Computers in Human Behavior 38 (2014) 159–173

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation

Aakash Taneja *, Jennifer Vitrano, Nicolas J. Gengo

Richard Stockton College of New Jersey, 101 Veera King Farris Drive, Galloway, NJ 08205, United States

ARTICLE INFO

Article history:
Available online 28 June 2014

Keywords:
Facebook
Online social networking
Privacy control
Rational choice
Rationality-based beliefs
Theory of planned behavior

ABSTRACT

Online social networking sites like Facebook provides a fast and easy way to connect with friends and family. Users need to post and share their personal information in order to get the best possible experiences on Facebook. However, the spreading of private information can also lead to serious and harmful issues. Therefore, privacy becomes an important component in the use of Facebook and it is the user's responsibility to protect his or her profile. This study draws upon the theory of planned behavior and the rational choice theory to investigate the rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook. The results show that individual's attitude toward using privacy controls is influenced by benefit of using privacy controls, cost of using privacy controls, and cost of not using privacy controls. Further, benefits of using privacy controls is shaped by beliefs regarding intrinsic benefit and resource safety; cost of not using privacy controls is shaped by beliefs regarding resource vulnerability, threat severity, privacy risk and privacy intrusion; and cost of using privacy controls is shaped by beliefs about intrinsic cost and work impediment. Theoretical and practical implications of the findings are discussed in the paper.

1. Introduction

Online social networking is a fast and easy way to stay connected with friends and family through the Internet. Online social networking sites (SNSs) like Facebook, Myspace, Instagram and LinkedIn allow users to create and manage profiles that can be used to connect with others and create a personal network with the objective of social interaction, connection and communication (Cheung, Chiu, & Lee, 2011). In order to connect with others, users build their profiles by generating content that reflects their personalities and interests, and by posting information about themselves, such as describing their interests, and sharing photos, posts, links, events, and much more. With the advent of technology and the large amounts of information traveling across the Internet, personal information is harder to keep private; thus, sharing information this way could lead to risks. Social networking sites have the responsibility of maintaining the assurance and security of their users' private information. However, information can be shared without users' knowledge in ways that they may not appreciate, so it is important for users to act responsibly for safeguarding their information.

Facebook is one of the most popular online social networking sites with users ranging from teenagers to older adults. However, the vast majority of users are young adults. Facebook allows users to create profiles, post information about them, and add friends to build their social circles. Users are able to connect with others in ways that are similar to relationships in the real world, except Facebook brings it to a higher level. Virtual communities are created among users that share similar interests and explore new interests. With continuous updates flooding users' news feeds, Facebook keeps users interested in coming back to the site (Stutzman, Capra, & Thompson, 2011). Facebook also provides a unique research environment because of its heavy usage patterns and its ability to bridge online and offline connections (Ellison, Steinfield, & Lampe, 2007). In order for users of Facebook to get the best possible experiences, users must post and share their personal information. Therefore, privacy becomes an important component in the use of Facebook.

Different users want their personal information to be seen in different ways. While some users want to keep their lifestyles discreet, and only use the site as a means to keep in touch, others post as much information and as many status updates as possible. Public and private information alike can be found and shared on social networking sites like Facebook. However, the spreading of private information can also lead to serious and harmful issues.

* Corresponding author. Tel.: +1 609 652 4948.
E-mail address: aakash.taneja@stockton.edu (A. Taneja).

http://dx.doi.org/10.1016/j.chb.2014.05.027
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

Privacy issues have hung over sites like Facebook as users many times do not think about the repercussions of sharing their information on Facebook. Although privacy controls exist on Facebook, it is at the user's expense to activate and protect his or her profile. The objective of this study is to investigate the rationality-based beliefs affecting individual's attitudes and intention to use privacy controls available on Facebook.

The rest of the paper is organized as follows. The next section presents a brief review of the relevant literature followed by this study's theoretical framework and research model. Next, we present the research methodology. We then provide data analysis and results. Finally, we conclude by discussing our findings, their implications, and future research directions.

2. Literature review

The use of social networking websites, especially Facebook, has continued to be an important topic for researchers. Many researchers have conducted studies on various aspects of the use of Facebook, including people's motives in using Facebook, information disclosure, privacy concerns, trust related issues, and the importance of privacy controls available on Facebook.

Pempek, Yermolayeva, and Calvert (2009) studied college students' use of Facebook and found that students facilitate social relationships by connecting with offline friends and searching for new friends in order to develop their individual identities as they experience emerging adulthood, and to gather feedback on their disclosed information to feel good about themselves. Kim, Kim, and Nam (2010) used self-construal to explore how individuals define and relate themselves to their surroundings and others for assessing the relationship between people's understanding of self as a predictor of social computing (Facebook use) and satisfaction. The other factors involved in the study were social and nonsocial motivations, use behaviors (use time, average stay time per login, number of "friends" in SNS, and profile length), and satisfaction. They found that users with higher self-construal have stronger motivations to use Facebook to build social relationships. From an organizational use perspective, Fernandez (2009) described libraries' potential for using Facebook as a means to connect with their library patrons. The author realized that this outreach not only has advantages, but also collides with the privacy concerns associated with disclosing sensitive library information through Facebook. Peluchette and Karl (2009) notes that businesses use Facebook to investigate potential employees, and explore the factors that influence college students' posting of inappropriate information.

Researchers have conducted interesting studies related to information disclosure on social networking sites. Nagle and Singh (2009) observes that Facebook users' are willing to disclose their personal information based on the friendship circle. Users are willing to allow strangers into their friendship circle so long as there are mutual connections, i.e. mutual friends. Boyle and Johnson (2010) found that Myspace users were more willing to disclose broad pieces of information, including age, race and gender, than they were for more personal information. Moreover, users will disclose information based on their reasons for creating profiles. Joinson (2008) notes the fact that Facebook's social search capabilities benefit users to the extent that they are willing to disclose their information in order to get the most out of using Facebook.

As individuals need to provide adequate levels of personal information in order to gain the desired benefits of using Facebook, privacy-related concerns arise. Acquisti and Gross (2006) studied college users' privacy concerns and its impact on their usage of and attitudes toward Facebook and found that despite the knowledge of the various risks to disclosing private information online, students' privacy concerns have little effect on their membership of and information revealed on Facebook. However, they also found that these students do not realize the visibility of their profiles and information to other parties on the vast Facebook network. Dwyer, Hiltz, and Passerini (2007) noted that trust and privacy influenced users' willingness to make friends and disclose information on the social networking sites. Debatin, Lovejoy, Horn, and Hughes (2009) argue that Facebook users who have experienced privacy invasions are more likely to change how they disclose their personal information than users who merely heard about others' privacy invasions.

While Fogel and Nehmad (2009) studied how risk-taking is involved in the usage of social networking sites and found that trust and privacy are major issues, Lo (2010) notes that perceived risk and trust determine whether users are willing to disclose personal information on social networking sites. Brandtzæg, Luders, and Skjetne (2010) claims that sociability and content sharing, important aspects involved in the success of social networking sites, are affected by users' privacy concerns. Lo and Riemenschneider (2010) also found that internet privacy concern, trust in the site, trust in friends, and trust in everyone affect users' willingness to provide information. Nosko, Wood, and Molema (2010) studied the types of information that can be disclosed on Facebook, as well as the types of user characteristics that are likely to disclose certain information. They found that as age increased, less information was disclosed. Also, users in a relationship revealed more sensitive personal information and potentially stigmatizing information. Walrave, Vanwesenbeeck, and Heirman (2012) found that both young and adult users place little trust in SNS but disclose their personal information for communicating with their friends. They found that privacy concerns affect how adults disclose information and open their profiles, and peer-pressure influences adolescents to disclose more information.

The extant literature has investigated the importance of privacy controls on Facebook. Lewis, Kaufman, and Christakis (2008) observed the factors that determine whether college students will have private Facebook profiles. The factors that influence college students' use of privacy settings stem from social influence and personal incentive mechanisms. Joinson (2008) notes the fact that Facebook's social search capabilities benefit users to the extent that they are willing to leave their privacy settings more open in order to get the most out of the function. Hoadley, Xu, Lee, and Rosson (2010) showed that the news feed's easy-to-use features were only made possible by allowing more specific access to sensitive and personal information.

