, perceived usefulness is also influenced by perceived ease of use because, other things being equal, the easier the system is to use, the more useful it will be (Davis *et al.*, 1989). The original TAM depicts that attitude is a mediating variable between the two determinants and behavioral intention. Studies demonstrated that without the mediating attitude construct, the explanatory power of the model is equally good and the model is more parsimonious (Davis *et al.*, 1989). As a result, it has become a norm to exclude the attitude construct from TAM. In addition, behavioral intention is frequently used as the primary surrogate of users' acceptance. Thus, a parsimonious formulation of TAM has only three constructs: PU, PEU and BI.

Specifically tailored for modeling users' acceptance of information systems, the TAM has very good explanatory power, explaining about 40 percent of the variance in usage intentions and behavior (Venkatesh and Davis, 2000). Therefore, the TAM has been adopted to study the acceptance of various information systems. In the present study, we derive our research model with TAM as the theoretical foundation.

### 3.2 Research models and hypotheses

For the purposes of this research, we define privacy concern (PC) as "the degree to which a user believes using a system would result in a loss of control over their personal information." To understand the impact of privacy concern on users' acceptance of SNW, we need to conceptualize PC in a way that it can be integrated in the general framework of the TAM.

*3.2.1 Privacy concern as a direct determinant of BI.* While it is not directly included in TAM, PC may exert its influence on acceptance as a direct determinant of behavioral intention. The rationale is that PC can be regarded as a factor that negatively affects attitude toward using SNWs. In other words, PC is one of the behavioral beliefs (like PU and PEU) that jointly affect attitude. The limited studies on privacy concern in SNW have suggested that users' privacy concern creates negative attitudes toward SNW (Boyd, 2008; Schmidt, 2006). Privacy concern can also be conceptualized as a type of perceived risk. For instance, Featherman and Pavlou (2002) defined "privacy risk" as "potential loss of control over personal information, such as when information about you is used without your knowledge or permission." This conceptualization is similar to our definition of privacy concern. The findings of their study indicate that, as perceived risk decreases, a user's willingness to use the system increases. In a related work, Featherman and Fuller (2003) found that perceived risk evaluations were a direct causal deterrent to adoption. Therefore, we propose the following hypothesis:

*H1.* Privacy concern (PC) has a direct negative influence on a user's intention to use SNW.

*3.2.2 Privacy concern as a moderator in TAM.* Another way that privacy concern may exert its effect on users' acceptance of SNWs is by moderating the relationships between PEU/PU and BI in the TAM. In a meta-analysis study, King and He (2006) identified considerable variability in relationships among TAM constructs, suggesting that moderator variables may exist. In other words, certain factors may affect the relationship between PU and BI, between PEU and BI, or between PEU and PU. King and He (2006)



further proposed both the type of user and the type of usage as moderators in TAM. Through the meta-analysis, they found evidence of the proposed moderating effects. In a separate meta-analysis study, Schepers and Wetzels (2007) compared TAM studies by examining moderating effects of one individual-related factor (type of respondent), one technology-related factor (type of technology), and one contingent factor (culture). Their study found significant moderating effects for all three factors on the relationships depicted in the TAM. In a conceptual paper, Sun and Zhang (2006) reviewed existing TAM related studies and recommended the addition of moderating factors to enhance explanatory power and to overcome the inconsistencies in previous studies. They proposed ten moderating factors, which are categorized into three groups: organizational factors, technological factors and individual factors. Some of these factors, such as gender (Gefen and Straub, 1997), age (Venkatesh *et al.*, 2003), culture (Straub *et al.*, 1997), experience level (Venkatesh, 2000), and perceived risk (Im *et al.*, 2008), have been examined in prior studies. However, privacy concern, despite its growing importance in the SNW context, has not been previously studied as a moderator in the TAM.

As discussed previously, privacy concern is a concept related to the risk of privacy invasion. It can be regarded as an individual factor that may have significant moderating effects on user's acceptance of SNWs. Im *et al.*'s study on perceived risk can therefore serve as a reference for our research. The study (Im *et al.*, 2008) found that, for users perceiving a higher risk in using the technology, PU has smaller effects on BI than those perceiving a lower risk. On the other hand, PEU has a larger effect on BI for the high perceived risk group than the low perceived risk group. The second finding, however, is inconsistent with that of Featherman and Fuller (2003), which found the impact of PEU on BI disappeared as perceived risk increased. The inconsistency in moderation directions may be caused by the difference in the conceptualization of perceived risk or in the research context. Since in this study we are interested in assessing whether there is a moderating effect of PC in TAM relationships, we propose the following hypotheses without specifying moderation directions:

*H2a.* The effect of PU on BI will vary with different levels of privacy concern (PC).

*H2b.* The effect of PEU on BI will vary with different levels of privacy concern (PC).

Figures 1 and 2 depict the two research models created with TAM as the foundation.

#### 4. Research method

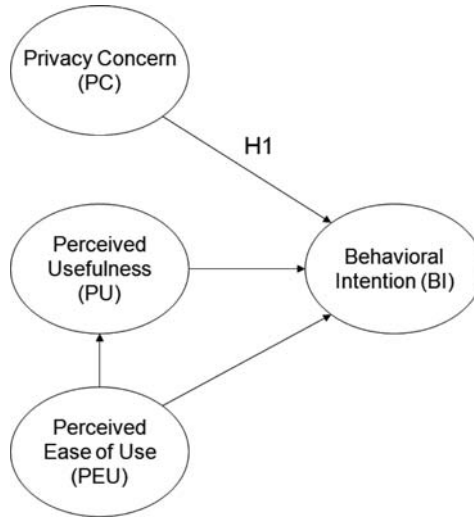
A survey study was employed to collect data in order to evaluate the level of privacy concerns among SNW users, and to test the research hypotheses outlined previously. The survey method is a typical approach for testing models in IS research (Galliers, 1992). Pinsonneault and Kraemer (1993) suggested that survey research is especially appropriate for explanatory models where the phenomena must be studied in natural settings and when the phenomena of interest occur in the recent past. This is the case in our study. We want to investigate the impact of privacy concern on users' acceptance of SNW in natural settings.

##### 4.1 Measurement development

A survey questionnaire was developed to measure each of the constructs contained in our research model. Measurement items for the constructs in the research model were

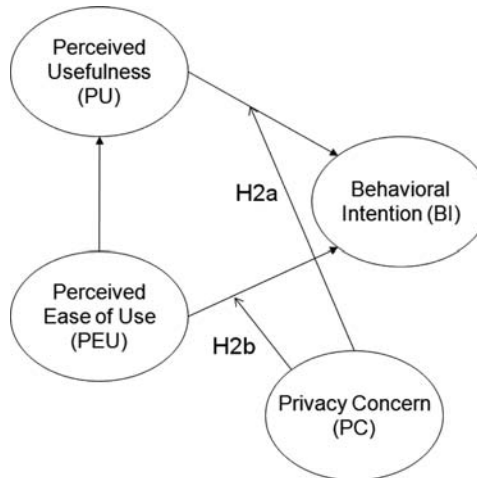
**Figure 1.**  
Model 1 (PC  
conceptualized as an  
antecedent of BI)

---



**Figure 2.**  
Model 2 (PC  
conceptualized as  
moderating the effect of  
PU and PEU on BI)

---



adapted from prior studies. For instance, items to measure PU, PEU, and BI were developed based on the work of Davis and his colleagues (Davis, 1989; Venkatesh and Davis, 2000). Items to measure PC were based on the work in Featherman and Pavlou (2002) and Acquisti and Gross (2006). Each item was measured on a seven-point Likert scale where 1 means “strongly agree” and 7 means “strongly disagree.” The list of the items is displayed in the Appendix.

In addition to the measurement items for the constructs in the research models, we also included questions about SNW users’ demographics and their usage pattern in the survey questionnaire.

4.2 Data collection

A pilot study was used to ensure that the survey items are relevant to the users of social networking web sites. Based on the feedback from the pilot study, refinements were made to the questionnaire items. The finalized survey questionnaire was then distributed to undergraduate students enrolled in introductory MIS courses at a college in the Northeastern USA. These MIS courses are required for all business majors. In total, 439 survey questionnaires were returned from the survey participants. After screening out incomplete responses, the survey yielded 428 usable responses. Table I provides the summary of respondents' demographic information as well as their SNW usage patterns.

Measure/items	Frequency	Percentage
<i>Age</i>		
Under 18	11	2.6
18-23	323	75.5
24-29	69	16.1
30-39	17	4
40 +	8	1.9
<i>Gender</i>		
Female	189	45.2
Male	229	54.8
<i>Years of using SNW</i>		
< 1	65	15.2
1-2	67	15.7
3-4	164	38.3
5 +	132	30.8
<i>Frequency of logging onto social network<sup>a</sup></i>		
Several times a day	271	63.3
Once a day	101	23.6
Once for several days	23	5.4
Once a week	16	3.7
Biweekly	7	1.6
Once a month	9	2.1
Others	1	0.2
<i>Time spent for each session<sup>a</sup></i>		
< 30 minutes	285	66.6
30 minutes-1 hour	108	25.2
1-2 hours	23	5.4
> 2 hours	12	2.8
<i>Privacy setting: private info accessible to<sup>a</sup></i>		
Friends only	333	77.8
Friends and their friends	42	9.8
Public	37	8.6
I don't know	16	3.7

Note: <sup>a</sup>Based on the online social network visited most frequently

**Table I.**  
Profile of respondents

4.3 Data analysis

SPSS was used to aggregate user profiles, generate descriptive statistics, and test the reliability and validity of the measurement. MPlus (Version 2.5) was used to conduct the Structural Equation Modeling (SEM) analysis for model testing. SEM has been widely used in behavioral science research for the causal modeling of complex and multivariate data sets in which the research gathers multiple measures of proposed constructs (Hair *et al.*, 1998). SEM is also widely used in MIS research to validate instruments and test linkages between constructs (Chin, 1998; Gefen *et al.*, 2000).

4.3.1 *Descriptive statistics.* The descriptive statistics, including the minimum value, the maximum value, the mean value, and the standard deviation, for each survey item are listed in Table II. The description of each survey item can be found in the Appendix.

4.3.2 *Instrument validity and reliability.* Using SPSS' component-based confirmatory factor analysis (CFA), analyses were done to examine the validity and reliability of the survey items. As shown in Table III, the factor loading of each item on the corresponding construct is above 0.600, indicating satisfactory convergent validity of the measurement items (Hair *et al.*, 1998). The factor loadings are low on the unrelated

**Table II.**  
Descriptive statistics of  
survey items

	Minimum	Maximum	Mean	Std deviation
PU1	1.0	7.0	1.748	1.1212
PU2	1.0	7.0	2.292	1.1416
PU3	1.0	7.0	2.140	1.0436
PC1	1.0	7.0	3.182	1.5754
PC2	1.0	7.0	3.481	1.5925
PC3	1.0	7.0	3.492	1.6034
PEU1	1.0	7.0	2.201	1.0182
PEU2	1.0	7.0	2.117	1.1576
PEU3	1.0	7.0	1.886	1.0462
IN1	1.0	7.0	2.889	1.4421
IN2	1.0	7.0	2.026	1.0136
IN3	1.0	7.0	2.209	1.0575

**Table III.**  
Confirmatory factor  
analysis and reliability

	PC	IN	PEU	PU
Cronbach's alpha	0.829	0.716	0.751	0.738
PU1	0.046	0.094	0.136	0.866
PU2	-0.070	0.356	0.335	0.629
PU3	0.022	0.426	0.214	0.636
PC1	0.828	-0.009	0.065	0.027
PC2	0.880	-0.010	0.021	-0.033
PC3	0.879	-0.055	-0.043	0.026
PEU1	0.021	0.420	0.613	0.126
PEU2	0.025	0.095	0.864	0.116
PEU3	0.018	0.134	0.792	0.311
IN1	-0.080	0.822	0.041	0.104
IN2	0.000	0.677	0.425	0.233
IN3	0.003	0.707	0.186	0.287

constructs, providing support for discriminant validity. With regard to the reliability of survey items, the Cronbach's alpha of the items for each construct is above .700, a recommended cut-off value for satisfactory reliability (Nunnally, 1978). Therefore, the instrument validity and reliability are found to be satisfactory, and ready for further analysis, i.e. model testing and path analysis.

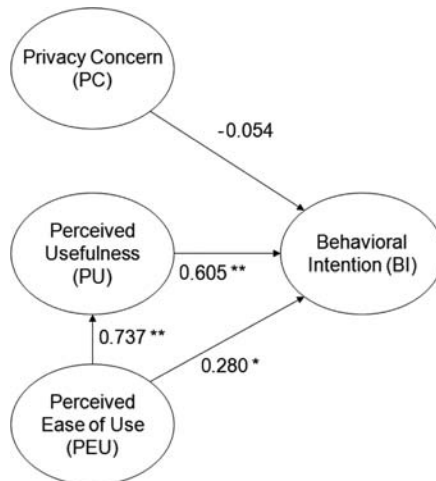
4.3.3 *The level of privacy concerns.* One of the research questions is concerned with the level of privacy concern among SNW users. As seen in descriptive statistics in Table I, the average value of each privacy concern item is below 4 ("neutral" in the Likert scale). In other words, the survey respondents on average do have privacy concern when using SNWs. To test the level of significance, a one-sample *t*-test was performed in SPSS. The result is shown in the following table (see Table IV). With *p*-value being less than 0.000 for each of the *t*-tests, it is supported that the privacy concern is statistically significant among SNW users.

4.3.4 *Test of research model 1.* The full structural model as illustrated in Figure 1 was tested using MPlus. The resulting standardized path coefficients are shown in Figure 3. The model fit indices are displayed in Table V. The results indicate that Research Model 1 has a relatively good fit with the data. However, the direct effect of PC on BI is insignificant, even though the path coefficient is negative, as expected.

4.3.5 *Test of research model 2.* Research model 2 conceptualizes PC as a moderator in the TAM, as shown in Figure 2. To test the moderating effects using SEM, it is suggested to divide the data set into two groups based on high and low values of the

	<i>t</i>	Test value = 4 (privacy concern is neutral)		Mean difference
		df	Sig. (two-tailed)	
PC1	-10.739	427	0.000	-0.8178
PC2	-6.738	427	0.000	-0.5187
PC3	-6.557	427	0.000	-0.5082

**Table IV.**  
One-sample *t*-test of privacy concern



Note: \*:  $p < 0.05$ ; \*\*:  $p < 0.01$

**Figure 3.**  
Standardized path coefficients of model 1

candidate moderating variable. Then, a comparison of modeling fit can be done across the groups to determine the significance of the moderating effect (Cortina *et al.*, 2001; Dabholkar and Bagozzi, 2002). For example, to test the moderating effect of gender, the dataset can be divided into two sub-sets, one for male and the other for female. Then, the full structural model will be tested twice using multi-group testing in SEM. First, model parameters will be estimated separately for all groups (male and female). Second, an additional model testing will be done with regression coefficients constrained to be equal across groups. A chi-square difference test should be done afterwards to examine the relative fit of the two models. If the second model (invariant path coefficients) fits significantly worse than the first, it can be concluded that the moderating effect is statistically significant.

In our data analysis, we followed similar procedures in existing literature (Dabholkar and Bagozzi, 2002; Im *et al.*, 2008). First, we divided the dataset into two sub-sets by the median of the average of PC items (3.33). After this step, there are two groups identified in the dataset, one labeled as low privacy concern (the average of PC items is above 3.33) and the other labeled as high privacy concern (the average of PC items is below 3.33). Second, we used multi-group testing in SEM to run two analyses, one for free estimate across groups (Model 2X), the other for constraining equal path coefficients across groups (Model 2Y). The model fit indices are displayed in Table VI. The comparison of path coefficients is shown in Figures 4 and 5.

To assess the moderating effect of privacy concern, we need to do a chi-square difference test between Model 2 X and Model 2 Y. According to the statistics in Table VI, chi-square change is 15.3 (= 141.2-125.9), and the change in degree of freedom is 3 (= 57-54). The *p*-value of this chi-square difference is .0016, indicating that the model fit with coefficients constrained as the same across groups is significantly worse than the model fit with no constraints. In other words, the moderating effect of privacy concern on TAM relationships is statistically significant.

4.4 Discussion of the results

The survey results show that the privacy concern of SNW users is significantly different from neutral. This finding is consistent with the overall observations of

**Table V.**  
Goodness-of-fit indices of  
research model 1  
(*n* = 428)

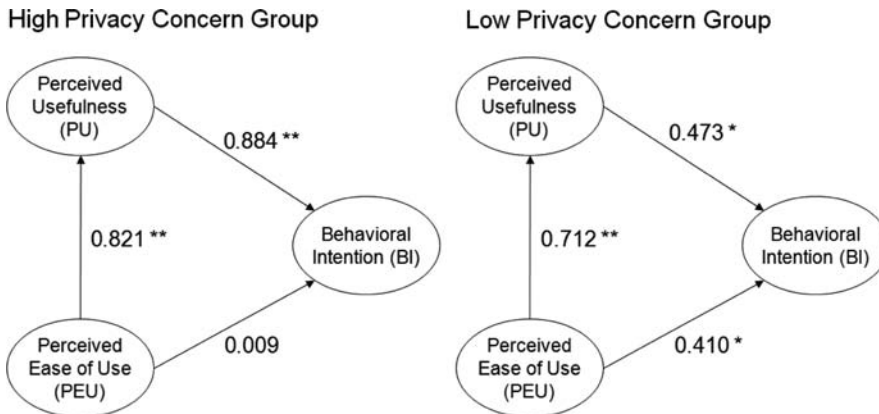
df	$\chi^2$				
49	111.61 *	2.28	0.966	0.055	0.039

**Notes:** CFI = Comparative fit index; RMSEA = Root mean square error of approximation; SRMR = Standardized root mean square residual. \**p* < 0.001

**Table VI.**  
Goodness-of-fit indices of  
model 2X and 2Y  
(*n* = 428)

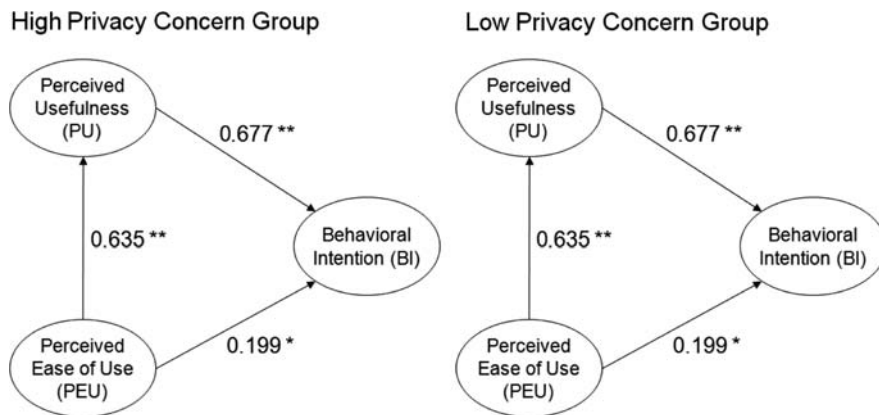
	Df	$\chi^2$	$\chi^2/df$	CFI	RMSEA	SRMR
Model 2X (free estimate across groups)	54	125.90	2.33	0.947	0.079	0.074
Model 2Y (same coefficients across groups)	57	141.20	2.48	0.938	0.083	0.091

**Notes:** CFI = Comparative fit index; RMSEA = Root mean square error of approximation; SRMR = Standardized root mean square residual



Notes: Free estimate across groups; \*,  $p < 0.05$ , \*\*,  $p < 0.01$

Figure 4. Standardized path coefficients of model 2X (free estimate across groups)



Notes: Path coefficients are constrained as same across groups; \*,  $p < 0.05$ ; \*\*,  $p < 0.01$

Figure 5. Standardized path coefficients of model 2Y (path coefficients are constrained as same across groups)

studies on privacy related issues in the new media, particularly involving Facebook (Jaroslovsky, 2010; Schmidt, 2006; Story and Stone, 2007).

In addition to the findings of significant privacy concern, this study investigated the impact of privacy concern on users' acceptance of SNWs. As shown in Figure 3, while the original relationships in the TAM are supported by our data, the direct link between PC and BI is not significant. Therefore, we did not find evidence in this study to support *H1*. In other words, our study shows that privacy concern has no direct impact on user's intention to use SNW. This finding is consistent with recent studies that focused primarily on the direct impact of privacy concern on intention to use SNWs and found insignificant effects (von Stetten *et al.*, 2011; McKnight *et al.*, 2011). There are a number of possible explanations for this finding. First, the respondents in this study have a relatively high control over their privacy options in SNWs. As shown in Table I, 77.8 percent of the users in our sample make their private information

accessible to their friends only. Even though there is privacy concern in general, their attitude toward SNW is not significantly negative (Gross and Acquisti, 2005). Second, the majority of respondents in this study are typical undergraduate college students who may share the characteristic that privacy concern has no direct impact on their use of SNW, a phenomenon known as the “privacy paradox” (Barnes, 2006).

With regard to *H2*, we did find the moderating effect of privacy concern in this study. As reported in the previous section, Model 2X in Figure 4 clearly shows the difference in path coefficients between the high privacy concern group and the low privacy concern group. For the relationship between PU and BI, the high privacy concern group has a higher path coefficient than the low privacy concern group (0.884 vs 0.473). In other words, for users with higher privacy concern, the perceived usefulness will have a stronger influence on behavior intention. Thus, *H2a* is supported. Our data analysis indicates that with higher privacy concern, the effect of PU on BI is strengthened. This finding is different from that of Im *et al.* (2008), in which the moderating direction is opposite. There are several possible reasons for this inconsistency. First, the concept of privacy concern in this study and that of perceived risk in Im *et al.* (2008) are two related but different constructs. According to Im *et al.* (2008), perceived risk was measured using five categories: financial (worth the cost), performance (effectiveness), social (changes in work), psychological (frustration), and physical (comparison to other products). On the other hand, privacy concern in this study refers to a person’s awareness and assessment of risks related to privacy violations. It is narrower in scope than the comprehensive concept of perceived risk. Thus, it is possible that the two constructs may have different moderating effects on TAM relationships. Second, the research settings between the two studies are different. Im *et al.* (2008) studied the effects of perceived risk in using different communication technologies for a group decision-making task. The present study investigated the effects of privacy concern in using SNWs for individual purposes. Hence, the nature of technology usage may change the moderating effects.

For the relationship between PEU and BI, the high privacy concern group has a lower path coefficient than the low privacy concern group (0.009 vs 0.410). This difference shows that, for users with higher privacy concern, the perceived ease of use will have a weaker (in fact, statistically insignificant) influence on behavior intention. Thus, *H2b* is supported. Our study finds that with higher privacy concern, the effect of PEU on BI is attenuated. This finding is consistent with that of Featherman and Fuller (2003), but different from the results in Im *et al.* (2008). The inconsistency can be explained similarly as mentioned previously.

In summary, this study found that with higher privacy concern, the effect of PU on BI is strengthened, while the effect of PEU on BI is attenuated. One possible explanation is that when SNW users have higher privacy concern over using SNWs, it means they may perceive a higher risk of privacy violation. Thus, the SNW will be evaluated with greater caution. In this situation, the decision to use the SNW is heavily influenced by the perceived usefulness (utility) in order to justify the potential loss of privacy. On the other hand, those who have high privacy concern also feel the social networking site easier to use than those who have low privacy concern. As such, PEU has a weaker impact on intention to use for those who have high PC and perceive the social networking site easier to use. In other words, if an user already feel it easy to use, then ease of use will have a weaker effect on your future use.



---

## 5. Conclusion

In summary, we investigated the effect of users' privacy concern on their acceptance of SNW. Using TAM as the theoretical foundation, we developed research models to hypothesize two types of effects:

- (1) Privacy concern having direct effect on behavioral intention (BI).
- (2) Privacy concern moderating the effects of perceived usefulness (PU) and perceived ease of use (PEU) on BI.

Using data collected from a survey study, we tested the research models. Our data analysis indicates that the direct effect of privacy concern on behavioral intention is not significant. On the other hand, privacy concern significantly moderates the effects of PU and PEU on BI.

Our research aims to better understand the impact of privacy concern on users' acceptance of SNW. While some prior studies have been done to examine privacy concern in the context of SNW, the goal of our study is to empirically evaluate the direct and moderating effect of privacy concern on users' acceptance of SNW. Latest studies in the IS field (von Stetten *et al.*, 2011; McKnight *et al.*, 2011) are consistent with our finding that privacy concern has no significant impact on intention to use SNWs. In addition to testing the direct impact of privacy concern, this study is one of the first to examine the moderating effect of privacy concern in the context of SNWs. Therefore, this study provides additional insights into the dynamics of privacy issues in SNW settings. The research community may build on the findings of the present study to investigate other related variables, such as privacy control, age, and gender, as they are related to privacy concern in SNW.

Aside from its theoretical value, our research results have significant practical implications. The findings may provide SNW operators with a deeper understanding of how privacy concern may affect users' acceptance of a particular SNW. First, the absence of a significant impact of privacy concern on intention to use SNWs may explain why users keep using certain SNWs (for example, Facebook) even after reports of privacy violations have been released. Second, based on the findings from this study, the operators of SNW should develop different strategies and tactics to enhance users' acceptance depending on their level of privacy concern. To engage users who have a relatively high level of privacy concern, efforts should be focused on improving the usefulness of the site. This is because (as shown in Figure 4), for users with high privacy concern, perceived usefulness has a significant impact on their usage intention while perceived ease of use does not. For these users, SNW operators need to identify their social networking needs such as friendship and a sense of belonging. Then the corresponding features can be developed and promoted to these users to improve the perceived usefulness. On the other hand, if users have relatively low privacy concern, features that make users perceive the system both easy to use and useful should be adopted to engage them, since both perceptions significantly affect such users' acceptance. For example, the user interface should include intuitive icons and navigation schemes to allow users to easily update profiles, add comments, search for information, etc.

There are several limitations to our study. First, the research respondents are largely young college students. While a variance in privacy concern exists among them, the overall level of variance may not represent the general population of SNW users. Future research may investigate the impact of privacy concern on different age

groups. Second, SNW users are located in different countries across the world. Different cultures may have different privacy orientations, which potentially have different influence on SNW usage pattern. The research respondents of the present study are American college students. Thus, the impact of culture was not examined in this study. Third, this study focused on assessing the impact of privacy concern on SNW usage intention. It did not investigate the sources of privacy concern. Additional research that can identify the determinants of privacy concern in SNW context may provide valuable knowledge to SNW operators, marketers, and other parties.

There are several areas about privacy concern in SNW settings that warrant further investigation. First, the sources of privacy concern in the context of online social networking can be identified. The findings may help SNW operators design effective privacy controls to reduce user's privacy concern. Second, the interplay of some demographic information and privacy concern can be further investigated. For instance, age, work experience, and Internet experience may affect SNW users' level of privacy concern. Third, longitudinal studies can be done to examine the individual user's privacy concern over time. This may provide valuable insights into the dynamic nature of privacy concern.

### References

- Acquisti, A. and Gross, R. (2006), "Imagined communities: awareness, information sharing, and privacy on the Facebook", *Lecture Notes in Computer Science*, Springer, Heidelberg, pp. 36-58.
- Ajzen, I. and Fishbein, M. (1980), *Understanding Attitudes and Predicting Behavior*, Prentice Hall, Englewood Cliffs, NJ.
- Alexa (2010), "Top 500 sites on the web", available at [www.alexa.com/topsites](http://www.alexa.com/topsites) (accessed January 28, 2010).
- Amoako-Gyampah, K. and Salam, A.F. (2004), "An extension of the technology acceptance model in an ERP implementation environment", *Information & Management*, Vol. 41 No. 6, pp. 731-45.
- Barnes, S.B. (2006), "A privacy paradox: social networking in the United States", *First Monday*, Vol. 11 No. 9.
- Boyd, D.M. (2008), "Facebook's privacy trainwreck: exposure, invasion, and social convergence", *Convergence*, Vol. 14 No. 1, pp. 13-20.
- Boyd, D.M. and Ellison, N.B. (2007), "Social network sites: definition, history, and scholarship", *Journal of Computer-Mediated Communication*, Vol. 13 Nos 1, article 11.
- Cha, J. (2010), "Factors affecting the frequency and amount of social networking site use: motivations, perceptions, and privacy concerns", *First Monday*, Vol. 15 No. 12, p. 12.
- Chew, M., Balfanz, D. and Laurie, B. (2008), "(under)Mining privacy in social networks", paper presented at Web 2.0 Security and Privacy 2008, Oakland, CA.
- Chin, W.W. (1998), "Issues and opinion on structural equation modeling", *MIS Quarterly*, Vol. 22 No. 1, pp. vii-xvi.
- Cortina, J.M., Chen, G. and Dunlap, W.P. (2001), "Testing interaction effects in LISREL: examination and illustration of available procedures", *Organizational Research Methods*, Vol. 4 No. 4, pp. 324-60.

- Dabholkar, P.A. and Bagozzi, R. (2002), "An attitudinal model of technology-based self-service: moderating effects of consumer traits and situational factors", *Journal of Academy of Marketing Science*, Vol. 30 No. 3, pp. 184-201.
- Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 318-40.
- Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989), "User acceptance of computer technology: a comparison of two theoretical models", *Management Science*, Vol. 35 No. 8, pp. 982-1003.
- Dwyer, C., Hiltz, S.R. and Passerini, K. (2007), "Trust and privacy concern within social networking sites: a comparison of facebook and myspace", paper presented at the Thirteenth Americas Conference on Information Systems, Keystone, CO.
- Facebook (2007), "Leading web sites offer Facebook beacon for social distribution", available at: [www.facebook.com/press/releases.php?p=9166](http://www.facebook.com/press/releases.php?p=9166) (accessed January 28, 2010).
- Featherman, M. and Fuller, M.A. (2003), "Applying TAM to e-services adoption: the moderating role of perceived risk", *Proceedings of 36th Hawaii International Conference on System Sciences (ICSS 2003)*, Big Island, HI, January 6-9.
- Featherman, M.S. and Pavlou, P.A. (2002), "Predicting e-services adoption: a perceived risk facets perspective", *Eighth Americas Conference on Information Systems, Dallas, TX*.
- Fogel, J. and Nehmad, E. (2009), "Internet social network communities: risk taking, trust, and privacy concerns", *Computers in Human Behavior*, Vol. 25, pp. 153-60.
- Gallaughar, J. (2010), *Information Systems: A Manager's Guide to Harnessing Technology*, FlatWorld Knowledge, Irvington, NY.
- Galliers, R. (1992), *Information Systems Research: Issues, Methods & Practical Guidelines*, Blackwell Scientific, Boston, MA.
- Gefen, D. and Straub, D.W. (1997), "Gender differences in the perception and use of e-mail: an extension to the technology acceptance model", *MIS Quarterly*, Vol. 21 No. 4, pp. 389-400.
- Gefen, D. and Straub, D.W. (2000), "The relative importance of perceived ease of use in is adoption: a study of ecommerce adoption", *Journal of the Association for Information Systems*, Vol. 1 No. 8, pp. 1-28.
- Gefen, D., Straub, D.W. and Boudreau, M.-C. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4 No. 7, pp. 1-70.
- George, J. (2002), "Influences on the intent to make internet purchases", *Internet Research*, Vol. 12 No. 2, pp. 165-80.
- Gross, R. and Acquisti, A. (2005), "Information revelation and privacy in online social networks", *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA*, pp. 71-80.
- Hair, J.F. Jr, Anderson, R.E., Tatham, R.L. and Black, W.C. (1998), *Multivariate Data Analysis with Readings*, 5th ed., Prentice Hall, Englewood Cliffs, NJ.
- Hu, P.J., Chau, P., Sheung, O. and Tam, K. (1999), "Examining the technology acceptance model using physician acceptance of telemedicine technology", *Journal of Management Information Systems*, Vol. 16 No. 2, pp. 91-112.
- Igbaria, M., Guimaraes, T. and Davis, G. (1995), "Testing the determinants of microcomputer usage via a structural equation model", *Journal of Management Information Systems*, Vol. 11 No. 4, pp. 87-114.
- Im, I., Kim, Y. and Han, H.J. (2008), "The effects of perceived risk and technology type on users' acceptance of technologies", *Information & Management*, Vol. 45, pp. 1-9.

- Introna, L.D. and Pouloudi, A. (1999), "Privacy in the information age: stakeholders, interests and values", *Journal of Business Ethics*, Vol. 22 No. 1, pp. 27-38.
- Jaroslowsky, R. (2010), "Facebook founder has nothing to hide except privacy blind spot", *Business Week*, June 9.
- Johnson, B. (2010), "Privacy no longer a social norm, says Facebook founder", *The Guardian*, January 11.
- Johnson, J.L. (1989), "Privacy and the judgment of others", *The Journal of Value Inquiry*, Vol. 23 No. 2, pp. 157-68.
- Karyda, M., Gritzalis, S., Park, J.H. and Kokolakis, S. (2009), "Privacy and fair information practices in ubiquitous environments", *Internet Research*, Vol. 19 No. 2, pp. 194-208.
- King, W.R. and He, J. (2006), "A meta-analysis of the technology acceptance model", *Information & Management*, Vol. 43, pp. 740-55.
- Lanier, C.D. and Saini, A. (2008), "Understanding consumer privacy: a review and future directions", *Academy of Marketing Science Review*, Vol. 12 No. 2.
- Lee, Y., Kozar, K. and Larsen, K. (2003), "The technology acceptance model: past, present, and future", *Communications of the Association for Information Systems*, Vol. 12 No. 50, available at: <http://aisel.aisnet.org/cais/vol12/iss1/50>.
- McCarthy, C. (2008), "AOL buys social network Bebo for \$850 million", available at: [http://news.cnet.com/8301-13577\\_3-9893014-36.html](http://news.cnet.com/8301-13577_3-9893014-36.html) (accessed January 30, 2010).
- McKnight, D.H., Lankton, N. and Tripp, J. (2011), "Social networking information disclosure and continuance intention: a disconnect", *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 44)*, Manoa, HI, January 4-7.
- McWhirter, D.A. and Bible, J.D. (1992), *Privacy as a Constitutional Right*, Quorum Books, New York, NY.
- Milne, G.R. and Gordon, M.E. (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework", *Journal of Public Policy & Marketing*, Vol. 12, Fall, pp. 206-15.
- Nowak, G. and Phelps, J. (1992), "Understanding privacy concerns", *Journal of Direct Marketing*, Vol. 6 No. 4, pp. 28-39.
- Nowak, G. and Phelps, J. (1995), "Direct marketing and the use of individual-level consumer information: determining how and when 'privacy' matters", *Journal of Direct Marketing*, Vol. 9 No. 3, pp. 46-60.
- Nunnally, J.C. (1978), *Psychometric Theory*, 2nd ed., McGraw-Hill, New York, NY.
- Pavlou, P.A., Liang, H. and Xue, Y. (2007), "Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective", *MIS Quarterly*, Vol. 31 No. 1, pp. 105-36.
- Phelps, J., Nowak, G. and Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 27-41.
- Pinsonneault, A. and Kraemer, K. (1993), "Survey research methodology in management information systems: an assessment", *Journal of Management Information Systems*, Vol. 10 No. 1, pp. 75-106.
- Preibusch, S., Hoser, B., Gürses, S. and Berendt, B. (2007), "Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling", *Proceedings of the Data Mining for User Modelling Workshop (DM.UM '07)*, Corfu, pp. 50-62.
- Prosser, W. (1960), "The torts of privacy", *California Law Review*, Vol. 48 No. 3, pp. 383-423.

- Rimenschneider, C. and Hardgrave, B. (2001), "Explaining software development tool use with the technology acceptance model", *Journal of Computer Information Systems*, Vol. 41 No. 4, pp. 1-8.
- Rose, G., Khoo, H. and Straub, D. (1999), "Current technological impediments to business-to-consumer electronic commerce", *Communications of the AIS*, Vol. 1 No. 16, pp. 1-73.
- Rosenblum, D. (2007), "What anyone can know: the privacy risks of social networking sites", *IEEE Security and Privacy*, Vol. 5 No. 3, pp. 40-9.
- Schepers, J. and Wetzels, M. (2007), "A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects", *Information & Management*, Vol. 44 No. 1, pp. 90-103.
- Schmidt, T.S. (2006), "Inside the backlash against Facebook", *Time*, September 6.
- Shin, D.H. (2010), "The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption", *Interacting with Computers*, Vol. 22 No. 5, pp. 428-38.
- Shin, D.H. and Kim, W.Y. (2008), "Applying the Technology Acceptance Model and flow theory to cyworld user behavior: implication of the Web 2.0 user acceptance", *CyberPsychology & Behavior*, Vol. 11 No. 3, pp. 378-82.
- Siklos, R. (2005), "News Corp. to acquire owner of Myspace.com", *New York Times*, July 18.
- Sloane, J. (2007), "Facebook got its \$15 billion valuation – now what?", *Wired Magazine*.
- Story, L. and Stone, B. (2007), "Facebook retreats on online tracking", *New York Times*, November 30.
- Straub, D., Keil, M. and Brenner, W. (1997), "Testing the technology acceptance model across cultures: a three country study", *Information & Management*, Vol. 33 No. 1, pp. 1-11.
- Sun, H. and Zhang, P. (2006), "The role of moderating factors in user technology acceptance", *International Journal of Human-Computer Studies*, Vol. 64 No. 2, pp. 53-78.
- Sweney, M. (2010), "Mark Zuckerberg: Facebook 'almost guaranteed' to reach 1 billion users", *The Guardian*.
- Venkatesh, V. (2000), "Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model", *Information Systems Research*, Vol. 11 No. 4, pp. 342-65.
- Venkatesh, V. and Davis, F.D. (2000), "A theoretical extension of the technology acceptance model: four longitudinal field studies", *Management Science*, Vol. 46 No. 2, pp. 186-204.
- Venkatesh, V., Davis, F. and Morris, M. (2007), "Dead or alive? The development, trajectory and future of technology adoption research", *Journal of the Association for Information Systems*, Vol. 8 No. 4, available at: <http://aisel.aisnet.org/jais/vol8/iss4/10>.
- Venkatesh, V., Morris, M.G., Davis, F.D. and Davis, G.B. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-78.
- von Stetten, A., Wild, U. and Chrennikow, W. (2011), "Adopting social network sites - the role of individual IT culture and privacy concerns", *Proceedings of the Americas Conference on Information Systems (AMCIS 2011)*, Detroit, MI, 4-7 August.
- Warren, S.D. and Brandeis, L. (1890), "The right of privacy", *Harvard Law Review*, Vol. 4 No. 5, pp. 193-220.
- Westin, A. (1967), *Privacy and Freedom*, Atheneum, New York, NY.
- Willis, T. (2008), "An evaluation of the technology acceptance model as a means of understanding online social networking behavior", *Theses and Dissertations*, Paper 568, available at <http://scholarcommons.usf.edu/etd/568>.

Zhou, T. (2011), "Understanding online community user participation: a social influence perspective", *Internet Research*, Vol. 21 No. 1, pp. 67-81.

### Further reading

Nicolaou, A.I. and Harrison, M.D. (2006), "Perceived information quality in data exchanges", *Information Systems Research*, Vol. 17 No. 4, pp. 332-51.

### Appendix. Measurement items

On a scale of 1 to 7 (1 = strongly agree, 2 = agree, 3 = somewhat agree, 4 = neutral, 5 = somewhat disagree, 6 = disagree, 7 = strongly disagree), please rate each of the following statements.

#### *Perceived usefulness (PU)*

- (PU1) Using this online social network makes it convenient for me to stay in touch with my friends and classmates.
- (PU2) Overall, I find this online social network to be useful.
- (PU3) Using this online social network is useful for me to network with other people.

#### *Perceived ease of use (PEU)*

- (PEU1) It is easy for me to become skillful at using this online social network.
- (PEU2) Overall, I find this online social network to be easy to use.
- (PEU3) Interacting with this online social network does not require a lot of mental effort.

#### *Privacy concern (PC)*

- (PC1) I am concerned about the negative consequences of unknown parties accessing my private information on this online social network.
- (PC2) I am concerned that my private information on the online social network may be misused.
- (PC3) I am concerned that unknown parties have access to my private information on this online social network.

#### *Behavioral intention (BI)*

- (IN1) If I could, I would like to stop using this online social network.
- (IN2) I intend to continue using this online social network.
- (IN3) It is my intention to use this online social network in the future.

*Note:* The responses to the reverse-worded IN1 was re-coded in data analysis

---

**About the authors**

Xin Tan is an Assistant Professor in the Department of Information Systems and Decision Sciences at Fairleigh Dickinson University. He received his PhD from the University of Nebraska-Lincoln. His current research interests include the development and implementation of information systems, and user acceptance of emerging information technologies and information systems. He has published research papers in *Communications of the ACM*, *Information Systems Journal*, *Data & Knowledge Engineering*, *IEEE Transactions on Professional Communication*, *Information Resource Management Journal*, and *Journal of Computer Information Systems*. Xin Tan is the corresponding author and can be contacted at: [xtan@fdu.edu](mailto:xtan@fdu.edu)

Li Qin is an Assistant Professor of Management Information Systems in the Department of Information Systems and Decision Sciences at Silberman College of Business, Fairleigh Dickinson University. She received her PhD and MBA from Rutgers University. Her research interests include semantic web, information security, and electronic commerce.

Yongbeom Kim is a Professor of Information Systems at Fairleigh Dickinson University. He received his PhD in information systems from the Stern School of Business of New York University. His research interests include performance evaluation of interactive computer systems, enterprise systems, and IS education. He has published in such journals as the *Journal of Management Information Systems*, *Information Processing & Management*, *Information Resources Management Journal*, *Business Process Management Journal*, and *Journal of Information Systems Education*.

Jeffrey Hsu is an Associate Professor of Information Systems at the Silberman College of Business, Fairleigh Dickinson University. He is the author of numerous papers, chapters, and books, and has previous business experience in the software, telecommunications, and financial industries. His research interests include human-computer interaction, e-commerce, IS education, and mobile/ubiquitous computing. He is Managing Editor of *International Journal of Data Analysis and Information Systems (IJDAIS)*, Associate Editor of *International Journal of Information and Communication Technology Education (IJICTE)*, and is on the editorial board of several other journals. Dr Hsu received his PhD in Information Systems from Rutgers University, a MS in Computer Science from the New Jersey Institute of Technology, and a MBA from the Rutgers Graduate School of Management.