AN EMPIRICAL INVESTIGATION OF THE PRIVACY CONCERNS OF SOCIAL NETWORK SITE USERS IN TAIWAN

Kuang-Ming Kuo, Paul C. Talley*
Department of Healthcare Administration, I-Shou University, Taiwan (R.O.C.)
Department of International Business Administration, I-Shou University, Taiwan (R.O.C.)
Email: atlanta.ga@msa.hinet.net, Email: kuangmingkuo@gmail.com

Abstract

The study has two purposes: (1) to investigate the impact of awareness and control on Social Network Sites (SNSs) users’ information privacy concerns, and (2) to understand how information privacy concerns and the notion of trust shape users’ risk perceptions. The study collects data using survey methodology. A total of 356 SNS users are analyzed via partial least squares. Users regard awareness of and direct control over personal information disclosed on SNSs to be relative to their information privacy concerns in a positive and a negative direction, respectively. Furthermore, information privacy concerns and trust may collectively influence their perceived risk towards SNS. It is therefore advisable for SNS service providers to pay more attention to their own understanding of how awareness and control principles influence users’ information privacy concerns. Further, SNS providers should also propose more effective means necessary to reduce users’ information privacy concerns overall.

Keywords: Information privacy concerns, Social network site, Trust, Risk, Social contract theory

1. Introduction

A Social Network Site (SNS) refers to a virtual community in which individuals with similar interests can intercommunicate by sharing personal profiles (Shin, 2010). SNSs, such as Facebook, MySpace, and Google+, have become popular online communities that numerous people use regularly to socialize with their friends, families, and colleagues. As of January 2014, Facebook has more than 1.3 billion monthly active users around the globe (Statistic Brain, 2014). Via SNSs, individuals can not only search and observe their friends through various postings, but they can also see who their friends choose to know. It is now commonplace for any given individual to have hundreds, or even thousands, of friends located around the world. Hence, a SNS truly possesses abundant personal information readily available to viewers for any reason.

While SNSs offer a great variety of chances for interpersonal communicative interaction, the public has already voiced far-reaching concerns about SNSs (Hoy & Milne, 2010). One critical issue is the privacy concerns aroused when an SNS collects so much detailed personal information such as gender, interests, hometown, residence, mobile phone number, campus room, favorite stuff, among others (Lewis, Kaufman, & Christakis, 2008), and the potential for such information to possibly be misused (Dwyer, 2011; Young & Quan-Haase, 2013). Further, leading SNSs, including Facebook and Google, publicly express that privacy should be regarded as an unimportant concern (Dwyer, 2011). The general attitude that has been adopted by two of the biggest social networks, Google and Facebook, is that users should assume full responsibility for their own privacy concerns through a process of self-control, self-censorship, lowered expectations, and acclimatization (Huff Post Tech, 2011; Protalinski, 2011). Facebook even proclaims that as new privacy problems come along with the introduction of newer functions, people will just have to learn to accept it as they always have (Pepitone, 2014).

Users’ attitudes toward privacy may influence the amount and the kind of information posted and shared on SNSs (Acquisti & Gross, 2006), which may in its turn have an important impact on the vibrancy (i.e., driving of profitability) of SNSs (Stutzman, Capra, & Thompson, 2011; Weiss, 2009). Without users providing a regular input of content, these SNSs would become less attractive to potential users. Consequently, a knowledge of what factors
arouse SNS users’ information privacy concerns and, in turn, what consequences those information privacy concerns will cause, are imperative for SNS service providers to possess in order to know how to keep the proliferation of SNSs unimpaired.

Previous studies regarding SNS focused on issues such as why users participate in such virtual communities (Tsai & Pai, 2014), or on their loyalty to SNS (Chiu, Cheng, Huang, & Chen, 2013). Further, most research on SNS is mainly U.S. based (e.g., Stutzman et al., 2011), it is thus necessary to culturally balance understandings of SNS usage by considering the issue from a global perspective. Taiwanese are now the biggest users of Facebook in Asia and Twitter also interests in boosting its presence in Taiwan (Chiu, 2013). Hence, Taiwan thus provides an interesting context in which to explore SNS usage. In Taiwan, there is the Computerized Personal Information Protection Act which regulates the privacy protection of personal information (Department of Justice, 2010). However, the concept of privacy protection is still evolving in Taiwan as compared with the United States and the European market, where government regulation is a commonly adopted approach to protect privacy (Culnan & Bies, 2003).

Privacy concerns present an important issue in e-commerce because consumers care about whether their disclosed personal information is fairly handled by online organizations. The primary concerning object is the online organization that collects and then uses individual’s personal information. However, the concerning objects in SNS context are far more complicated than that of e-commerce. Besides, SNS service providers may collect and use SNS users’ personal information, SNS users’ friends and other users may also collect and use such information for their own advantage. These differing concerned objects make the SNS a different context from that of general e-commerce. To better understand the complex privacy concerns shared among various concerned objects in SNSs, it is better to adopt a “divide and conquer” strategy. Hence, our study first focuses on two salient concerned objects (i.e., users themselves and service providers) in the SNS context to investigate the privacy issue.

1.1 Privacy, information privacy, and information privacy concerns

The definitions of privacy vary in different disciplines and there is no single concept of privacy that can be embraced across all disciplines (Smith, Dinev, & Xu, 2011). For example, privacy refers to the “right to be left alone” in the law (Warren & Brandeis, 1890) and “control” in social sciences (Culnan, 1993). Further, Altman (1976) argues that privacy encompasses social and interpersonal aspects. Consequently, to effectively measure privacy is not an easy task and there is a tendency to use privacy concerns as a proxy for measuring privacy (Smith et al., 2011). Information privacy concerns, a subset of the overall concept of privacy (Bélanger & Crossler, 2011), refers to the ability of an individual to personally control information about one’s self while information privacy concerns are the degree to which an individual is concerned about organizational practices related to the collection and use of his/her personal information (Smith, Milberg, & Burke, 1996).

Smith et al. (1996) proposed and validated an instrument that measures the primary dimensions of individual’s information privacy concerns. The result was a 15-item instrument that comprises four dimensions of the concerns for information privacy (CFIP) scale: collection, unauthorized secondary use, improper access, and errors. Stewart and Segars (2002) further verified these four dimensions. Malhotra, Kim, & Agarwal (2004) also developed a multi-dimensional scale of Internet users information privacy concerns (IUIPC). IUIPC contains three components of privacy concerns: collection of personal information, control over personal information, and awareness of organizational privacy. It should be noted that CFIP was more widely adopted than IUIPC, but IUIPC has been under-utilized (Bélanger & Crossler, 2011).

Malhotra et al. (2004) viewed control as the most important component of IUIPC. However, Margulis (2003a, 2003b) argued that viewing control-related phenomenon as privacy has not helped much to illuminating this issue. Further, Laufer & Wolfe (1977, p. 26) recognized control as a mediating variable in a privacy system since “a situation is not necessarily a privacy situation simply because the individual perceives, experiences or exercises control.” In addition to collection, awareness is another component of IUIPC (Malhotra et al., 2004). Dinev & Hart (2006a) proposed social awareness which refers to an individual’s active involvement and increased interest in focal issues to predict
privacy concerns. For example, Internet users with high social awareness (i.e., interested in social issues and policies) will closely track Internet privacy issues. Further, plenty of studies also demonstrate that awareness is a determinant of privacy concerns (Cepedes & Smith, 1993; Foxman & Kilcoyne, 1993; Sheehan & Hoy, 2000). Based on the above discussions, it may be reasonable to assume that control and awareness is different from the privacy concept and can be considered as antecedents to such privacy concerns.

1.2 Trust and risk in social networking context

Trust and risk are two salient beliefs in any information privacy context (Malhotra et al., 2004). Altman (1976) argued that privacy exists as an interpersonal boundary process which depicts a boundary between the person and others. Further, privacy can also be viewed as an input and output process (Altman, 1976) which may refer to how a person may receive communications from others, or send output comprised of information, to others. An interpersonal boundary may be opened, or closed for that matter, primarily based upon interpersonal factors such as the level of trust on the information receiver (Altman & Taylor, 1973). Further, it is the risk that elicits the person’s protective behavior of closing the interpersonal boundary which separates public and private information (Xu, Dinev, Smith, & Hart, 2011). In an e-commerce context, Pan & Zinkhan (2006) argued that consumers are worried about their privacy risks along with the collection or secondary use of personal information without their given consent. Consequently, rendering personal information to online organizations demands individuals to surrender a certain level of trust. Okazaki, Li, & Hirose (2009) found that privacy concerns were a significant predictor of trust and perceived risk in mobile advertising.

Meanwhile, trust and risk have been identified as vital factors that affect individual’s intentions in a social networking context. For example, Taddei & Contena (2013) found that trust influences what people are willing to share in SNSs. Shin (2010) reported that trust significantly influences an individual’s attitude toward SNSs. Further, Fogel and Nehmad (2009) found that risk-taking belief is significantly different between male and female as well as between those who maintain SNS profiles and those do not. Gross & Acquisti (2005) list several risks that SNS users may face including embarrassment, blackmailling, stalking, and even identity theft. Further, McKinsey & Company (2013) reported that only 6% of global executives do not associate any risks with use of social technologies including SNS. Brandtzæg, Liders, & Skjetne (2010) further argue that trust has not been sufficiently investigated in social networking context. Based on the above discussions, it seems timely and reasonable to investigate the role that trust and risk play in the use of SNSs.

1.3 Theoretical background

1.3.1 Antecedents—privacy concerns—outcomes model

The study of privacy concerns across disciplines and contexts may be facilitated by Smith et al.’s (2011) proposal of an APCO (antecedents—privacy concerns—outcomes) model. The APCO model clearly demonstrates the relationships between and among privacy concerns and their antecedents and consequences. The antecedents of privacy concerns may include privacy experiences, privacy awareness, personality differences, demographic differences, and culture/climate. Notably, these relationships between antecedents and privacy concerns have not been affirmed through sufficient studies (Smith et al., 2011). Contrary to the antecedents, the outcomes of privacy concerns which may include behavioral intention (e.g., to disclose personal information), regulation issues, privacy calculus (i.e., weighing between risks/costs and benefits), trust, and risk have been largely investigated.

1.3.2 Social contract theory

Social Contract Theory (SCT) provides one of the theoretical underpinnings for our study. SCT postulates that the exchange of consumers’ personal information with a marketer is viewed similar to an implied social contract (Pan & Zinkhan, 2006). One of the primary talking points of SCT is that “norm-generation micro-social contracts must be grounded in informed consent, buttressed by rights of existence and voice” (Dunfee, Smith, & Ross, 1999, p. 19), which is useful for the study of perceptual fairness and justice within information exchange contexts (Malhotra et al., 2004). A social contract is initiated when social norms (i.e., generally recognized obligations) are expected to govern the behavior of those involved. The implied social contract is considered “fair” if the marketer obeys fair information practices which reflects three conditions.
of “knowledge, notice, and no” (Culnan, 1995). Knowledge refers to consumers’ awareness that personal information has been collected. Then, consumers must become aware that their personal information may be shared with other interested parties. Lastly, consumers must be empowered to confine the sharing of their personal information to other parties by reserving the right to say “no” to such an exchange. The above conditions may imply that consumers are presumed to possess certain rights regarding their information privacy when engaging online transactions (Pan & Zinkhan, 2006). More specifically, it is knowledge (i.e., consumers are aware of collection and informed about reuse of personal information) and control (consumers exercise control over reuse) that make privacy exist (Culnan, 1995) from the lens of SCT. The notion of SCT has been applied to many studies concerning business/marketing ethics (e.g., Culnan, 1995; Dunfee et al., 1999; Malhotra et al., 2004) and also SNS privacy (e.g., Fogel & Nehmad, 2009), which provided a reasonable foundation for studying privacy issues in a SNS context.

1.4 Previous SNS privacy-related literature

There are a number of studies focusing privacy issues in a SNS context. For example, Fogel & Nehmad (2009) used college students as subjects and found that individuals with SNS profiles and males have greater risk-taking attitudes. Further, students trust Facebook more than MySpace. Females are concerned with privacy more than males. Shin (2010) examined the SNS adoption pattern of users and found that security, privacy, and trust predict users’ attitudes toward SNS adoption. Mohamed & Ahmad (2012) investigated the antecedents (i.e., perceived severity, perceived vulnerability, self-efficacy, response efficacy, reward, and gender) and consequences (privacy measure) of privacy concerns in a SNS context. The results reveal that only response efficacy and rewards are not significant predictors of privacy concerns, and privacy concerns significantly predict privacy measures. Brandtzæg et al. (2010) explored the influence of content sharing and sociability on SNS users’ privacy experiences and usage behavior. They found that content sharing and sociability may challenge users’ social privacy notions over which they are mostly concerned. Lewis et al. (2008) investigated the factors influencing SNS users’ preference for privacy and found that both social influences and personal incentives are significant predictors. All these studies provide insightful conclusions and have advanced our knowledge of privacy in a SNS context. However, none of these studies empirically validated constructs including awareness, control, privacy concerns, trust, and risk perceptions in one model simultaneously. Although our proposed model is simple, the relationships among these constructs cannot be oversimplified and may require thoughtful study. Without clarification of the relationships among these constructs, it may not be able to well manage privacy issues regarding SNSs.

The purposes of this study are twofold. The first purpose is to investigate the impact of awareness and control perceptions on SNS users’ information privacy concerns. The second purpose is to understand how information privacy concerns and trust shape users’ risk perceptions. The findings of the present study can assist the respective SNSs to obtain a better knowledge of users’ beliefs and responses to relative privacy concerns so that the SNSs will not negatively impact their users’ privacy anticipations. Such assistance may lead to higher adoption rates and regular usage of the SNSs.

2 Research model and research hypotheses

2.1 Conceptual model formulation

To build our research framework, we first use the APCO model as our overarching foundation in order to articulate that privacy concerns mediate between their antecedents and consequences. Hence, the foci of this research are on the antecedents and consequences of SNSs users’ privacy concerns. Regarding the antecedents, the rationale is explained as follows. We consider the relationships between SNS users and service providers as an implied social contract, as stated in the SCT. When users agree to register and use the SNS, both the behaviors of users and service providers are governed by social norms. That is, users should be informed that SNSs will collect their personal information, and then the collected information may be shared with third parties. This belief basically reflects the construct of awareness which will be integrated into our model. Meanwhile, to be a fair social contract, users should be further empowered to control the SNS’s handling of their personal information, and this belief is equivalent to the construct of control in our model. If SNS service providers do not inform users about their information practices, or if they render users’ personal information to third parties without the
permissions of users, SNS users may thus arouse privacy concerns. Based on the above discussions, awareness and control are considered as two antecedents of privacy concerns according to SCT (Dunfee et al., 1999).

Second, regarding the consequences of privacy concerns, when SNS users provide personal information to SNSs, they may anticipate that SNSs will protect the privacy rights inherent to their personal information. Consequently, users may demonstrate a greater level of trust if they believe that SNS service providers will protect their information privacy and will not break the implied social contract. Contrarily, SNS users may also show a certain degree of risk if they suspect that SNS service providers may breach the implied social contract and thus violate their information privacy. According to SCT, both trust and risk are thus regarded as the consequences of privacy concerns. By integrating the APCO and SCT, we were able to design our research framework (see Figure 1).

Prior literature has found that a number of variables which were not included in our research framework also have impact on individual’s risk perceptions. For example, Mohamed & Ahmad (2012) confirmed that females were more concerned with information privacy than males. Fogel & Nehmad (2009) reported that males had significantly higher scores than females in risk aversion perceptions. Rhodes & Pivik (2011) found that gender and age influence an individual’s perceived risk when individuals are engaged in risky driving habits. SNS users express significantly more trust on Facebook than Myspace (Dwyer, Hiltz, & Passerini, 2007; Fogel & Nehmad, 2009). Further, Sheehan (1999) found that males and females significantly differ in how online practices influence their privacy. Hence, to eliminate those unknown influences, we have included three control variables in the proposed model, namely gender (Fogel & Nehmad, 2009; Sheehan, 1999; Mohamed & Ahmad, 2012; Rhodes & Pivik, 2011), age (Rhodes & Pivik, 2011), and also the types of SNSs (Dwyer et al., 2007; Fogel & Nehmad, 2009).

2.2 Research hypotheses

2.2.1 The effect of awareness on privacy concerns

The present study defines the factor of awareness as the degree to which the user is concerned about knowing the SNS’s information practices (Culnan, 1995; Malhotra et al., 2004), while privacy concerns refer to an individual’s concerns about any possible future loss of privacy as a result of information revelation to SNSs (Xu et al., 2011). In general, consumers do not know that their personal information was collected until they receive unsolicited contacts as a result (Sheehan & Hoy, 2000). That is, consumers will not become concerned about privacy when marketers collect and use their personal information without informing them until they are made aware in some manner of this prior event (Milne, 2000). Similarly, SNS users may perceive their privacy right is protected only if SNS service providers can comply with the implied social contract by informing users of their information practices according to SCT (Dunfee et al., 1999). Culnan (1995) found that consumers who are unaware of name removal procedures from a mailing list are less likely to be concerned about privacy than consumers who are aware of the same. Debatin, Lovejoy, Horn, & Huges (2009) reported that those SNS users who were not familiar with privacy settings were also more likely to not protect their profiles. Further, prior studies (e.g., Malhotra et al.,
2004; Milne, 2000) have also investigated the association between awareness and privacy concerns and have affirmed that consumers’ awareness is associated alongside privacy concerns. Consequently, the greater the awareness of an SNS’s information practices are by the user, the stronger the privacy concerns those users will have. Thus, the present study hypothesizes the following:

H1: Awareness will have a positively influenced relationship with SNSs users’ information privacy concerns.

2.2.2 The effect of control on privacy concerns

Sheen & Hoy (2000) found that the notion of control is an important dimension, as are related notions of exchange and long-term relationships. In this study, control refers to an individual’s beliefs that they can manage the circulation of their information (Xu et al., 2011). According to the concept of fair social contract, SNS service providers should empower users with the decision as to how their personal information is used; and, by giving users more control, SNSs will alleviate users’ privacy concerns (Phelps, Nowak, & Ferrell, 2000). Previous studies (Culnan, 1993; Foxman & Kilcoyne, 1993) revealed that information privacy will be perceived only when individuals are given partial/full control over their own information. Prior study (Phelps et al., 2000) has also determined that control is closely associated with consumers’ routine privacy concerns regarding shared personal information. More specifically, individuals’ perceptions of control over the circulation of their information were negatively associated with privacy concerns (Milne & Boza, 1999; Xu et al., 2011; Xu, Michael, & Chen, 2013; Zhao, Lu, & Gupta, 2012). That is, individuals will be less concerned about personal privacy given that they feel they can control the dissemination of their own information within limits set by the users themselves. Thus, the second hypothesis postulates the following:

H2: Control will have a negatively influenced relationship with SNSs users’ privacy concerns.

2.2.3 The effect of privacy concerns on trust

This study defines trust as an individual’s willingness to undertake a level of risk while experiencing uncertain circumstances (Milne & Culnan, 2004). Users are extremely concerned about the disposition of their personal information and these privacy concerns have a detrimental influence on e-commerce (Dinev & Hart 2006a, 2006b). Hence, it is deemed important for organizations to find solutions related to overall privacy concerns rather than simply to ignore them. From a social contract viewpoint, SNS users may trust SNS service providers to a lesser extent if users believe that service providers have not handled users’ personal information fairly (i.e., violating the implied social contract). In extant literature, online information privacy is often viewed as a negative antecedent to trust, rather than as a direct influence on behavioral intention (Joinson, Reips, Buchanan, & Schofield, 2010). For instance, Shin (2010) affirmed that if users sensed that an SNS safeguards their privacy, those users will have higher trust in it as a direct result. Further, Van Slyke, Shim, Johnson, & Jiang (2006) affirmed that concern for privacy influences individuals’ trust whenever shopping at Amazon.com. Extrapolating from the literature to this study, it could be argued that heightened privacy concerns should consequently lower trust in SNSs. This study therefore states the hypothesis:

H3: Privacy concerns will have a negative relationship with individual’s trust about SNSs.

2.2.4 The effect of privacy concerns on risk

Risk perception is an individual’s beliefs concerning the possibility of gains or losses related to the acquisition of a product/service online (Mayer, Davis, & Schoorman, 1995). Prior literature (Culnan, 1995; Phelps et al., 2000) asserted that the information interchange taking place between individuals and organizations serves to create an implied social contract. One key point of such a contract is that organizations will use and then safeguard individuals’ information properly for some form of mutual benefit. People with strong privacy concerns may worry that organizations do not choose to safeguard their information adequately enough to fulfill the bilateral nature of this social contract. As a result, this may further deepen individuals’ risk perceptions when dealing with a specific online organization such as a SNS. If SNS users hold that SNS service providers choose not to realize promised obligations stated in the implied social contract, users may perceive that they are taking a significant risk with their privacy rights. Previous studies (Malhotra et al., 2004; Van Slyke et al., 2007) also provided that privacy concerns heightened an individual’s risk
perceptions. Hence, the present study proposes the following hypothesis:

H4: Privacy concerns will have a positive relationship with an individual’s risk perceptions about SNSs.

2.2.5 The effect of trust on risk

Culnan and Armstrong (1999) asserted that trust is especially imperative to reduce risk perceptions under conditions of information asymmetry, such as when an individual’s lack of knowledge about how their information will eventually be used occurs. In a social networking context, users who trust the service providers are less likely to anticipate negative outcomes when dealing with SNSs. But when potential risks increase, such as when service providers violate the implied social contract, users’ trust may become a vital factor for initiating risk-taking behavior. Numerous investigations (e.g., Jarvenpaa & Tractinsky, 1999; Okazaki et al., 2009; Pavlou, 2003) suggest that trust influences risk perceptions. Van Slyke et al. (2006) empirically validated that individuals’ trust related to e-commerce websites lowers their risk perceptions regarding those websites. From this literature, it is obvious that one result of trust is that it will possibly mitigate an individual’s risk perceptions. Based on the discussions above, the present study hypothesizes:

H5: Trust will have a negative relationship with individual’s risk perceptions about SNSs.

3. Method

3.1 Measures

The questionnaire used in this study consisted of two parts. The first part collects respondents’ demographic data, and the second part deals with their perceptions about awareness, control, information privacy concerns, trust, and risk perceptions. These research constructs were measured using previously validated instruments. Excluding demographic questions, all items were based on a 5-point Likert scale (1 for strongly disagree and 5 for strongly agree).

Based on APCO and SCT, the constructs employed in our model includes awareness which refers to the degree to which the user is concerned about knowing the SNS’s information practices (Culnan, 1995; Malhotra et al., 2004), control means an individual’s beliefs that they can manage the circulation of their information (Xu et al., 2011), privacy concerns depicts an individual’s concerns about any possible future loss of privacy as a result of information revelation to SNSs (Xu et al., 2011), trust measures an individual’s willingness to undertake a level of risk while experiencing uncertain circumstances (Milne & Culnan, 2004), and risk means an individual’s beliefs concerning the possibility of gains or losses as related to the acquisition of a product/service online (Mayer et al., 1995).

The instruments for awareness and control utilized three items respectively and were adapted from Malhotra et al. (2004) and Dinev and Hart (2004), respectively. The information privacy concerns construct was measured by using four items found in Xu et al. (2011). Trust and risk were measured by using four and five items respectively and were adapted from Malhotra et al. (2004). The original questionnaire is in English and is not appropriate for the target subjects. Thus, we used a back-translation approach to ensure that the meaning of original scales would be retained when translating the English items into a traditional Chinese version. The English version of the instrument was first translated into traditional Chinese by one author, and then an independent translator back-translated the Chinese version into English. Original and back-translated scales were then compared, and discrepancies were revised and corrected between these two versions of the questionnaires by three experts. A pretest was then conducted to establish the scales via a convenience sampling of 10 undergraduate students. Modification of words and phrases were made to items resulting in a final scale which was justified for further testing.

3.2 Sample and data collection

Since it is said that young people are most likely to join in some SNSs (Hoy & Milne, 2010), focusing research on young adults is especially important if researchers are to obtain a better knowledge of how SNSs are being connected to people’s lives. Consequently, subjects in this study were undergraduate students from a large university located in southern Taiwan. Students enrolled in various classes were invited to participate in the paper-and-pencil survey after class since the classrooms were not equipped with computers and Internet connectivity. The questionnaires were
voluntarily administered to 400 students from March 1st to April 30th, 2012 by the authors. A total of 372 surveys were collected, of which 16 were deemed unusable due to numerous missing data items.

4. Results

4.1 Descriptive statistics

Of the 356 valid responses, 56.5% of respondents were female and 43.5% were male. Nearly 72% of the respondents were 20-24 years of age. Further, the majority were sophomores (50%) while junior level students represented the fewest number of respondents (8.7%). All respondents were said to have profiles on SNSs and only 1.7% of them check their profiles less than once per week, indicating these respondents should have sufficient background knowledge about the survey content. Finally, most respondents use Facebook as their primary SNSs. Details of the respondents are shown in Table 1.

Table 1 Descriptive statistics of respondents’ characteristics

<table>
<thead>
<tr>
<th>Profile</th>
<th>Items</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>155</td>
<td>43.5</td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>201</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=19</td>
<td>91</td>
<td>25.6</td>
<td></td>
</tr>
<tr>
<td>20-24</td>
<td>257</td>
<td>72.2</td>
<td></td>
</tr>
<tr>
<td>25-30</td>
<td>6</td>
<td>1.7</td>
<td></td>
</tr>
<tr>
<td>&gt;=31</td>
<td>2</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td>College status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Freshman</td>
<td>33</td>
<td>9.3</td>
<td></td>
</tr>
<tr>
<td>Sophomore</td>
<td>178</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Junior</td>
<td>31</td>
<td>8.7</td>
<td></td>
</tr>
<tr>
<td>Senior</td>
<td>114</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>SNS profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Several times per day</td>
<td>99</td>
<td>27.8</td>
<td></td>
</tr>
<tr>
<td>Once each day</td>
<td>64</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Primary SNSs usage</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>352</td>
<td>98.9</td>
</tr>
<tr>
<td>Google+</td>
<td>4</td>
<td>1.1</td>
</tr>
</tbody>
</table>

4.2 Data analysis

The proposed model and hypotheses were empirically validated utilizing partial least square (PLS), supported by SmartPLS 2.0 M3 software (Ringle, Wende, & Will, 2005). PLS was chosen because of the collected data being non-normal, whilst PLS makes no distributional assumptions (Hair, Hult, Ringle, & Sarstedt, 2013).

4.2.1 Measurement model

The measurement model in PLS is usually assessed according to three tests: reliability, convergent validity, and discriminant validity (Hair et al., 2013). Reliability can be evaluated via factor loading, Cronbach’s α, and composite reliability (CR) (Hair et al., 2013). In the present study, the factor loadings of all constructs (See Table 2) were above the threshold of 0.7 (Fornell & Larcker, 1981), indicating sufficient item reliability (see Table 2). Also the measure of Cronbach’s α and CR were higher than the recommended 0.7 thresholds, demonstrating sufficient reliability. For convergent validity, Fornell & Larcker (1981) suggested that the value of average variance extracted (AVE) of at least 0.5 reveals sufficient convergent validity. As per this criterion, the constructs used in this study demonstrated sufficient convergent validity (see Table 3). Furthermore, the inter-construct correlations matrix (see Table 4) exhibits that the square root of AVE for each construct was larger than the correlation of the specific construct with any other constructs in the model, thus indicating adequate discriminant validity (Fornell & Larcker, 1981).
Table 2 Item-to-construct loadings

<table>
<thead>
<tr>
<th>Item/Construct</th>
<th>Awareness</th>
<th>Control</th>
<th>Privacy concerns</th>
<th>Trust</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aw1</td>
<td>0.86</td>
<td>-0.70</td>
<td>0.39</td>
<td>-0.02</td>
<td>0.38</td>
</tr>
<tr>
<td>Aw2</td>
<td>0.91</td>
<td>-0.67</td>
<td>0.40</td>
<td>0.00</td>
<td>0.30</td>
</tr>
<tr>
<td>Aw3</td>
<td>0.87</td>
<td>-0.62</td>
<td>0.45</td>
<td>0.05</td>
<td>0.32</td>
</tr>
<tr>
<td>Co1</td>
<td>-0.54</td>
<td>0.76</td>
<td>-0.29</td>
<td>-0.13</td>
<td>-0.19</td>
</tr>
<tr>
<td>Co2</td>
<td>-0.65</td>
<td>0.85</td>
<td>-0.35</td>
<td>-0.03</td>
<td>-0.29</td>
</tr>
<tr>
<td>Co3</td>
<td>-0.67</td>
<td>0.88</td>
<td>-0.46</td>
<td>0.08</td>
<td>-0.36</td>
</tr>
<tr>
<td>Pc1</td>
<td>0.42</td>
<td>-0.41</td>
<td>0.81</td>
<td>-0.04</td>
<td>0.37</td>
</tr>
<tr>
<td>Pc2</td>
<td>0.39</td>
<td>-0.37</td>
<td>0.85</td>
<td>-0.07</td>
<td>0.43</td>
</tr>
<tr>
<td>Pc3</td>
<td>0.34</td>
<td>-0.33</td>
<td>0.83</td>
<td>-0.06</td>
<td>0.42</td>
</tr>
<tr>
<td>Pc4</td>
<td>0.44</td>
<td>-0.39</td>
<td>0.86</td>
<td>-0.05</td>
<td>0.43</td>
</tr>
<tr>
<td>Tr1</td>
<td>0.04</td>
<td>-0.01</td>
<td>-0.02</td>
<td>0.74</td>
<td>-0.10</td>
</tr>
<tr>
<td>Tr2</td>
<td>-0.08</td>
<td>0.03</td>
<td>-0.04</td>
<td>0.79</td>
<td>-0.14</td>
</tr>
<tr>
<td>Tr3</td>
<td>0.03</td>
<td>-0.04</td>
<td>-0.05</td>
<td>0.75</td>
<td>-0.06</td>
</tr>
<tr>
<td>Tr4</td>
<td>0.05</td>
<td>-0.03</td>
<td>-0.09</td>
<td>0.81</td>
<td>-0.13</td>
</tr>
<tr>
<td>Ri1</td>
<td>0.33</td>
<td>-0.33</td>
<td>0.42</td>
<td>-0.10</td>
<td>0.79</td>
</tr>
<tr>
<td>Ri2</td>
<td>0.18</td>
<td>-0.21</td>
<td>0.31</td>
<td>-0.12</td>
<td>0.79</td>
</tr>
<tr>
<td>Ri3</td>
<td>0.34</td>
<td>-0.31</td>
<td>0.43</td>
<td>-0.08</td>
<td>0.84</td>
</tr>
<tr>
<td>Ri4</td>
<td>0.36</td>
<td>-0.30</td>
<td>0.39</td>
<td>-0.11</td>
<td>0.81</td>
</tr>
<tr>
<td>Ri5</td>
<td>0.26</td>
<td>-0.22</td>
<td>0.40</td>
<td>-0.16</td>
<td>0.75</td>
</tr>
</tbody>
</table>
### Table 3. Reliability and validity

<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Factor loading</th>
<th>CR</th>
<th>Cronbach’s α</th>
<th>AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness (Malhotra et al., 2004)</td>
<td>SNSs seeking information should disclose the way the data are collected, processed, and used.</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A good user online privacy should have a clear and conspicuous disclosure.</td>
<td>0.91</td>
<td>0.91</td>
<td>0.85</td>
<td>0.77</td>
</tr>
<tr>
<td></td>
<td>It is very important to me that I am aware and knowledgeable about how my personal information will be used.</td>
<td>0.87</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control (Dinev &amp; Hart, 2004)</td>
<td>I would only submit accurate and personal information to SNSs if the site allowed me to control the information I volunteer.</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I would only provide accurate and personal information to SNSs if the site allowed me to control the information they use.</td>
<td>0.85</td>
<td>0.87</td>
<td>0.78</td>
<td>0.69</td>
</tr>
<tr>
<td></td>
<td>I would only provide accurate and personal information at SNSs if their control policy is verified / monitored by a reputable third party.</td>
<td>0.88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy concerns (Xu et al., 2011)</td>
<td>I am concerned that the information I submit to SNSs could be misused.</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am concerned that others can find private information about me from SNSs.</td>
<td>0.85</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am concerned about providing personal information to SNSs, because of what others might do with it.</td>
<td>0.83</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am concerned about providing personal information to SNSs, because it could be used in a way that I did not foresee.</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: CR: Composite reliability; AVE: Average variance extracted
Table 3. Reliability and validity (cont.)

<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Factor loading</th>
<th>CR</th>
<th>Cronbach’s α</th>
<th>AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust (Malhotra et al., 2004)</td>
<td>SNSs would tell the truth and fulfill promises related to (the information) provided by me.</td>
<td>0.74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I trust that SNSs would keep my best interests in mind when dealing with (the information).</td>
<td>0.79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNSs are in general predictable and consistent regarding the usage of (the information).</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNSs are always honest with users when it comes to using (the information) that I would provide.</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk (Malhotra et al., 2004)</td>
<td>In general, it would be risky to give personal information to SNSs.</td>
<td>0.79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There would be high potential for privacy loss associated with giving personal information to SNSs.</td>
<td>0.79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal information could be inappropriately used by SNSs.</td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Providing SNSs with my personal information would involve many unexpected problems.</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I would feel unsafe giving personal information to SNSs.</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: CR: Composite reliability; AVE: Average variance extracted
Table 4. Correlations between constructs

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Standard deviation</th>
<th>Awareness</th>
<th>Control</th>
<th>Privacy concerns</th>
<th>Trust</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>4.23</td>
<td>0.70</td>
<td>(0.88)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>1.86</td>
<td>0.66</td>
<td>-0.75</td>
<td>(0.83)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy concerns</td>
<td>4.20</td>
<td>0.69</td>
<td>0.47</td>
<td>-0.45</td>
<td>(0.84)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>3.28</td>
<td>0.77</td>
<td>0.01</td>
<td>-0.01</td>
<td>-0.07</td>
<td>(0.80)</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>3.94</td>
<td>0.66</td>
<td>0.38</td>
<td>-0.35</td>
<td>0.49</td>
<td>-0.14</td>
<td>(0.77)</td>
</tr>
</tbody>
</table>

Note: Diagonal elements within parentheses show the square root of average variance extracted (AVE).

4.2.2 Structural model

A bootstrapping procedure was used to test the statistical significance of each path coefficient. The structural model results are depicted in Figure 2. The structural model showed that four hypotheses were supported and one (H3) failed to support (see Table 5). Overall, the model explained about 26% of the determined variance in the risk perceptions. Further, the effects of three control variables (gender, age, and types of SNSs) were also tested, along with the hypotheses. The results indicated that only one control variable, types of SNSs, had a significant effect on risk perception. However, the results regarding the hypotheses remain unchanged.

Figure 2. Structural model results

Table 5. Hypothesis testing results

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>β</th>
<th>t-statistic</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Awareness→Privacy concerns</td>
<td>0.29</td>
<td>6.15***</td>
<td>Yes</td>
</tr>
<tr>
<td>H2: Control→Privacy concerns</td>
<td>-0.22</td>
<td>4.89***</td>
<td>Yes</td>
</tr>
<tr>
<td>H3: Privacy concerns→Trust</td>
<td>0.06</td>
<td>1.69</td>
<td>No</td>
</tr>
<tr>
<td>H4: Privacy concerns→Risk</td>
<td>0.49</td>
<td>16.94***</td>
<td>Yes</td>
</tr>
<tr>
<td>H5: Trust→Risk</td>
<td>-0.01</td>
<td>3.29**</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**: p<0.01, ***p<0.001

4.2.3 Common method bias

Since the study collected both independent and dependent variables simultaneously from the same respondent, common method bias might be a concern (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). First, the study randomized the items when surveying the samples, which may also reduce common method bias (Straub, Boudreau, & Genfen, 2004). Second,
the Harman’s single factor test was used to ensure that there was no significant method effect on the proposed relationships (Malhotra, Kim, & Patil, 2006). We use exploratory factor analysis and found that more than two factors can be extracted, the first factor explaining about 33% of variance. Third, we further adopted a marker-variable approach to detect common method bias proposed by Liang, Saraf, Hu, & Xue (2007). Most method factor loadings are not significant (except two items for measuring control and one for risk) and the ratio of substantive variance to method variance is roughly 85:1. With the insignificance and slight magnitude of method variance, the common method bias should not become a serious issue in this study.

5. Discussion and Implications

5.1 The effect of awareness on privacy concern

The results of hypothesis H1 supported the proposition that there exists a positive association between awareness and SNSs users’ information privacy concerns. That is, the more users may wish to understand about how SNSs handle their personal information, the more privacy they are ultimately concerned with.

The significant results of H1 might indicate that SNSs should provide effective means for creating users’ awareness throughout their privacy statements and related information practices. Extant literature suggests that most users are willing to share online profiles/information given that privacy issues are adequately addressed (Wang & Wu, 2014; Stutzman et al., 2011). Although SNSs provide privacy statements with which to inform their users, these statements are mainly focused on what information will be shared with other organizations, but it does not delineate who can assess such information (Timm & Duven, 2008). Further, privacy statements are notorious for their difficulty to read (Stutzman et al., 2011) and thus attract low usage and attention by customers (Milne & Culnan, 2004). Consequently, besides providing more explicit privacy statements that are easier to read for their users, SNS providers should present these statements in a more attractively to increase their acceptance and understanding.

5.2 The effect of control on privacy concern

With regards to H2, the results supported a negative relationship between the factor of control and SNS users’ privacy concerns. That is, the more users are able to exert control over their personal profiles, the less privacy concerns users will have aroused. The significant results of H2 might be used to imply that SNSs should offer effective means for users to have more control over their profiles in order to alleviate those users’ privacy concerns. In terms of Facebook, currently the default setting is that all friends of a user can see the entire profile but that a user can also restrict others from viewing that same profile. However, most users do not know how to use the privacy-protective settings that are provided (Acquisti & Gross, 2006). In other words, they do not alter the privacy controls to inhibit others from looking at their shared information because of a lack of knowledge or familiarity with the specified function.

Furthermore, one of the major concepts of adopting fair information practices (Federal Trade Commission, 2000) tends to be a provision of control provided to online users regarding the subsequent use of information (Sheehan & Hoy, 2000). Hence, besides authorizing users to control who can and cannot view their profiles, SNSs should also explicitly articulate how users’ information will be shared with other interested parties and, more importantly, to empower users to control whether or not the SNSs can share their information with those other parties if so desired. That is, users could protect themselves through the effective use of privacy control measures made implicitly available in SNSs. Further, another suggestion is that SNSs designers should create privacy controls that are easy to use and even permit users to have their own rules of information disclosure that may serve to prevent personal information from leaking to non-related, or malicious, entities and thus doing harm.

5.3 The effect of privacy concerns on trust

In testing hypothesis H3, the results failed to support the proposition. That is, it was determined that users’ privacy concerns do not have a significant effect on their trust in the use of SNSs. This result is quite surprising when taken on face value. Although previous literature demonstrates an association between privacy concerns and trust in e-commerce context (Culnan & Armstrong, 1999; Van Dyke et al., 2007), these results may not prove suitable within the context of SNSs. A plausible explanation is that despite SNSs providing evident privacy statements on their web sites, they only assure users that the site conforms to those lawful practices necessary to
safeguard users’ privacy, but that the disclosure does not ensure that the given organization is trustworthy (Bélanger, Hiller, & Smith, 2002). Prior literature (Friedman, Khan, & Howe, 2000) also suggests that building trust online requires fulfilling many characteristics. Hence, it can be construed that SNSs users may be left to think safeguarding privacy alone is not sufficiently adequate enough to trust SNSs; in lieu of this finding, they may anticipate other information practices to be in place such as security measures to increase their trust perceptions (Shin, 2010). In other words, the expressions of privacy found in statements made by the SNSs may not be useful to drive conclusions evincing trust in those SNSs. This finding is important to SNS service providers in that it suggests that a prominent online display of privacy statements is regarded as important, but when taken alone, these statements do not ensure high trust perceptions among potential and actual users. In fact, it has been indicated that SNSs such as Facebook can not necessarily be trusted by users (Dwyer, 2011) since only 4% of overall users have expressed no reservations to trusting Facebook completely (Acquisti & Gross, 2006).

5.4 The effect of privacy concerns on risk

The results of hypothesis H4 supported the proposition that there is a positive relationship existing between SNSs users’ privacy concerns and their risk perceptions. That is, the greater a sense of privacy concern users of the SNS have, the sharper the increase in the risks they will eventually perceive. Accordingly, users may demonstrate protective attitudes such as sharing minimal personal information, restricting others to access their profiles, or even providing intentionally fabricated information, which will certainly influence the vibrancy and vitality of the SNSs.

Undoubtedly, users’ privacy concerns are surely important enablers for both their risk perceptions and their reactions to SNS’s mal-information practices. Previous literature (Malhotra et al., 2004) argues that perceived risk is important to an individual’s decision of whether or not to use online services. Even unintentional privacy violations by organizations may effectively increase consumers’ risk perceptions (Van Slyke et al., 2006). In general, users with SNS profiles have higher risk-taking attitudes and are thus more comfortable with the potential risks associated with sharing information on the Internet (Fogel & Nehmad, 2009). However, there is still a requirement for SNSs to take effective measures deemed necessary to reduce users’ risk perceptions. The first step is to reduce SNS users’ overall privacy concerns in real terms. This study suggests that SNSs may encourage users to recommend their adoptive privacy protection behaviors since online users are easily influenced by others’ online recommendations (Hsiao, Lin, Wang, Lu, & Yu, 2010). Further, the study also suggests that SNSs should clearly explain that any agreement to share personal information may induce some potential risks before the creation of a new personal profile. Likewise, the limitations of usage may not be entirely within the control framed by the user who provided the information initially.

5.5 The effect of trust on risk

In testing hypothesis H5, the results revealed a negative relationship between trust and users’ risk perceptions. That is, pre-existing levels of trust in SNSs can significantly diminish users’ risk perceptions. Thus, how to increase users’ trust in the handling of their information by SNSs is undoubtedly an imperative. Prior literature suggests various ways to build online trust, including improving brand images (Friedman et al., 2000; Hsiao et al., 2010) or adopting programs or procedures with trusted third parties (Shin, 2010). Since the trust relationship between users and SNSs may be a key to obtaining future market share and commercial success, building a higher trust relationship between users and services is one important task that SNSs must fully acknowledge in their own self-interest. Hence, it is suggested that the SNSs should endeavor to promote privacy-related activities, such as training or education which go beyond basic postings of disclosure statements, in order to improve their public images. Further, new methodologies and mechanisms for establishing trust should be employed. When users become more trusting in the SNSs efforts to secure users’ privacy, users’ risk perceptions will be mitigated as well.

5.6 Theoretical and managerial implications

Our study contributes to the theory related to SNS privacy by integrating APCO model and SCT. The contribution lies in its combination of theories from information systems and sociology. By using an interdisciplinary lens, it is helpful for researchers to obtain a better understanding of the relationships among awareness, control, privacy concerns, trust, and risk. Further, we consider awareness and control
as antecedents of, but not components of, privacy concerns, and the results demonstrate the relationships truly exist. This finding may shed some light on the necessity of differing definitions of privacy concerns according to differing contexts. Also the relationship between privacy concerns and trust is not supported which may indicate that trust is more context-specific, such that SNS users trust certain individual SNS service provider but not others. Meanwhile, the present study also confirms that privacy concerns and trust jointly influence SNS users’ risk perceptions. Future studies can include extra factors that are contrary to, but nevertheless influential on, users’ privacy concerns thus further advancing the knowledge on the formulation of privacy concerns throughout.

Finally, this study assumes trust as an antecedent of risk variable according to prior literature (Jarvenpaa & Tractinsky, 1999; Malhotra et al., 2004) and empirically validates the relationship. The results demonstrate that trust predicts risk in SNS context which proves the importance of the relationship between trust and risk.

In addition to implications for theory, SNS service providers can also draw practical implications from this study. The study proposes that awareness and control as antecedents of privacy concerns truly exist. The finding may further imply that fair information practices (Federal Trade Commission, 2000) continue to play a role in influencing users’ privacy concerns. SNS service providers should pay more attention to this issue to stem very erosion of their user base. Since privacy concerns may seriously hinder SNSs from proliferating, or even surviving intact, SNS service providers could try to integrate these two all-important principles into the design of the SNS in order to reduce users’ ongoing privacy concerns. More importantly, SNS service providers must ensure that users are able to fully understand and then to know how to use the privacy-protective features pro-offered.

Further, extant risk perceptions are the results of a combination of privacy concerns and trust factors as confirmed in the study. The results might indicate that SNS service providers should be more cautious since SNS users have increasing risk perceptions leading to higher privacy concerns even if they still voluntarily choose to share their personal information. More importantly, the stronger the relationship between privacy concerns and risk perceptions is, the greater the suggestion is that users’ privacy concerns remain important to SNSs usage levels. Thus, the SNS service provider should propose more effective means to reduce users’ privacy concerns. Further, the SNS service providers should engage in the trust-building process more enthusiastically since trust can mitigate users’ risk perceptions and increase usage.

5.7 Control variables

Of the three control variables, only types of SNSs significantly and negatively influence risk perception. In our study, it might be construed that Facebook users perceive less risk than other SNS users. The exact relationships of types of SNSs with other variables remain interesting issues open to future study.

6. Conclusions and limitations

The purposes of this study are to propose a model in order to investigate the impact of awareness and control on SNS users’ privacy concerns and then to understand how such privacy concerns and shared notions of trust shape risk perceptions. One important finding of this study is that SNS users regard that to be aware of and to have direct control over personal information disclosed in the SNS may relate to their information privacy concerns in both a positive and negative direction, respectively. Further, privacy concerns and trust collectively influence user’s perceived risk notions towards SNSs. However, the influence of privacy concerns on trust is not supportable.

Several common limitations may exist in this study. First, the sample is drawn from only one single university and not from a more representative sampling. Consequently, inferences to the larger population cannot be safely made. Further, the survey conducted in this study was based on self-report rather than observation and the recording of behavioral patterns in participants’ social profiles. Further, we have only considered the first and the second party of the expanded privacy model proposed by Conger, Pratt, & Loch (2013, p. 405). Future research could further cover the third and even the fourth party when studying privacy issues in a social networking context. Meanwhile, it is more interesting to study actual behavior as the dependent variable in privacy studies. Hence, future study may
try to capture this issue and may also consider the influence of the privacy-paradox phenomenon.

7. Contributions

The results of this study add to the literature in several ways. While adding to the current state-of-the-art knowledge on the influence of awareness and control on privacy concerns, the results are also helpful to understand the extent of users’ risk perceptions of SNSs in terms of their privacy concerns and trust. First, this study lends support to the notion that by empowering self-control to SNS users and revealing more transparency over what is happening regarding their personal information can help protecting the privacy of SNS users (Weiss, 2009). Second, the results of this study illuminate implications for the improvement of SNS service providers throughout the industry to meet customer expectations. Specifically, user provided information is the most resource for SNS to improve their services and also respond to competition in the dynamic marketplace. Finally, the study also sheds lights on privacy issues relating to SNS which are less explored. More investigations may be required to obtain a better understanding on privacy issues regarding SNSs.

Acknowledgement:

This research and paper were supported by National Science Council (Grant No. NSC-102-2410-H-214-019) and I-Shou University (Grant No. ISU102-S-01), Taiwan (R.O.C.).

References