While Guo (2010) discussed the features of Facebook contributing to privacy issues, including news feeds, beacons, third parties and privacy policies, Gross and Acquisti (2005) found that privacy preferences are rarely used, resulting in privacy risks for the users. These studies shed light on the fact that SNS users are freely open to revealing their personal information online and connecting to friends and strangers. Brandtzæg et al. (2010) suggests that these sites employ privacy settings for users to customize the disclosure of their information in order to improve sociability and content sharing. In their study of medical students' use of Facebook, MacDonald, Sohn, and Ellis (2010) determined that the site's privacy controls must be properly adjusted to limit disclosure of sensitive content and other confidential information pertaining to the medical profession. Hull, Lipford, and Latulipe (2011) describes how Facebook's applications and news feeds present risks to privacy, and explains why the problem is caused by the design of each feature. It signifies the need for users to actively take controls of safeguarding their privacy. Chaulk and Jones (2011) conducted research concerning the use of Facebook as a medium for stalking, and provided implications for not using privacy controls. Bornoe and Barkhuus (2011) found that users had little or no knowledge about privacy settings, nor did they expend resources on privacy management; however, these users did use common sense for determining which information to disclose (e.g. avoiding inappropriate photos that may be seen by potential employers). Liu, Gummadi, Krishnamurthy, and Mislove (2011) compared Facebook users' ideal privacy settings with their actual privacy settings and provided suggestions for assisting users in privacy controls.

The analysis of the extant literature on Facebook shows that the prior research has primarily focused on motives behind using Facebook, information disclosure, privacy concerns related to the use of the platform, and the importance of available privacy controls. However the reasons an individual uses or does not use privacy controls available on Facebook are yet to be explored. It is therefore needed to conduct a theoretical based study for understanding factors influencing individuals' use of privacy controls available on Facebook.

3. Theoretical framework

3.1. Information security policy (ISP) compliance model

Information security risks are a major challenge for many organizations and ensuring information security is among the top priorities in many organizations. The information security policy (ISP) of an organization defines the roles, responsibilities, and instructions for employees to safeguard organization's information systems and computing assets (Bulgurcu, Cavusoglu, & Benbasat, 2010). Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, Bulgurcu et al. (2010) integrated the theory of planned behavior and the rational choice theory to develop ISP compliance model for identifying the antecedents of employee compliance with the ISP of an organization (Fig. 1).

Based on the theory of planned behavior, Bulgurcu et al. (2010) formulate that an employee's attitude toward compliance along with normative belief and self-efficacy determines intention to comply with the ISP. Next, the authors used rational choice theory to identify the antecedents of attitude toward ISP compliance.

The rational choice theory discusses how one makes a decision to fulfill some goal. According to this theory, an individual is faced with multiple choices to achieve a goal and each choice is an alternative course of action to fulfill the goal, and by comparing the costs and benefits of these alternatives, the individual arrives at an overall assessment of consequences, which is then used to make the best decision to fulfill the goal (Paternoster & Pogarsky, 2009). Drawing on the rational choice theory, Bulgurcu et al. (2010) suggests that employees choices are to comply or not comply with the ISP and the employees consider the benefits and costs of each choice. An employee's beliefs that performing or not performing the compliance behavior will lead to certain consequences (i.e., costs and benefits) are the determinants of an individual's attitude toward compliance behavior. Consistent with the rational choice theory, the authors define these as "beliefs about overall assessment of consequences of compliance and noncompliance". The beliefs about overall assessment of consequences of compliance or noncompliance are next influenced by an individual's beliefs about the outcomes of compliance and noncompliance. The beliefs about outcomes are defined as the beliefs that certain events will follow from performing (or not performing) the compliance behavior.

In Bulgurcu's ISP compliance model, the proximal determinants of employees' attitudes toward compliance are perceived benefit of compliance, perceived cost of compliance, and perceived cost of noncompliance. Further, benefit of compliance is influenced by intrinsic benefit, safety, and rewards; cost of compliance is influenced by work impediment; and cost of noncompliance is influenced by sanctions, intrinsic cost, and vulnerability.

We adopt Bulgurcu's ISP compliance model as the theoretical framework and examine the proximal determinants of individuals' attitudes toward using privacy controls. Although ISP compliance could be either compulsory or expected within organizations, specification of a set of security policies itself is associated with employees perceiving its compliance as mandatory (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). While Bulgurcu's study pertains to adoption of a behavior which, depending on the organization, could be mandatory or not strictly mandatory, our research is related to adoption of a behavior which is entirely voluntary and completely under users' discretion. In addition, while the consequence of an individual's ISP compliance behavior is targeted toward organization's resources, the effect of an individual's use of privacy controls available on Facebook, the behavior of interest in this study, is targeted toward an individual's own information resources.

Based on theoretical grounding and practical empiricism, we also identify individuals' salient beliefs about outcomes of using or not using privacy controls to develop our research model. These beliefs include intrinsic benefits, resource safety, and response efficacy (determinants of benefit of using privacy controls); resource

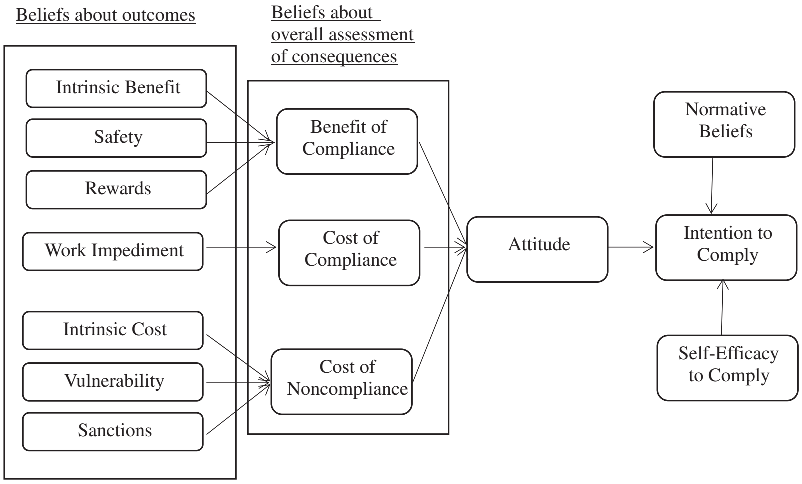

Fig. 1. Information security policy compliance model (Bulgurcu et al., 2010).

vulnerability, threat severity, privacy risk, and privacy intrusion (determinants of cost of not using privacy controls); and intrinsic cost and work impediment (determinants of cost of using privacy controls).

4. Research model

With the advent of technology and the large amount of information that travels through the Internet, personal information is harder to keep private. One way private information is stored and shared on the Internet is through social networking sites. Because different users wish to expose varying levels of their personal information, Facebook provides mechanisms to allow users to control the level of access to their information given to others. We define Facebook privacy controls as the settings an individual can use to limit the access of information given to others and controls which people and apps can see their information on Facebook. We adopt Bulgurcu's ISP compliance model and use the theory of planned behavior along with the rational choice theory to develop our research model and understand the beliefs affecting individual's attitude toward and intentions to use privacy controls on Facebook (Fig. 2). Based on the theory of planned behavior (Fishbein & Ajzen, 1975), an individual's intention to use Facebook privacy controls is used as a dependent variable in this study.

4.1. Determinants of intention to use privacy controls

4.1.1. The theory of planned behavior (TPB)

The theory of planned behavior (Fishbein & Ajzen, 1975) discusses an individual's intention toward a given behavior, which is defined as an indication of his or her readiness to use privacy controls available on Facebook. It is suggested from this theory that intention toward a given behavior can be predicted from attitudes toward the behavior, social norms, and perceived behavioral controls.

4.1.1.1. Attitude. Attitude is defined as the degree to which the performance of the behavior is positively or negatively valued by an individual (Fishbein & Ajzen, 1975). Prior studies have demonstrated that attitude toward behavior positively affects the intention to perform a behavior. As hypothesized in the TPB (Fishbein & Ajzen, 1975), if an individual has a positive attitude toward the use of privacy controls, he or she is more likely to have an intention to use privacy controls available on Facebook. Therefore,

H1. Attitude toward using Facebook privacy controls is positively related to intention to use Facebook privacy controls.

4.1.1.2. Social norm. Social norm is defined as the perceived social pressure to engage or not to engage in a behavior (Fishbein & Ajzen, 1975). While some studies have found social norm to influence intention (Hung, Ku, & Chang, 2003), others have not. For example: Mathieson (1991) and Venkatesh, Morris, Davis, and Davis (2003)'s work in technology acceptance model (TAM) based research found that social norms influences intention only when it is mandatory (not voluntary) to adopt the system. It is pertinent to note that these TAM based studies have primarily focused on the adoption of technology primarily used for utilitarian purposes (Sledgianowski & Kulviwat, 2009) that focus on increasing the user's task performance while encouraging efficiency (Van der

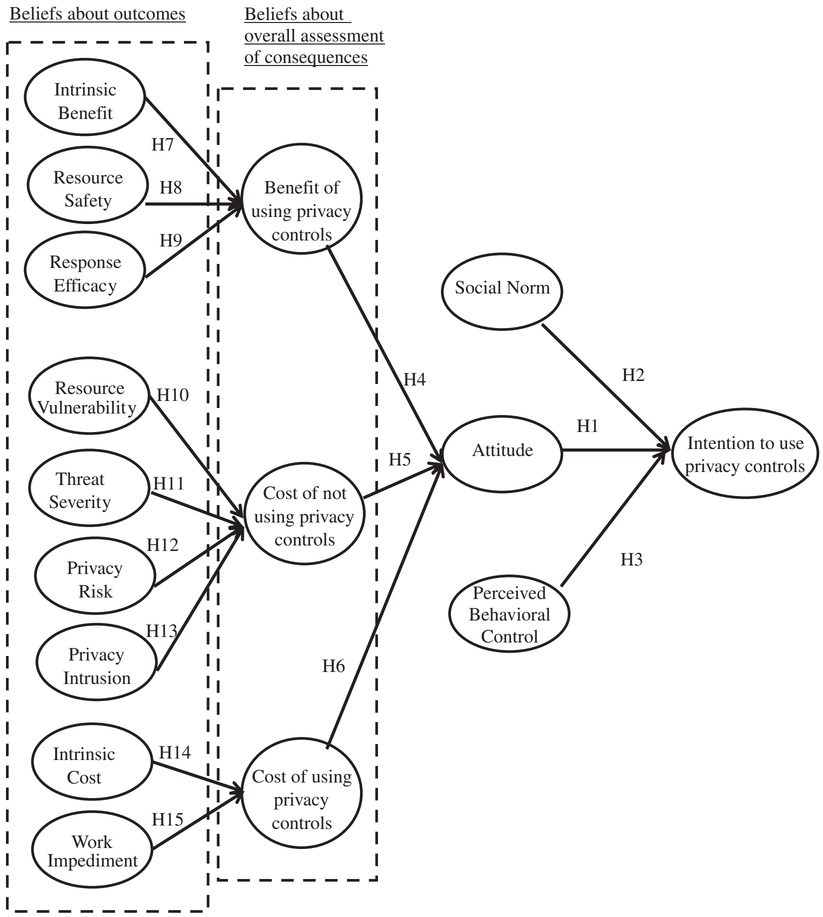

Fig. 2. Research model.

Heijden, 2004). However, Facebook is a hedonic system which allows the user to experience fun and enjoyment while using the system (Van der Heijden, 2004) by interacting with friends, family members, and others. Individuals therefore share information and accordingly use privacy controls based on the norms of what they perceive that others are expecting them to do (Christofides, Muise, & Desmarais, 2009). As hypothesized in the TPB, if an individual perceives that the norm in his or her reference group is favorable toward the use of privacy controls, the individual is more likely to have an intention to use privacy controls available on Facebook. Therefore,

H2. Social norms in favor of using Facebook privacy controls are positively related to intention to use Facebook privacy controls.

4.1.1.3. