Computers in Human Behavior 80 (2018) 143–157

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

Information privacy, consumer alienation, and lurking behavior in social networking sites☆

Jaime Ortiz [a], Wen-Hai Chih [b, *], Faa-Shyan Tsai [c]

[a] Vice Provost, Global Strategies and Studies, University of Houston, E.W. Cullen Bldg. Suite 101, 4302 University Dr., Houston, TX 77204-2039, United States
[b] Professor, Department of Business Administration, National Dong Hwa University, No. 1, Sec. 2, Da Hsueh Rd., Shoufent, Hualien 97401, Taiwan, ROC
[c] Customer Feedback Manager, Department of Product Management, QNAP System, Inc., No. 22, Zhongxing Road, Xizhi District, New Taipei City, 221, Taiwan, ROC

ARTICLE INFO

Article history:
Received 19 June 2017
Received in revised form
14 September 2017
Accepted 5 November 2017
Available online 5 November 2017

Keywords:
Information security awareness
Concern for information privacy
Consumer alienation
Privacy risk belief
Lurking
Self-concealment

ABSTRACT

This study investigates the relationships among information security awareness, concern for information privacy, consumer alienation, privacy risk belief, lurking, and self-concealment. It explores the mediation effects of concern for information privacy/consumer alienation between information security awareness and privacy risk belief as well as the mediation effect of lurking between privacy risk belief and self-concealment. The results confirm that information security awareness has significant and positive effects on concern for information privacy, consumer alienation, and privacy risk belief. Concerns for information privacy and consumer alienation have significant and positive effects on privacy risk belief. Privacy risk belief has a significant and positive effect on lurking and self-concealment. Lurking has a significant and positive effect on self-concealment. Concerns for information privacy and consumer alienation are mediators between information security awareness and privacy risk belief. In addition, perceived privacy empowerment is a moderator between privacy risk belief and lurking as well as between privacy risk belief and self-concealment.

1. Introduction

People enjoy the growing prevalence of social networking sites' (SNSs') communities along with their rapid popularity. SNSs not only provide an open fora for discussion but they also allow users to easily and swiftly expressing their thoughts, views, ideas, or sharing knowledge with others (Pi, Chou, & Liao, 2013). InsightXplorer (2015) indicated that SNSs are popular among Taiwanese to engage in a social networking behavior. However, they remain concerned about information security problems behind the booming development of SNSs. There are more and more incidents regarding embezzled accounts and leaking of personal private information as SNSs expand. SNSs users gradually raise their information security awareness (ISA) because of networking crime reported by the media.

SNSs users express concerns about releasing personal private information which subsequently may generate apprehension for information privacy and risk beliefs of sharing information when they experience ISA (Malhotra, Kim, & Agarwal, 2004). Consumers get alienated and enhance their concern for information privacy (CFIP) with regard to powerless (inability to affect certain market practices) and normlessness (distrust of business and market practices) because of the *status quo* of perceived privacy empowerment supplied by SNS providers when they become aware of information privacy problems (Schwaig, Segars, Grover, & Fiedler, 2013). Higher general privacy concerns for online consumers are reflected by lower self-disclosure of personal information (Li, Sarathy, & Xu, 2011), which subsequently creates a lurking behavior and conceals personal private information in a SNS. SNSs users lose their confidence to get online and generate emotions that further reduce their intentions to disclose information. In turn, they gradually become lurkers because of the alienation induced by powerlessness (Ahn, Kwolek, & Bowman, 2015). Along these lines, privacy protection belief refers to a situation when consumers believe and expect that online vendors will keep their personal private information from hacking or unauthorized using (Li et al., 2011). The perceived privacy empowerment provided by SNSs

☆ **Article Classification:** Information Security, Social Media

* Corresponding author.
E-mail addresses: jortiz22@uh.edu (J. Ortiz), whchih@gms.ndhu.edu.tw (W.-H. Chih), shyan880005@gmail.com (F.-S. Tsai).

https://doi.org/10.1016/j.chb.2017.11.005
0747-5632/

vendors can increase users' trust and willingness of disclosure personal private information (Dyke, Midha, & Nemati, 2007). In fact, "privacy risk belief has a significant and negative impact on online consumers' behavioral intention to disclose their personal private information" (Li et al., 2011, p. 438). Users' attitudes of privacy influence their disclosure behaviors on Facebook (Stutzman, Capra, & Thompson, 2011). Hence, an individual with a privacy risk belief reduces her/his information disclosure which is the behavior of self-concealment and participates in SNSs through lurking.

Previous studies used ISA to find a relationship between users' attitudes and behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010). In their quest, they omitted the influence of ISA on CFIP, consumer alienation, and privacy risk belief. Hence, this study fills up these research gaps to redeem prior shortcomings.

As far as the consequences of privacy risk belief, past research investigated the influence of users' behavioral intentions mainly based on privacy calculus theory (Li et al., 2011). Stutzman et al. (2011) later confirmed the effect of privacy attitudes on disclosure. Users reduce their willingness to disclose information when they perceive risks. Self-concealment is just one of the two sides of disclosures and has rarely been examined in the context of the negative behavior caused by privacy risk belief including lurking and the concealment behavior of personal information. Lurking was mainly used to explain the behavior and the influence extent on CFIP generated from computer anxiety (Osatuyi, 2015) without treating lurking as the consequence. This study also fills up these two research gaps and investigates the effects of privacy risk belief on lurking and self-concealment.

Besides, previous studies only confirmed that negative privacy attitudes reduce the willingness to disclose information by an individual (Stutzman et al., 2011) instead of examining the transformation process regarding the effects of users' privacy attitudes on the reduction of disclosing personal information. Self-concealment is on the opposite side of self-disclosure. In other words, privacy risk belief increases an individual's willingness of self-concealment. Therefore, this study tackles this research gap and treats lurking as the mediation effect between privacy risk belief and self-concealment. In addition, prior research only confirmed the effects of privacy risk belief on negative behavior instead of investigating the detailed consequences of privacy risk belief. Thus, this study incorporates perceived privacy empowerment as the moderation effect to examine its influence on the relationships between privacy risk belief and lurking/self-concealment to fill up the research gap.

A key factor of the success and sustainability of SNS is user's attitude and behavior in the long-run. SNSs providers make continuous and repeated efforts to attract more users and supply effective information related to Internet advertisement and marketing in SNSs' communities (Kang & Shin, 2008). However, there are questions regarding the user's attitude and behavior about personal private information after the occurrence of privacy risk in SNSs. These questions are: i) Does ISA influence privacy risk belief through concern for information privacy or consumer alienation? ii) Does privacy risk belief influence lurking and self-concealment after the effects of concern for information privacy and consumer alienation? iii) Is perceived privacy empowerment a moderator between privacy risk belief and lurking/self-concealment?

There are three research objectives in this study. The first research objective is to investigate the effects of ISA on concern for information privacy and consumer alienation as well as the effects of ISA, concern for information privacy, and consumer alienation on privacy risk belief of SNSs users. The second research objective is to examine the relationships among privacy risk belief, lurking, and self-concealment to understand the self-protection procedure of lurking and self-concealment adopted by SNSs users with the influence of privacy risk belief. This research framework proposes two mediation effects to further investigate the relationships among constructs. Smith, Milberg, and Burke (1996) indicated that people show concern for information privacy about threats coming from the collection and unauthorized secondary use of personal private information by others. Individuals generate ISA and concern for information privacy to subjectively assess potential loss and expected risk (Li et al., 2011). Therefore, this study treats concern for information privacy as the mediator between ISA and privacy risk belief and tests such a mediation effect. In addition, SNSs users believe that they cannot change the *status quo* of SNSs and feel powerlessness and normlessness (Schwaig et al., 2013). The business ethics factor includes the collection of personal information without the consent of the customer in SNS environments. This study treats consumer alienation as the mediator between ISA and privacy risk belief and tests this mediation effect. The third research objective is to assume perceived privacy empowerment as the moderator between privacy risk belief and lurking/self-concealment and tests these moderators according to the privacy calculus theory which indicates an opposite relationship between privacy protection belief and privacy risk belief.

There are indeed studies around SNSs issues. However, there is no research on SNSs users' behaviors regarding privacy calculus framework from the perspectives of lurking and self-concealment. There are four contributions of this study related to the usage and behavior of SNSs users. The first contribution is about the effects of ISA on concern for information privacy, consumer alienation, and privacy risk belief. This study investigates the relationships among ISA, concern for information privacy, consumer alienation, and privacy risk belief to understand SNSs users behaviors. The second contribution is about the effects of privacy risk belief on lurking and self-concealment. Previous scholars have only discussed the negative effects of concern for information privacy and privacy risk belief on users' behavioral intentions which subsequently let them to discontinue their usage. This study investigates the final behavior of privacy risk belief such as lurking and self-concealment. The third contribution is about the mediation effects of concern for information privacy, consumer alienation, and lurking. It has been envisioned that SNSs users' behavior can be influenced. SNSs users assess whether continue to use or take a self-protection behavior when they perceive risks from SNSs. The fourth and fifth contributions are related to the moderator of perceived privacy empowerment. Perceived privacy empowerment can raise users' trust toward SNSs and increase their willingness to disclose personal information (Dyke et al., 2007). This study investigates the moderators of perceived privacy empowerment between privacy risk belief and lurking/self-concealment from the perspective of perceived privacy empowerment of users.

2. Literature review and hypotheses development

2.1. Theoretical foundation

Privacy protection belief refers to a situation when consumers believe and expect that online vendors will keep their personal private information from hacking or unauthorized using (Li et al., 2011). The perceived privacy empowerment provided by SNSs vendors can increase users' trust and willingness of disclosure personal private information (Dyke et al., 2007). In fact, "privacy risk belief has a significant and negative impact on online consumers' behavioral intention to disclose their personal private information" (Li et al., 2011, p. 438). Users' attitudes of privacy influence their disclosure behaviors on Facebook (Stutzman et al., 2011). Hence, an individual with a privacy risk belief reduces her/

his information disclosure which is the typical behavior of self-concealment and participates in SNSs through lurking.

It is worth to reflect on the issue of improving information security environment to raise users' continuity in SNSs. Large SNSs such as Facebook and Google often raise the security level of their users and improve their privacy protection as a response to their pressure for information security and account protection. SNSs provide data protection measures to satisfy users' requirements for information privacy (Berendt, Günther, & Spiekermann, 2005; Milne & Culnan, 2004). In spite of providing SNSs users the function of information protection and reminding them about the importance of information security issues to reduce their information security risks embedded in personal data, photos, or videos, SNSs users lack of an understanding about information security policy and the available set-up functions for information privacy (Berendt et al., 2005; Milne & Culnan, 2004). SNSs users generate concern for information privacy and worry about the disclosure of personal private information because they do not know how to set up protection procedures under the lack of ISA. In addition, SNSs users gradually feel powerless, generate alien psychology, and unconsciously reveal or ignore to protect their personal private information. The first motivation of this study is to investigate the relationships among ISA, concern for information privacy, and consumer alienation.

SNSs users express more concern about privacy issues related to personal private information abuse and accounts being hacked when they provide additional personal private information in SNSs (Whelan, 2005). Privacy risk belief influences the disclosure of personal information (Culnan & Bies, 2003; Dinev & Hart, 2006). SNSs users feel the concern for information privacy and the existence of risk beliefs when releasing personal information (Malhotra et al., 2004). The investigation of the effects of ISA, concern for information privacy and consumer alienation on privacy risk belief is the second motivation of this study.

Privacy risk belief negatively affects consumers' behavioral intention to disclose personal information (Li et al., 2011) to the extent of getting concerned about their privacy being disclosed in SNSs (Stutzman et al., 2011). These studies have only investigated the influence on users' self-disclosure behaviors after the generation of privacy risk belief. There has been no research on people's behavior of lurking and self-concealment. The third motivation of this study is then to explore the effects of privacy risk belief on lurking and self-concealment.

Privacy protection belief and privacy risk belief are two opposite constructs in the privacy calculus theory. Users generate privacy protection belief and reduce privacy risk belief when they subjectively think that SNSs providers have the capability of protecting their personal private information. Users modify their lurking behaviors depending on the perception of how their personal private information is protected. They are not easily influenced by others about their personal private information and generate privacy risk belief if SNSs vendors can provide secure mechanisms to assure their privacy. The investigation of the moderator for perceived privacy empowerment between privacy risk belief and lurking/self-concealment is the fourth motivation of this study.

2.2. Information security awareness

ISA refers to the degree of protection awareness users toward web vendors who set up security and protection mechanisms to assure users generating trusting beliefs and intentions (McKnight, Choudhury, & Kacmar, 2002). ISA is an important element of an effective information security management program (Cavusoglu, Cavusoglu, Son, & Benbasat, 2009). An individual or an institution faces extreme threat when there is a loss of effectiveness in their protection systems. The increase of an individual's ISA can effectively reduce the problem of system abuse or shortage of information security cognition. SNSs vendors provide various measures to ameliorate their users' information security performances (Albrechtsen & Hovden, 2010).

Bulgurcu et al. (2010, p. 532) defined ISA as "an employee's general knowledge about information security and her/his cognizance of the information security policies (ISP) of his organization". General information security awareness (GISA) and information security policy awareness (ISPA) are two dimensions of ISA. The definitions of general information security awareness and ISP awareness are "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications" and "an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements" (Bulgurcu et al., 2010, p. 532). von Solms (1999) considered that SNSs providers must set up an information security policy and formally announce it to their users. SNSs users must thoroughly read SNSs' relevant regulations to know their information security policies and become aware of their information privacy when they open an account in SNSs.

2.3. Concern for information privacy

Information privacy refers to the ability of individuals to control their personal information (Culnan & Bies, 2003; Stone, Gueutal, Gardner, & McClure, 1983). Concern for information privacy is a subjective opinion of justice within the scope of information privacy for an individual (Campbell, 1999). Privacy and Internet security are the major concerns for disclosing personal information in SNSs (Bryer & Chen, 2010).

Smith et al. (1996) proposed 15 measurement items for four operationalized dimensions of concern for information privacy. These dimensions are collection, unauthorized secondary use, improper access, and errors. Collection refers to the action of gathering personal data whether it is legal or not. An individual's main concern is whether SNSs providers collect and store her/his data appropriately or not. Unauthorized secondary use refers to individuals' concerns whether SNSs vendors gather their data for one purpose and inappropriately use such data for another purpose without their authorization. Improper access refers to other unauthorized people use an individual's personal information for different purposes and view this particular data without her/his authorization. Errors refer to an individual's concern whether SNSs providers can adequately protect her/his data without any accident or intentional errors (Slyke, Shim, Johnson, & Jiang, 2006).

The concept of people's privacy and concern comes from privacy social norms which "take into account how other people or friends influence the SNS user into keeping their information privacy" (Zlatolas, Welzer, Hericko, & Hölbl, 2015, p. 162). Altman (1977) proposed the concept of influence of culture on personal privacy. In the past, public opinion and norms were important ingredients to the concepts of privacy and value. Facebook users should use a variety of settings for privacy concern (Christofides, Muise, & Desmarais, 2009).

2.4. Consumer alienation

Consumer alienation involves a sense of segregation from the norms and values of the marketplace in terms of a business ethics factor. Alienated consumers feel powerlessness and normlessness regarding their information privacy (Schwaig et al., 2013). The marketplace is understood as all the institutions that offer goods or services and conduct related actions or performances (Johnson,

1996). Nowadays, there is consensus that alienated consumers do not intend to accept or identify themselves with current market institutions, practices, and outputs. Instead, they must get involved in these institutions to appropriately play the role as consumers (Mady, 2011; Pruden, Shuptrine, & Longman, 1974; Shuptrine, Pruden, & Longman, 1977). However, these consumers do not take their expected roles when they enter the marketplace to engage in a transaction. Consequently, they become more socially isolated (Mady, 2011). Seeman (1959) systematically identified five alternative meanings of alienation: powerlessness, meaninglessness, normlessness, isolation, and self-estrangement. Powerlessness refers to an individual's consciousness that her/his action cannot achieve the consequence which s/he pursues (Mady, 2011; Seeman, 1959). Powerlessness is a state in which consumers are unable to affect a business action to meet their requirements (Johnson, 1996). An alienated consumer considers that s/he cannot control any perspective encountered in the marketplace (Lambert, 1981). Meaninglessness refers to a state in which an individual is not sure about what s/he should believe in. The lack of a clear set of standards in the behavior of an individual buyer meets the phenomenon of meaninglessness where consumers feel that the transactions or products are not worth the effort (Mady, 2011; Pruden et al., 1974). On the other hand, normlessness is that social norms regulating behavior do not provide effective rules any more for individuals to follow (Mady, 2011) and marketers will conduct unethical, unjust, and undesirable ways to attain their selfish purposes (Johnson, 1996). Finally, isolation is a sense of estrangement or isolation from the marketplace which includes institutions, practices, and outputs of the market system (Johnson, 1996; Mady, 2011; Middleton, 1963; Seeman, 1959). Self-estrangement, as social isolation, refers to an individual who regards her/himself as an alien and more easily relates to others rather than to her/him (Mady, 2011) as well as the lack of ability to recognize her/his behavior and role as a consumer (Allison, 1978). This individual's consumption pattern is to satisfy others' expectations instead of herself/himself (Mady, 2011).

2.5. Privacy risk belief

Recently, people have paid more attention on Internet privacy issues. Companies such as Amazon, eBay, Facebook, and Google have severely suffered due to privacy-related problems. Consumers decide to disclose their personal information based on cost-benefit analysis established around the privacy calculus framework. Privacy risk belief is the potentially negative consequence within the privacy calculus framework. Consumers subjectively think about privacy risk belief as the expected loss to a specific online vendor by disclosing their personal information (Li et al., 2011). They are most concerned about the illegal abuse of personal private information. Owing to the perpetual property of SNSs, any issued information or uploaded document can be duplicated or edited by others. It is possible that personal private information gets stolen and utilized by others no matter how much time has passed. Overall, 88.2 percent of all respondents who are over 16 years old worry about their personal private information on Internet purchases (Cole, 2004). Therefore, people gradually pay more attention on the issue of privacy.

2.6. Lurking

The participation and contribution of SNSs members on community activities vary as time goes by. They adopt multiple roles when participating in a community during a different time period (Lave & Wenger, 1991; Wenger, 1998). A lurker refers to a SNS member who observes instead of actively participating in a SNS (Bishop, 2007; Dennen, 2008; Osatuyi, 2015). A lurker is "one of the 'silent majorities' in an electronic forum, one who posts occasionally or not at all but is known to read the group's postings regularly" (Sun, Rau, & Ma, 2014, p. 111). Lurkers are individuals who read other members' messages but never post any content (Neelen & Fetter, 2010) or post messages once in a while (Golder & Donath, 2004). A lurker is the one who does not publish or post a message for a certain period of time and does not make any contribution to the community (Nonnecke & Preece, 2001) as well as posts less than three messages from the beginning (Ganley, Moser, & Groenewegen, 2012).

Chen (2004) proposed three quantitative criteria for a lurker. First, a lurker logs weekly into the community to observe the activities in SNSs throughout a six week span. Second, her/his weekly frequency of postings is less than the online group average. Third, the ratio of her/his frequency of postings over the login frequency count is higher than the online group average. Regrettably, not many studies have investigated these criteria because the online community culture, topic, and size may exert effects on lurking behaviors. Posters send messages to online communities from time to time and make contributions to these communities. In contrast, lurkers never send messages to online communities, remain silent all the time, and read more postings than they create, edit, or write (Sun et al., 2014). Prior studies not only regarded a lurker as a free-rider but also portrayed a negative attitude toward her/him (Kollock & Smith, 1996; Morris & Ogan, 1996; Rheingold, 1993; Sun et al., 2014; Wellman & Gulia, 1999).

The reasons a lurker does not join a conversation in SNSs are highlighted by Nonnecke, Andrews, and Preece (2006). The majority of lurkers think that it is enough for them to just browse and read (Nonnecke et al., 2006). Lurkers think that they can satisfy their needs by just browsing messages. However, once lurkers feel distractions and do not satisfy the online information content, they leave the SNSs immediately (Mo & Coulson, 2010; Nonnecke et al., 2006). SNSs users are considered lurking and do not disclose their opinions and thoughts when they feel anxiety. It is then their best choices to join SNSs (Osatuyi, 2015).

2.7. Self-concealment

In psychology, an individual chooses to hide personal negative or depressed information, emotion, behavior, thought, or incident when s/he faces others. Self-concealment refers to the tendency of keeping certain distance away from others related to personal private information for individuals. These behaviors include providing negative comments in concealment, getting away from others, and being concerned about self-exposure (Larson & Chastain, 1990). Self-concealment indicates the internal maladaptive regulation process in various clinical phenomena (Masuda & Latzman, 2012). Self-concealment is not part of the fundamental personal characteristics of individuals. However, an individual chooses to hide personal private information when s/he faces a special situation. For instance, an individual worries about the risk of disseminating personal private information and provides false data when s/he fills it out (Cepeda-Benito & Short, 1998).

Moscovitch (2009) considered that an individual generates social community anxiety when s/he is afraid of being supervised and assessed by others in public for her/his behavior due to the disclosure of her/his weakness. The defects of self-attribute are anxiety, appearance, personality, and social skills. An individual generates response and behavior of bad adaptation such as concealing her/his personal private information and actual feeling because of disturbances in the communication of SNSs.

SNSs users generate negative emotions such as anxiety, avoidance, and frustration because of the service provided by the SNSs or during the process of establishing a relationship with others

(Bevan, Pfyl, & Barclay, 2012). An individual's behavior and decision are influenced by her/his emotion. Beaudry and Pinsonneault (2010) indicated that an individual modifies her/his behavior based on emotion and the situation to influence the usage for both smartphone users and SNSs users.

Stutzman et al. (2011) pointed out that individuals' attitudes toward privacy influence their disclosure practices in the SNSs. Self-disclosure refers to an individual who disseminates her/his personal information such as experiences, feelings, and personal thoughts for the purpose of sharing personal information in the interaction with others (Derlega, Metts, Petronio, & Margulis, 1993; Greene, Derlega, & Mathews, 2006; Wheeless & Grotz, 1976; Wheeless, 1978). On the contrary, self-concealment refers to an individual who conceals her/his personal information on purpose and does not disclose personal information or provide inaccurate information during an interpersonal interaction. People generate self-concealment to lower their self-disclosure behaviors if concern for information privacy is higher no matter if they conduct commercial transactions or simply share information and communicate emotions in SNSs. An individual with self-concealment avoids to struggle with the anxiety of self-disclosure (Larson & Chastain, 1990). Therefore, SNSs users choose self-concealment and reduce the amount and frequency of self-disclosure to minimize risk. Thus, they can avoid the trouble associated with self-disclosure when they generate privacy risk belief and subsequently generate concern for self-disclosure.

2.8. Perceived privacy empowerment

Perceived privacy empowerment refers to as how users perceive the degree of empowerment of controlling personal private information from the privacy mechanisms provided by SNSs vendors (Slyke et al., 2006). In other words, it is the degree of user's' perception about the protection of personal information privacy. Web merchants indicated that SNSs providers can increase consumers' trust if they reduce users' concerns for information privacy (Slyke et al., 2006).

2.9. Hypotheses development

Fishbein (2008) identified variables that may directly or indirectly affect the consequence of any action. Ajzen and Albarracin (2007) argued that an individual's background such as experience, demographics, knowledge, and disposition can influence her/his intention and behavior on the effects of appropriate antecedents. Therefore, this study infers that users' behaviors related to ISA facilitate information security further diminish the information privacy problem. SNSs users express stronger privacy concerns if they have higher privacy awareness (Boyd & Hargittai, 2010). For example, Zlatolas et al. (2015) indicated that students have become more aware of the privacy issues on Facebook based on the results of Boyd and Hargittai's study (2010). An organization offers security awareness to its employees as the most crucial element to convince them to modify their behaviors into compliance (Siponen, 2000). Lee and Larsen (2009) pointed out that executives of small- and medium-sized businesses generate additional concerns for information privacy when they have higher ISA to reduce the effect of threat appraisal on intention to adopt anti-malware software for their organizations based on the protection motivation theory. This study proposes the following hypothesis.

H1. SNSs members' information security awareness has a significant and positive effect on concern for information privacy.

Consumers generate alienation because they feel powerless and normless about the privacy protection practice provided by web vendors when they pay attention to personal private information and are aware of an information privacy problem (Schwaig et al., 2013). Alienated consumers embrace less consumption activities because they have no control over the scenario they face in the marketplace (Mady, 2011). Consumers generate alienation with normlessness to marketplace when there is ISA and feel that SNSs providers are not able to improve their information privacy problem. This study proposes the following hypothesis.

H2. SNSs members' information security awareness has a significant and positive effect on consumer alienation.

An individual's attitude toward conducting a certain action is related to her/his belief about behavior-related outcomes (Ajzen, 1991; Fishbein & Ajzen, 1975; Fishbein, 2007). It is common for SNSs users to reduce their perception level of privacy protection belief when they first browse or are unfamiliar with an online vendor with strong concern for information privacy or awareness of the existence of information security problem in disclosing their personal information (Li et al., 2011; Smith et al., 1996). This study proposes the following hypothesis.

H3. : SNSs members' information security awareness has a significant and positive effect on privacy risk belief.

Concern for information privacy is defined as an individual's subjective views of fairness and the concern about information privacy (Li et al., 2011; Malhotra et al., 2004). It reflects the individual's perception of information privacy belief for risk in the website environment (Li, 2014). SNSs user's privacy risk belief increases when s/he perceives unfriendly intention or behavior from others and anticipates the threat of personal privacy in SNSs environment. General privacy concern has a significant and positive effect on privacy risk belief (Buchanan, Paine, Joinson, & Reips, 2007; Dinev & Hart, 2006; Smith et al., 1996; Stewart & Segars, 2002). Owing to the conflict of internal emotion of privacy protection belief and privacy risk belief, a SNS user increases her/his perception of privacy risk belief when s/he has strong concern for information privacy (Li et al., 2011). This study proposes the following hypothesis.

H4. SNSs members' concern for information privacy has a significant and positive effect on privacy risk belief.

A SNS user gets alienated when s/he feels powerless and does not trust the transaction taking place at the SNSs market. S/he generates greater negative attitudes when s/he has a higher alienation and expresses higher concerns for her/his information privacy and usage experience (Schwaig et al., 2013). Consumer alienation has a positive effect on concern for information privacy which subsequently has a negative effect on attitude toward the information practice (Schwaig et al., 2013). In addition, Li et al. (2011) indicated that general privacy concern for disclosing personal private information has a significant and positive effect on privacy risk belief. Therefore, this study infers that consumer alienation has a significant and positive effect on privacy risk belief and proposes the following hypothesis.

H5. SNSs members' alienation has a significant and positive effect on privacy risk belief.

Privacy risk belief is the cost factor that governs user's information disclosure in the privacy calculus framework (Li et al., 2011). Risk beliefs have a negative effect on the intention to reveal personal private information in an online marketplace (Mesch, 2012; Zimmer, Arsal, Al-Marzouq, & Grover, 2010). Disclosure of personal private information through face-to-face interactions do not leave any record and others do not have the opportunity to keep

track the information shared which does not occur in an online environment. Therefore, people with a strong privacy risk belief tend to disclose their personal private information through face-to-face interactions (Chen & Marcus, 2012). A SNSs user reduces her/his information disclosure and becomes a lurker when s/he generates privacy risk belief. This study proposes the following hypothesis.

H6. SNSs members' privacy risk belief has a significant and positive effect on lurking.

SNSs users ignore the negative emotion of concern for information privacy and continue to use SNSs due to the influence of colleagues and others when they perceive the invasion of personal information privacy and subsequently generate privacy risk belief. Risk belief negatively affects SNSs users' intentions to disclose personal information (Mesch, 2012; Zimmer et al., 2010). SNSs users refrain from disclosing their personal information and become lurkers themselves when they generate privacy risk beliefs because of the influence of privacy. In fact, privacy risk belief has a negative effect on self-disclosure. Research on e-commerce confirmed that privacy risk belief has a significant and negative effect on disclosing personal private information to unfamiliar enterprises in e-commerce (Li et al., 2011).

Lurking and self-concealment are types of self-protection practices for SNSs users. They refuse to disclose personal private information to protect personal information security. A lurker chooses to conceal personal information and does not divulge actual personal private information based on self-protection principle. This study proposes the following hypotheses.

H7. SNSs members' privacy risk belief has a significant and positive effect on self-concealment.

H8. SNSs members' lurking has a significant and positive effect on self-concealment.

Privacy and network security are main barriers for SNSs users to disclose personal information (Bryer & Chen, 2010). SNSs providers can raise consumers' behavioral intention of disclosing their personal information if they increase their privacy protection beliefs based on the privacy calculus framework (Li et al., 2011). Consumers will continue to use SNSs if SNSs providers guarantee a safely perceived privacy empowerment under the influence of negative emotions such as concern for information privacy and privacy risk belief. This study proposes the following hypotheses.

H9. Perceived privacy empowerment has a significant moderation effect between privacy risk belief and lurking.

H10. Perceived privacy empowerment has a significant moderation effect between privacy risk belief and self-concealment.

3. Methodology

3.1. Questionnaire design, pre-test, and pilot study

This study uses prior constructs and validates them through a pre-test and three pilot tests. It also revises measurement items' wordings of constructs based on the feedback of Taiwanese SNSs users. This study invites two professors of management information systems and three active SNSs users to review the measurement items' wordings. Twelve independent rounds (3 people for each) of the pre-test with SNSs users are conducted. The measurement items' wordings were revised during the face-to-face interaction with SNSs users to make sure they embraced the SNSs context in Taiwan. Subsequently, this study conducts three pilot tests with different SNSs users to ensure the final questionnaire addresses the convergent validity, reliability analysis, and discriminant validity of the measurement items and constructs.

3.2. Sample and data collection

There are three parts in this framework. The first part includes information security awareness, concern for information privacy, consumer alienation, and privacy risk belief. The second part is the perspective of behavior which is the consequence of the effect of information privacy issue of SNSs users and includes lurking and self-concealment. The third part is the perceived privacy empowerment which acts as a moderator. Fig. 1 shows the research framework.

This study investigates users' attitudes and behaviors regarding the occurrence of privacy risk in SNSs. Hence, the target respondents are SNSs users. They respond to an online survey through mySurvey in http://www.mysurvey.tw in Taiwan. This study offers fifty 300 New Taiwan Dollars (NTD) and one hundred 100 NTD for a convenient store to raise their response rate. This online survey was conducted from December 9, 2016 to February 10, 2017. There were 489 valid samples out of 683 collected samples and the completion rate was 71.60%. Table 1 shows the respondent demographics. The demographic split is male (54.14%) vs. female (45.86%), 20–24 years old (73.46%), followed by under 19 years old (17.20%), with junior college/college degree (80.89%), followed by senior high school degree (11.04%), year experience of using Facebook for more than 4 years (51.38%), followed by 3–4 years (18.68%), daily hours on Facebook between 4 and 6 h (44.16%), followed by under 3 h (31.85%).

3.3. Measures

Information security awareness, concern for information privacy, consumer alienation, privacy risk belief, lurking, self-concealment, and perceived privacy empowerment are the seven constructs for this framework. This study applies a seven-point Likert scale anchored between 1 ("strongly disagree") and 7 ("strongly agree") to measure scale items for information security awareness, concern for information privacy, consumer alienation, and privacy risk belief. ISA is defined as a user's overall understanding of information security, the regulation of information policy, and the relevant knowledge related to potential problems and six measurement items are adapted from Bulgurcu et al. (2010). The definition of concern for information privacy is the degree of user's concern for information security and personal privacy and fourteen measurement items are adapted from Schwaig et al. (2013). Consumer alienation is defined as the degree of user's powerless regarding the SNSs' behaviors and mechanisms within the marketplace and twelve measurement items are adapted from Schwaig et al. (2013). The definition of privacy risk belief is the anticipation of the potential loss when a user provides her/his personal information and four measurement items are adapted from Li et al. (2011). The measurement items for lurking, self-concealment, and perceived privacy empowerment are measured by a five-point Likert scale anchored between 1 ("strongly disagree") and 5 ("strongly agree"). Lurking is defined as the degree by which a user only browses contents without disclosing personal private information in SNSs and four measurement items are adapted from Osatuyi (2015). The definition of self-concealment is a user's psychological tendency by concealing her/his inside negative or uneasy message toward others and ten measurement items are adapted from Larson and Chastain (1990). Perceived privacy empowerment is defined as a user's perception of a privacy protection mechanism provided by SNSs and four measurement

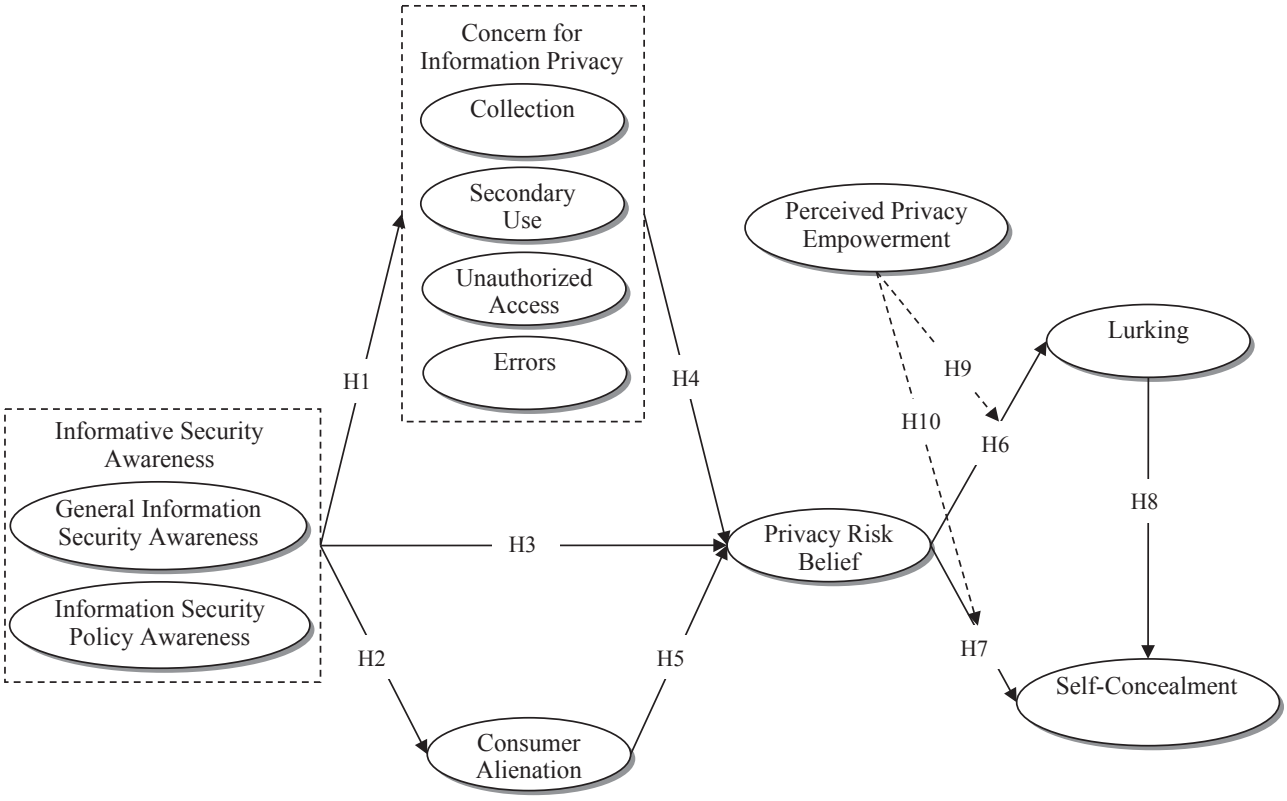

Fig. 1. Proposed model.

items are adapted from Dyke et al. (2007). Appendix shows all the constructs and measurement items.

4. Analysis and results

4.1. Common method variance

The problems of common method variance (CMV) are dealt through the adoption of prevention and post-detection procedures. As far as the prevention procedure, this study uses an anonymous questionnaire, random order for measurement items, various scales, and concealed constructs names to diminish SNSs users' concerns when they fill up the questionnaire (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). This study adopts Harman's one-factor test to detect the CMV according to previous findings (Harman, 1967) and applies the exploratory factor analysis (EFA) suggested by Podsakoff and Organ (1986) for a post-detection procedure. Table 2 indicates that nine factors can be extracted from the EFA and the first factor can explain 24.215% of the variance which is lower than 50%.

Table 1
Demographics of the respondents.

Demographics		Frequency	Percentage (%)	Accumulated Percentage (%)
Gender	Male	255	54.14	54.14
	Female	216	45.86	100.00
Age	Under 19 years old	81	17.20	17.20
	20-24 years old	346	73.46	90.66
	25-29 years old	12	2.55	93.21
	30-34 years old	12	2.55	95.76
	35-39 years old	4	0.84	96.60
	Over 40 years old	16	3.40	100.00
Education	Under Junior High School	1	0.21	0.21
	Senior High School	52	11.04	11.25
	Junior College/College	381	80.89	92.14
	Graduate	37	7.86	100.00
Year	Less than 1 year	37	7.86	7.86
Experience of Using Facebook	1-2 years	33	7.01	14.87
	Above 2–3 years	71	15.07	29.94
	Above 3–4 years	88	18.68	48.62
	Above 4 years	242	51.38	100.00
Daily Hours on Facebook	Under 3 h	150	31.85	31.85
	4-6 h	208	44.16	76.01
	7-9 h	79	16.77	92.78
	Above 10 h	34	7.22	100.00

Table 2
Initial eigenvalues.

Component	Eigenvalues	Variance (%)	Cumulative Variance (%)
1	11.139	24.215	24.215
2	4.963	10.790	35.004
3	4.038	8.778	43.782
4	2.691	5.850	49.632
5	1.813	3.941	53.573
6	1.693	3.681	57.254
7	1.318	2.864	60.119
8	1.267	2.755	62.874
9	1.172	2.549	65.423

This study also conducts the one factor analysis of confirmatory factor analysis (CFA) and incorporates all fifty measurement items except 4 reversed measurement items of seven constructs in one factor. Table 3 illustrate that not all of measurement items' factor loadings are larger than 0.50 (significant) and the model fit of one factor (Chi-quare = 9330.535, DF = 1175, χ^2/DF = 7.941, GFI = 0.414, AGFI = 0.364, IFI = 0.364, CFI = 0.361, RMSR = 0.137) is worse than the model fit of the proposed model (Chi-quare = 1881.926, DF = 975, χ^2/DF = 1.930, GFI = 0.846, AGFI = 0.829, IFI = 0.925, CFI = 0.925, RMSR = 0.062). Therefore, this study does not present a problem regarding CMV.

4.2. Measurement model

This study applies composite reliability (CR) and average variance extracted (AVE) to measure the convergent validity of measurement items and constructs through AMOS software with the maximum likelihood estimation (Hair Jr., Black, Babin, & Anderson, 2010). Table 4 shows that the CR values are all larger than 0.7 which validates the internal consistency for the measurement items of each construct (Hulland, 1999). All the AVE values are larger than 0.5 except lurking (0.440) and self-concealment (0.423). Nunnally (1978) proposed that a construct is reliable if the factor loadings of all measurement items are larger than 0.4 as well as the CR is larger than 0.6. Therefore, each construct has an appropriate convergent validity. Table 5 illustrates that all the correlations between any two constructs are larger than the square root of AVE of each construct to demonstrate the discriminant validity of this study (Fornell & Larcker, 1981).

This study uses squared multiple correlations (SMC) and Cronbach α (Bagozzi & Yi, 1988) to measure the internal consistency for reliability. It shows the reliability of each construct if all SMC values are larger than 0.2 (Bentler & Wu, 1993; Jöreskog & Sörbom, 1993) and the Cronbach α values are larger than 0.7 (Nunnally, 1978). The SMC values for each measurement are between 0.335 and 0.897 and the Cronbach α values fall between 0.752 and 0.901 which corroborates the internal consistency for each construct.

4.3. Structural model

The overall model fit (χ^2 = 1881.926, df = 975, $p < 0.001$, χ^2/df = 1.930, GFI = 0.846, TLI = 0.920, CFI = 0.925 and RMSEA = 0.044) is appropriate. Table 6 illustrates the results of the proposed hypotheses while Fig. 2 shows their path diagram. The proposed hypotheses are all supported. The results indicate that ISA has a significant and positive effect on concern for information privacy ($\gamma_{11} = 0.324$, $p < 0.001$), consumer alienation ($\gamma_{21} = 0.362$, $p < 0.001$), and privacy risk belief ($\gamma_{31} = 0.229$, $p < 0.001$), supporting H1, H2, and H3. In addition, concern for information privacy and consumer alienation have significant and positive effects on privacy risk belief ($\beta_{31} = 0.523$, $p < 0.001$; $\beta_{32} = 0.156$, $p < 0.001$),

Table 3
Common method variance.

	Factor Loadings
General Information Security Awareness	
GISA 1	0.468
GISA 2	0.452
GISA 3	0.468
Information Security Policy Awareness	
ISPA 1	0.279
ISPA 2	0.291
ISPA 3	0.363
Collection	
COL 1	0.521
COL 2	0.597
COL 3	0.522
COL 4	0.556
Secondary Use	
SU 1	0.632
SU 2	0.673
SU 3	0.657
SU 4	0.696
Unauthorized Access	
UA 1	0.633
UA 2	0.694
UA 3	0.652
Errors	
ERR 1	0.564
ERR 2	0.588
ERR 3	0.541
Consumer Alienation	
CA 1	0.236
CA 2	0.280
CA 3	0.271
CA 4	0.266
CA 5	0.335
CA 6	0.291
CA 7	0.362
CA 8	–
CA 9	–
CA 10	0.279
CA 11	–
CA 12	–
Privacy Risk Belief	
PRB 1	0.665
PRB 2	0.713
PRB 3	0.673
PRB 4	0.689
Lurking	
LK 1	0.250
LK 2	0.266
LK 3	0.374
LK 4	0.304
Self-Concealment	
SC 1	0.407
SC 2	0.298
SC 3	0.338
SC 4	0.276
SC 5	0.261
SC 6	0.390
SC 7	0.295
SC 8	0.351
SC 9	0.462
SC 10	0.282
Perceived Privacy Empowerment	
PPEM 1	0.137
PPEM 2	0.147
PPEM 3	0.193
PPEM 4	0.267

Note: GISA: General Information Security Awareness; ISPA: Information Security Policy Awareness; COL: Collection; SU: Secondary Use; UA: Unauthorized Access; ERR: Errors; CA: Consumer Alienation; PRB: Privacy Risk Belief; LK: Lurking; SC: Self-Concealment; PPEM: Perceived Privacy Empowerment.

Table 4
Analysis of measurement model.

Constructs	MLE Estimates		Squared Multiple Correlation (SMC)	Composite Reliability (CR)	Average of Variance Extracted (AVE)
	Factor Loading (λ_x/λ_y)	Measurement Error (δ/ε)			
General Information Security Awareness				0.879	0.708
GISA1	0.773***	0.402	0.598		
GISA 2	0.903***	0.185	0.815		
GISA 3	0.843***	0.289	0.711		
Information Security Policy Awareness				0.899	0.751
ISPA 1	0.913***	0.166	0.834		
ISPA 2	0.947***	0.103	0.897		
ISPA 3	0.722***	0.479	0.521		
Collection				0.857	0.600
COL 1	0.756***	0.428	0.572		
COL 2	0.842***	0.291	0.709		
COL 3	0.769***	0.409	0.591		
COL 4	0.726***	0.473	0.527		
Secondary Use				0.902	0.698
SU 1	0.771***	0.406	0.594		
SU 2	0.860***	0.260	0.740		
SU 3	0.865***	0.252	0.748		
SU 4	0.843***	0.289	0.711		
Unauthorized Access				0.893	0.735
UA 1	0.837***	0.299	0.701		
UA 2	0.869***	0.245	0.755		
UA 3	0.865***	0.252	0.748		
Errors				0.840	0.638
ERR 1	0.772***	0.404	0.596		
ERR 2	0.866***	0.250	0.750		
ERR 3	0.753***	0.433	0.567		
Consumer Alienation				0.888	0.502
CA 1	0.787***	0.381	0.619		
CA 2	0.834***	0.304	0.696		
CA 3	0.782***	0.388	0.612		
CA 4	0.707***	0.500	0.500		
CA 5	0.652***	0.575	0.425		
CA 6	0.629***	0.604	0.396		
CA 7	0.615***	0.622	0.378		
CA 8	–	–	–		
CA 9	–	–	–		
CA10	0.622***	0.613	0.387		
CA 11	–	–	–		
CA 12	–	–	–		
Privacy Risk Belief				0.901	0.696
PRB 1	0.841***	0.293	0.707		
PRB 2	0.898***	0.194	0.806		
PRB 3	0.797***	0.365	0.635		
PRB 4	0.796***	0.366	0.634		
Lurking				0.758	0.440
LK 1	0.610***	0.628	0.372		
LK 2	0.663***	0.560	0.440		
LK 3	0.734***	0.461	0.539		
LK 4	0.639***	0.592	0.408		
Self-Concealment				0.879	0.423
SC 1	0.761***	0.421	0.579		
SC 2	0.579***	0.665	0.335		
SC 3	0.608***	0.630	0.370		
SC 4	0.639***	0.592	0.408		
SC 5	0.611***	0.627	0.373		
SC 6	0.669***	0.552	0.448		
SC 7	0.663***	0.560	0.440		
SC 8	0.625***	0.609	0.391		
SC 9	0.689***	0.525	0.475		
SC 10	0.638***	0.593	0.407		
$\chi^2 = 1965.112$, df = 944, $p < 0.001$, $\chi^2/df = 2.082$, GFI = 0.842, RMSEA = 0.048, TLI = 0.915, CFI = 0.922					

Note: GISA: General Information Security Awareness; ISPA: Information Security Policy Awareness; COL: Collection; SU: Secondary Use; UA: Unauthorized Access; ERR: Errors; CA: Consumer Alienation; PRB: Privacy Risk Belief; LK: Lurking; SC: Self-Concealment.
-: Reversed measurement item.
***: All factor loading are significant at the $p < 0.001$ level.

supporting H4 and H5. Privacy risk belief has a significant and positive effect on lurking and self-concealment ($\beta_{43} = 0.326$, $p < 0.001$; $\beta_{53} = 0.263$, $p < 0.001$), supporting H6 and H7. Lurking has a significant and positive effect on self-concealment ($\beta_{54} = 0.648$, $p < 0.001$).

Table 5
Correlation matrix for measurement scales.

Constructs	AVE	Alpha	GISA	ISPA	CA	COL	SU	UA	ERR	PRB	LK	SC
GISA	0.708	0.875	0.841									
ISPA	0.751	0.893	0.474**	0.867								
CA	0.600	0.890	0.353**	0.197**	0.775							
COL	0.698	0.856	0.258**	0.150**	0.190**	0.835						
SU	0.735	0.901	0.244**	0.132**	0.106*	0.563**	0.857					
UA	0.638	0.890	0.246**	0.133**	0.096*	0.469**	0.758**	0.799				
ERR	0.502	0.835	0.297**	0.259**	0.208**	0.364**	0.468**	0.577**	0.709			
PRB	0.696	0.900	0.432**	0.220**	0.301**	0.478**	0.492**	0.485**	0.406**	0.834		
LK	0.440	0.752	0.170**	0.239**	0.178**	0.206**	0.143**	0.092*	0.239**	0.258**	0.663	
SC	0.423	0.799	0.229**	0.171**	0.217**	0.194**	0.200**	0.151**	0.283**	0.396**	0.582**	0.650

Note: GISA: General Information Security Awareness; ISPA: Information Security Policy Awareness; COL: Collection; SU: Secondary Use; UA: Unauthorized Access; ERR: Errors; CA: Consumer Alienation; PRB: Privacy Risk Belief; LK: Lurking; SC: Self-Concealment.
Diagonal elements are the square root of the average variance extracted of each construct; Pearson correlations are shown below the diagonal.
*: $p< 0.05$, **: $p < 0.01$.

Table 6
Results of proposed model.

Paths				Path Coefficients	Hypotheses	Test Results
γ_{11}	Information Security Awareness	→	Concern for Information Privacy	0.324***	H1	Supported
γ_{21}	Information Security Policy Awareness	→	Consumer Alienation	0.362***	H2	Supported
γ_{31}	Information Security Policy Awareness	→	Privacy Risk Belief	0.229***	H3	Supported
β_{31}	Concern for Information Privacy	→	Privacy Risk Belief	0.523***	H4	Supported
β_{32}	Consumer Alienation	→	Privacy Risk Belief	0.156***	H5	Supported
β_{43}	Privacy Risk Belief	→	Lurking	0.326***	H6	Supported
β_{53}	Privacy Risk Belief	→	Self-Concealment	0.263***	H7	Supported
β_{54}	Lurking	→	Self-Concealment	0.648***	H8	Supported

Note: ***: $p < 0.001$.

4.4. Moderation effect

This study validates the moderation effect of perceived privacy empowerment between privacy risk belief and lurking as well as between privacy risk belief and self-concealment through a multi-group causal analysis and separates samples into two subgroups based on the mean (3.86) of their perceived privacy empowerment. The numbers of samples for the high and low group of perceived privacy empowerment are 236 and 235, respectively. The set up for the high and low groups of perceived privacy empowerment are the constrained and the unconstrained models for the original samples without segregating them and later testing the moderation effect through the differences of chi-square values ($\triangle\chi^2$) between the constrained model and the unconstrained model as well as the p-value. Table 7 shows the result of the moderation effect for perceived privacy empowerment between privacy risk belief and lurking as well as the differences of chi-square values ($\triangle\chi^2$) between the constrained and the unconstrained model is 4.198 ($p < 0.001$) which confirms a significant difference between the high and low group of perceived privacy empowerment.

Table 8 illustrates the result of the moderation effect for perceived privacy empowerment between privacy risk belief and self-concealment as well as the differences in chi-square values ($\triangle\chi^2$) between the constrained and the unconstrained model is 8.568 ($p < 0.001$) which also underscores a significant difference between the high and low group of perceived privacy empowerment.

As far as the relationship between privacy risk belief and lurking, the standardized path coefficient for the high perceived privacy empowerment group is 0.275 ($p < 0.001$) whereas the standardized

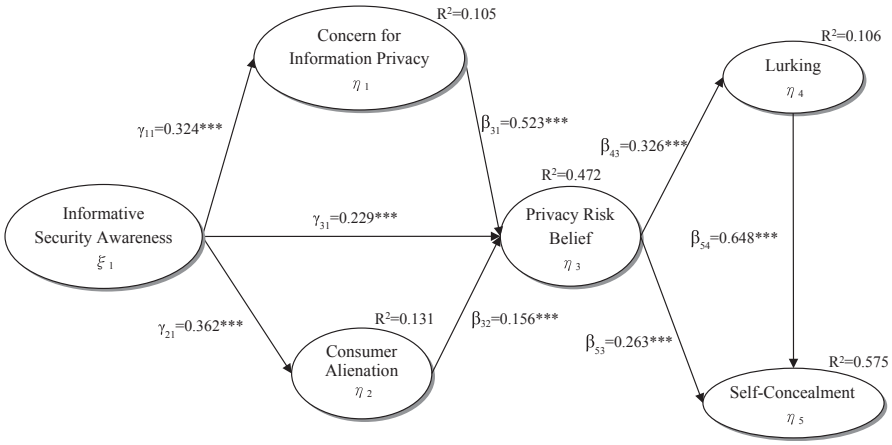

Fig. 2. Hypothesized model.

Table 7
The moderation effect of PPEM between PRB and LK.

	Structural Model	Unconstrained Model	$\triangle\chi^2$	*p*-value
χ^2 (DF)	130.886 (45)	126.688 (38)	4.198	0.000
GFI	0.935	0.937		
AGFI	0.896	0.881		
RMSEA	0.064	0.071		
			PPEM	
			High	Low
PRB→LK			0.275***	0.309***

Note: PRB: Privacy Risk Belief; LK: Lurking; PPEM: Perceived Privacy Empowerment.
***: $p < 0.001$.

path coefficient for the low perceived privacy empowerment group is 0.309 ($p < 0.001$). Though the standardized path coefficients between privacy risk belief and lurking are significant and positive for both groups, the value for the high perceived privacy empowerment group is smaller than the value for the low perceived privacy empowerment group. It demonstrates that privacy risk belief causes lower lurking for a SNSs user if s/he has a higher perceived privacy empowerment. Therefore, H9 is supported.

For the relationship between privacy risk belief and self-concealment, the standardized path coefficient for the high perceived privacy empowerment group is 0.431 ($p < 0.001$) whereas the standardized path coefficient for the low perceived privacy empowerment group is 0.413 ($p < 0.001$). Though the standardized path coefficients between privacy risk belief and self-concealment are significant and positive for both groups, the value of high perceived privacy empowerment group is larger than the value of low perceived privacy empowerment group. It indicates that privacy risk belief causes higher self-concealment for a SNSs user if s/he has a higher perceived privacy empowerment. Therefore, H10 is supported.

4.5. Mediation effect

This study measures mediation effects based on the results of a structural model. There are three mediation effects in this framework. (1) The mediation effect of concern for information privacy between ISA and privacy risk belief. (2) The mediation effect of consumer alienation between ISA and privacy risk belief. (3) The mediation effect of lurking between privacy risk belief and self-concealment. Table 9 shows that the values of the Sobel test are all larger than 1.96 (Sobel, 1982) and that all 95% confidence intervals of the Bootstrapping analysis for the 5000 simulations do not include 0 (Efron & Tibshirani, 1993) which implies that all three mediation effects are significant. Table 10 illustrates that all three mediation effects are partial mediators.

Table 8
The moderation effect of PPEM between PRB and SC.

	Structural Model	Unconstrained Model	$\triangle\chi^2$	*p*-value
χ^2 (DF)	234.763 (165)	226.195 (152)	8.568	0.000
GFI	0.932	0.935		
AGFI	0.914	0.910		
RMSEA	0.030	0.032		
			PPEM	
			High	Low
PRB→SC			0.431***	0.413***

Note: PRB: Privacy Risk Belief; SC: Self-Concealment; PPEM: Perceived Privacy Empowerment.
***: $p < 0.001$.

Table 9
Sobel test and bootstrapping confidence interval of mediator effects.

IV	M	DV	Sobel Test	Bootstrapping 95% Confidence Intervals			
				Percentile CI		Biased-method CI	
				Lower	Upper	Lower	Upper
ISA	CFIP	PRB	4.823***	0.0923	0.2245	0.0946	0.2294
ISA	CA	PRB	3.886***	0.0317	0.1080	0.0327	0.1114
PRB	LK	SC	4.948***	0.0480	0.1274	0.0464	0.1249

Note: IV: Independent Variable; M: Mediator Variable; DV: Dependent Variable; ISA: Information Security Awareness; CFIP: Concern for Information Privacy; CA: Consumer Alienation; PRB: Privacy Risk Belief; LK: Lurking; SC: Self-Concealment.
***: $p < 0.001$.

5. Conclusions

5.1. Key findings and contributions

SNSs users are more concerned about their personal information security when they have a stronger ISA. As the concept of privacy has evolved, SNSs users now pay more attention to their privacy issues. Most SNSs users are concerned about their personal private information and worry about their loss regarding privacy. Thus, they demand privacy protection (Boyle & Johnson, 2010).

SNSs users are aware of the problems of information privacy and there is nothing they can do about it. This subsequently generates alienation as they do not expect that SNSs would provide them with a secure environment when they have higher ISA (Mady, 2011; Schwaig et al., 2013). SNSs users produce a more negative attitude toward information privacy when they have higher alienation (Schwaig et al., 2013). The empirical results support the findings of Lee and Larsen (2009) in terms of the significant and positive effect of ISA on privacy risk belief. SNSs users protect themselves through threat appraisal and generate a strong risk belief regarding privacy when they have high sense of ISA.

Prior research underscored the reasons that prevent lurkers of having an active participation in the discussion of SNSs. Lurkers think that their needs consist of just browsing others' discussions in SNSs (Nonnecke et al., 2006). In addition, bad experiences in the usage of SNSs affect users becoming lurkers and reducing their self-disclosure (Osatuyi, 2015). Trust is the main factor of triggering behavior (Nonaka, Toyama, & Konno, 2000). Only members who trust each other can trigger their sharing for implicit information. A SNS user generates privacy risk belief and does not trust SNSs that induce her/him to become a lurker and not sharing personal information and self-concealment for personal information.

The protection of users' personal private information from SNSs providers affects users' degree of trust to SNSs. The operational complexity of SNSs and the website layout influence users' perceive risk (Metzger, 2004). The coefficient between privacy risk belief and lurking for a highly perceived privacy empowerment group is lower than of the low perceived privacy empowerment one. The effect of privacy risk belief on lurking is lower when SNSs users have a higher perceived privacy empowerment. Privacy empowerment provided by SNSs can reduce the possibility of a user with privacy risk belief becoming a lurker. This result supports previous findings which illustrate that SNSs increase consumers' trust if they can reduce users' concerns for information privacy (Slyke et al., 2006). Fodor and Brem (2015) also corroborated that trust has a significant and positive effect on usage intention. Users will have usage intention if SNSs providers can increase their trust.

SNSs users are concerned about their information privacy when they have ISA. SNSs users gradually generate alienation when they realize that they cannot change the *status quo* of the market. SNSs users are afraid of leaking personal private information when they

Table 10
Stepwise regression for mediator effects of threat appraisal and source credibility.

IV	M	DV	IV → DV		IV → M		IV + M→ DV			
							IV		M	
			β	S.E.	β	S.E.	β	S.E.	β.	S.E.
ISA	CFIP	PRB	0.369***	0.043	0.239***	0.035	0.216***	0.038	0.641***	0.048
ISA	CA	PRB	0.369***	0.043	0.318***	0.044	0.305***	0.044	0.201***	0.043
PRB	LK	SC	0.259***	0.028	0.180***	0.031	0.172***	0.024	0.480***	0.035

Note: IV: Independent Variable; M: Mediator Variable; DV: Dependent Variable; ISA: Information Security Awareness; CFIP: Concern for Information Privacy; CA: Consumer Alienation; PRB: Privacy Risk Belief; LK: Lurking; SC: Self-Concealment.
***: $p < 0.001$.

generate privacy risk belief. Their reactions to SNSs are to conceal their personal information and to not disclose their personal information. A SNSs user becomes a lurker and maintains a lurking behavior during the process of concealing personal information after s/he generates privacy risk belief.

5.2. Academic implications

Prior research failed to consider the assortment of aspects related to the antecedents of privacy risk belief. They only adopted general privacy concern, privacy perceived, and privacy awareness as the antecedents of privacy risk belief. This study proposes that concern for information privacy and the sub-dimensions of ISA such as general information security awareness (GISA) and information security policy awareness (ISPA) as well as consumer alienation which have seldom been investigated are antecedents of privacy risk belief. The new perspective of this research fills up the research gap from previous studies.

Privacy concern and alienation lead to lurking and concealment. A SNSs user gradually becomes a lurker and chooses to reduce self-disclosure from the point of protecting her/his personal private information when s/he faces the impact of any information privacy issue. Past research of lurking was in the fields of psychology or behavioral science. It barely adopted lurking as a behavioral variable even in the field of information technology. This study uses self-disclosure as a theoretical foundation. SNSs users reduce self-disclosure when they are affected by a negative emotion (Stutzman et al., 2011). Prior research confirmed that a user's concern for privacy has a negative effect on her/his attitude and usage intention. This study adopts lurking and self-concealment as the consequences of the effect of negative emotion for SNSs users. A SNS user will not completely quit using SNS but s/he would become a lurker and adopt self-concealment. There are three processes of social influence theory: compliance, identification, and internalization (Kelman, 1958). Zhou and Li (2014) referred to these three processes of social influence as subject norms, group norms, and social identity. Continuous intention and usage intention were widely discussed with social influence in past studies of SNSs users' behaviors (Wang, Meister, & Gray, 2013). This study infers about the reason why SNSs users choose lurking and self-concealment instead of not quitting using SNS is the effect of social influence. This kind of behavior is also called the herd behavior. Sun (2013) pointed out that herd behavior is quite common in the context of information technology usage behavior. A SNS user will give up her/his thought and follows others' actions when herd behavior occurs (Bikhchandani & Sharma, 2000).

SNSs users generate perceived privacy empowerment and think that SNSs facilitate the protection of personal privacy if SNSs vendors effectively provide privacy empowerment. Hence, they reduce lurking by lowering privacy risk belief. Both concern for information privacy and consumer alienation is important factors in the process of generating privacy risk belief for SNSs users with ISA. SNSs users treat privacy from a cost-benefit perspective based on self-protection and believing that personal privacy is risky in a SNSs environment due to the concern for information privacy and powerless of environment. SNSs users with a privacy risk belief go through the lurking process instead of concealing personal private information in SNSs. They do not stop using SNSs immediately but continue to use SNSs in a lurking way when they perceive the threat of privacy. In addition, these lurkers do not disclose their real personal information. Instead, they adopt self-concealment for the purpose of self-protection.

5.3. Practical implications

The fact that SNSs users need to fill out their personal information in order to open an account in SNSs causes problems of information security and has a huge impact on users' intentions to keep using SNSs. SNSs users reduced their SNSs activities in order to ameliorate the leak of personal private information. They restrict themselves to just browse the SNSs contents without expressing their thoughts and providing personal private information. The incidents of information security are serious because of the claim of sharing and publicity by SNSs. It is crucial for SNSs providers to make users' continuous participation in activities in SNSs. Nowadays; many enterprises utilize SNSs as the media for promoting products through the Internet. They increase the exposure of products through fan page advertisements or activities. SNSs activities are the best channels for delivering products' information. Businesses can quickly reach the dissemination effect by sharing information with their customers. They obtain revenues by increasing customers' utilizations or raising users' willingness of disseminating information in SNSs. This study provides guidelines for SNSs vendors to improve users' intentions of using SNSs and disclose their personal private information in SNSs.

Currently, the sense of ISA is common among SNSs users. SNSs providers must increase their safety levels of an information security system to prevent hackers intruding their systems and stealing users' personal private information. In addition, SNSs providers cannot release users' personal information to a third party under any circumstance without the authorization or permission from the SNSs users. SNSs providers must establish friendly and secure environments to mitigate users' concerns for information security as well as provide users' perceived privacy empowerment to alleviate their lurking and self-concealment. SNSs providers must improve privacy protection procedures for their users to increase their intentions of sharing information.

5.4. Limitations and future research directions

It is difficult to collect data from websites outside Taiwan. Future research may include conducting surveys from other countries to

increase the samples size and provide appropriate incentives for SNSs users to expand the scope of research. A longitudinal study is also desired to further extend SNSs users' long-term behaviors. Future research can integrate other relevant constructs such as brand, word-of-mouth (WOM), personality, and website responsiveness or adopt appropriate theoretical models to improve the predictability of the research framework.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Appendix. Information security awareness (7-point likert scale)

General information security awareness

GISA1. Overall, I am aware of the potential security threats and their negative consequences.
GISA2. I have sufficient knowledge about the cost of potential security problems.
GISA3. I understand the concerns regarding information security and the risks they pose.

Information Security Policy Awareness

ISPA1. I know the rules and regulations prescribed by the ISP of SNSs.
ISPA2. I understand the rules and regulations prescribed by the ISP of SNSs.
ISPA3. I know my responsibilities as prescribed in the ISP to enhance the information security systems of SNSs.
References: Bulgurcu et al. (2010).

Concern for information privacy (7-point likert scale)

Collection

COL1. It usually bothers me when SNSs ask for my personal information.
COL2. When SNSs ask for my personal information, I sometimes think twice before providing it.
COL3. It bothers me to give personal information to so many SNSs.
COL4. I am concerned with the fact that SNSs collect too much personal information about me.

Secondary use

SU1. SNSs should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
SU2. SNSs should never sell databases with personal information to other companies.
SU3. SNSs should never share personal information with other companies unless it has been authorized by the individual who provides the information.
SU4. When people give personal information to SNSs for some purpose, SNSs should never use the information for any other purpose.

Unauthorized access

UA1. SNSs should devote more time and effort to prevent unauthorized access to personal information.
UA2. SNSs should take more steps to make sure that the personal information in their databases is accurate.
UA3. SNSs should take more steps to make sure that unauthorized people cannot access personal information in their databases.

Errors

ERR1. All personal information in the SNSs databases should be double-checked for accuracy no matter how much the cost is.
ERR2. SNSs should devote more time and effort to verify the accuracy of the personal information in their databases.
ERR3. SNSs should have better procedures to correct errors in personal information.
References: Schwaig et al. (2013).

Consumer alienation (7-point likert scale)

CSAL1. It is not unusual to find out that businesses lie to the public.
CSAL2. SNSs do not care why people buy their products as long as they make a profit.
CSAL3. SNSs primarily objectives are to maximize profits rather than to satisfy their consumers.
CSAL4. Today it is difficult to identify with SNSs practices.
CSAL5. Unethical practices are widespread throughout SNSs.
CSAL6. Products are designed to wear out long before they should.
CSAL7. A product will usually break down as soon as its warranty is up.
CSAL8. SNSs are responsible for unnecessarily depleting our natural resources. (R).
CSAL9. Most claims about product quality are true. (R).
CSAL10. Harmful characteristics of products are often kept from consumers.
CSAL11. Advertisements usually present true pictures of their products. (R).
CSAL12. Most SNSs are responsive to the demands of their consumers. (R).
References: Schwaig et al. (2013).

Privacy risk belief (7-point likert scale)

PRB1. It would be risky to disclose my personal information to SNSs.
PRB2. There would be high potential losses associated with disclosing my personal information to SNSs.
PRB3. There would be too much uncertainty associated with giving my personal information to SNSs.
PRB4. Providing SNSs with my personal information would involve many unexpected problems.
References: Li et al. (2011).

Lurking (5-point likert scale)

LK1. I use SNSs to send messages without providing my personal information.
LK2. I add some friends simply to keep up with what is happening in their lives.
LK3. I register on some SNSs to just gossip.
LK4. I stay registered on some SNSs to set up online accounts with other organizations.
References: Osatuyi (2015).

Self-concealment (5-point Likert Scale)

SC1. I have an important secret that I have not shared with anyone.

SC2. If I shared all my secrets with my friends, they would like me less.

SC3. There are lots of things about me that I keep to myself.

SC4. Some of my secrets have really tormented me.

SC5. When something bad happens to me, I tend to keep it to myself.

SC6. I am often afraid I will reveal something I do not want to.

SC7. Telling a secret often backfires and I wish I had not said it.

SC8. I have a secret that is so private I would lie if anybody asked me about it.

SC9. My secrets are too embarrassing to share them with others.

SC10. I have such negative thoughts about myself that I would never share them with anyone.

Reference: Larson and Chastain (1990).

Perceived privacy empowerment (5-point likert scale)

PPEM1. SNSs perceive that the tools/options provided to SNSs users give them what they need to control their personal information.

PPEM2. The degree of autonomy in determining how personal information would be used is high.

PPEM3. SNSs influence on what happen to the information.

PPEM4. The overall perception of empowerment provided by SNSs is good.

References: Dyke et al. (2007).

References

Ahn, H., Kwolek, E. A., & Bowman, N. D. (2015). Two faces of narcissism on SNS: The distinct effects of vulnerable and grandiose narcissism on SNS privacy control. *Computers in Human Behavior, 45*(1), 375–381.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Ajzen, I., & Albarracin, D. (2007). Predicting and changing behavior: A reasoned action approach. In I. Ajzen, D. Albarracin, & R. Hornik (Eds.), *Prediction and change of health behavior: Applying the reasoned action approach* (pp. 1–22). London, UK: Lawrence Erlbaum.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.

Allison, N. (1978). A psychometric development of a test for customer alienation from the marketplace. *Journal of Marketing Research, 15*(4), 565–575.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66–84.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly, 34*(4), 689–710.

Bentler, P. M., & Wu, E. J. C. (1993). *EQS/Windows user guide*. Los Angeles, CA: BMDP Statistical Software.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101–106.

Bevan, J. L., Pfyl, J., & Barclay, B. (2012). Negative emotional and cognitive responses to being unfriended on Facebook: An exploratory study. *Computers in Human Behavior, 28*(4), 1458–1464.

Bikhchandani, S., & Sharma, S. (2000). Herd behavior in financial markets. *IMF Staff Papers, 47*(3), 279–310.

Bishop, J. (2007). Increasing participation in online communities: A framework for human–computer interaction. *Computers in Human Behavior, 23*(4), 1881–1893.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares. *First Monday, 15*(8), 1–24.

Boyle, K., & Johnson, T. J. (2010). MySpace is your space? Examining self-presentation of MySpace users. *Computers in Human Behavior, 26*(6), 1392–1399.

Bryer, T. A., & Chen, B. (2010). Using social networks in teaching public administration. In C. Wankel (Ed.), *Cutting-edge social media approaches to business education: Teaching with LinkedIn, Facebook, Twitter, second life, and blogs* (pp. 241–268). Charlotte, NC: Information Age Publishing.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Campbell, A. J. (1999). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing, 11*(3), 44–57.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2009). *Information security control resources in organizations: A multidimensional view and their key drivers*. Vancouver, Canada: Sauder School of Business, University of British Columbia. Working Paper.

Cepeda-Benito, A., & Short, P. (1998). Self-concealment, avoidance of psychological services, and perceived likelihood of seeking professional help. *Journal of Counseling Psychology, 45*(1), 58–64.

Chen, F. C. (2004). Passive forum behaviors (lurking): A community perspective. In *Proceedings of the 6th international conference on learning sciences* (pp. 128–135). Santa Monica, CA: International Society of the Learning Sciences. June 22-26.

Chen, B., & Marcus, J. (2012). Students' self-presentation on Facebook: An examination of personality and self-construal factors. *Computers in Human Behavior, 28*(6), 2091–2099.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology and Behavior, 12*(3), 341–345.

Cole, J. I. (2004). Surveying the digital future year four. *The Digital Future Report, 4*(1), 9–103.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Dennen, V. P. (2008). Pedagogical lurking: Student engagement in non-posting discussion behavior. *Computers in Human Behavior, 24*(4), 1624–1633.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure*. Newbury Park, CA: Sage.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer perceived privacy empowerment on trust and privacy concerns in E-commerce. *Electronic Markets, 17*(1), 68–81.

Efron, B., & Tibshirani, R. J. (1993). *An introduction to the bootstrap*. London, UK: Chapman and Hall.

Fishbein, M. (2007). A reasoned action approach: Some issues, questions, and clarifications. In I. Ajzen, D. Albarracin, & R. Hornik (Eds.), *Prediction and change of health behavior: Applying the reasoned action approach* (pp. 281–296). Hillsdale, NJ: Lawrence Erlbaum & Associates.

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making, 28*(6), 834–844.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley Publishing Company.

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-based Services adoption in Germany. *Computers in Human Behavior, 53*(1), 344–353.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Ganley, D., Moser, C., & Groenewegen, P. (2012). Categorizing behavior in online communities: A look into the world of cake bakers. In *Proceeding of system science (HICSS), 45th Hawaii international conference on IEEE* (pp. 3457–3466). Maui, HI: IEEE. January 4-7.

Golder, S. A., & Donath, J. (2004). Social roles in electronic communities. *Internet Research, 5*(1), 19–22.

Greene, K., Derlega, V. J., & Mathews, A. (2006). Self-disclosure in personal relationship. In A. L. Vangelisti, & D. Perlman (Eds.), *The Cambridge handbook of personal relationships* (pp. 409–427). New York, NY: Cambridge University Press.

Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Pearson Prentice-Hall.

Harman, H. H. (1967). *Modern factor analysis*. Chicago, IL: University of Chicago Press.

Hulland, J. (1999). Use of partial least squares in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195–204.

InsightXplorer. (2015). *The status of Taiwan social media*. InsightXplorer Biweekly Report, 44 http://www.ixresearch.com/category/reports/bi-weekly/. (Accessed 27 April 2016).

Johnson, E. B. (1996). Cognitive age: Understanding consumer alienation in the mature market. *Review of Business, 17*(3), 35–40.

Jöreskog, K. G., & Sörbom, D. S. (1993). *LISREL 8, A guide to the program and application*. Chicago, IL: SPSS Inc.

Kang, K. W., & Shin, S. K. (2008). A model of virtual community knowledge, exchange intentions: Perceived network structure, self-efficacy and individual, motivations. In *Proceedings of the 39th decision sciences institute (DSI) annual meeting* (pp. 2571–2576). Baltimore, MD: Decision Sciences Institute.

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Conflict Resolution, 2*(1), 51–60.

Kollock, P., & Smith, M. (1996). Managing the virtual commons: Cooperation and conflict in computer communities. In S. Herring (Ed.), *Computer-mediated communication: Linguistic, social and cross-cultural perspectives* (pp. 109–128). Amsterdam, Netherlands: John Benjamins.
Lambert, Z. V. (1981). Profiling demographic characteristics of alienated consumers. *Journal of Business Research, 9*(1), 65–86.
Larson, D. G., & Chastain, R. L. (1990). Self-concealment: Conceptualization, measurement, and health implications. *Journal of Social and Clinical Psychology, 9*(4), 439–455.
Lave, J., & Wenger, E. (1991). *Situated learning. Legitimate peripheral participation*. New York, NY: Cambridge University Press.
Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187.
Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications, 13*(1), 32–44.
Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434–445.
Mady, T. T. (2011). Sentiment toward marketing: Should we care about consumer alienation and readiness to use technology. *Journal of Consumer Behavior, 10*(4), 192–204.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.
Masuda, A., & Latzman, R. D. (2012). Psychological flexibility and self-concealment as predictors of disordered eating symptoms. *Journal of Contextual Behavioral Science, 1*(1), 49–54.
McKnight, M. D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems, 11*(3), 297–323.
Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online. *Computers in Human Behavior, 28*(4), 1471–1477.
Metzger, M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-mediated Communication, 9*(4). http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2004.tb00292.x/full. (Accessed 27 November 2015).
Middleton, R. (1963). Alienation, race, and education. *American Sociological Review, 28*(6), 973–977.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.
Mo, K. H., & Coulson, N. S. (2010). Empowering processes in online support groups among people living with HIV/AIDS: A comparative analysis of lurkers and posters. *Computers in Human Behavior, 26*(5), 1183–1193.
Morris, M., & Ogan, C. (1996). The internet as mass medium. *Journal of Communication, 46*(1), 39–50.
Moscovitch, D. A. (2009). What is the core fear in social phobia? A new model to facilitate individualized case conceptualization and treatment. *Cognitive and Behavioral Practice, 16*(2), 123–134.
Neelen, M., & Fetter, S. (2010). Lurking: A challenge or a fruitful strategy? A comparison between lurkers and active participants in an online corporate community of practice. *International Journal of Knowledge and Learning, 6*(4), 269–284.
Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and leadership: A unified model of dynamic knowledge creation. *Long Range Planning, 33*(1), 5–34.
Nonnecke, B., Andrews, D., & Preece, J. (2006). Non-public and public online community participation: Needs, attitudes and behavior. *Electron Commerce Research, 6*(1), 7–20.
Nonnecke, B., & Preece, J. (2001). Why lurkers lurk. In *Proceeding of 2001 - seventh Americas conference on information systems* (pp. 1–10). Boston, MA: AMCIS.
Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York, NY: McGraw-Hill.
Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior, 49*(1), 324–332.
Pi, S. M., Chou, C. H., & Liao, H. L. (2013). A study of Facebook groups members' knowledge sharing. *Computers in Human Behavior, 29*(5), 1971–1979.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.
Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531–544.
Pruden, H. O., Shuptrine, F. K., & Longman, D. S. (1974). A measure of alienation from the marketplace. *Journal of the Academy of Marketing Science, 2*(4), 610–619.
Rheingold, H. (1993). *The virtual community. Homesteading on the electronic frontier*. Reading, MA: Addision-Wesley Publishing Company.
Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50*(1), 1–12.
Seeman, M. (1959). On the meaning of alienation. *American Sociological Review, 24*(6), 783–791.
Shuptrine, F. K., Pruden, H. O., & Longman, D. S. (1977). Alienation from the marketplace. *Journal of the Academy of Marketing Science, 5*(3), 233–248.
Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.
Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415–444.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.
Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. *Sociological Methodology, 13*, 290–312.
von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security, 7*(1), 50–58.
Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–49.
Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468.
Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590–598.
Sun, H. (2013). A longitudinal study of herd behavior in the adoption and continued use of technology. *MIS Quarterly, 37*(4), 1013–1041.
Sun, N., Rau, P. P. L., & Ma, L. (2014). Understanding lurkers in online communities: A literature review. *Computers in Human Behavior, 38*, 110–117.
Wang, Y., Meister, D. B., & Gray, P. H. (2013). Social influence and knowledge management systems use: Evidence from panel data. *MIS Quarterly, 37*(1), 299–313.
Wellman, B., & Gulia, M. (1999). Net surfers don't ride alone: Virtual communities as communities. In B. Wellman (Ed.), *Networks in the global village* (pp. 331–366). Boulder, CO: Westview.
Wenger, E. (1998). *Communities of practice: Learning, meaning and identity*. Cambridge, UK: Cambridge University Press.
Wheeless, L. R. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research, 4*(2), 143–157.
Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338–346.
Whelan, B. (2005). *Facebook, A fun resource or invasion of privacy*. http://athensnews.com/issue/article.php3?story_id=21491. (Accessed 13 February 2016).
Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior, 37*(1), 283–289.
Zimmer, J., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115–123.
Zlatolas, L. N., Welzer, T., Hericko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*(1), 158–167.

Jaime Ortiz is the Vice Provost for Global Strategies and Studies at the University of Houston. His research focuses on topics related to economic growth and development, global investment decisions, and identification of sources and origins of technical change. He is the author, co-author, or editor of numerous books, book chapters, textbooks, research monographs and technical reports, and refereed journal articles.

Wen-Hai Chih is a Professor in the Department of Business Administration, National Dong Hwa University. His research interests include e-commerce, virtual community, social media, and social marketing. He has published more than 100 papers in 30 journals.

Faa-Shyan Tsai is a Customer Feedback Manager from the Department of Product Management, QNAP System, Inc. His research interests include social media, information privacy, social influence, and e-commerce.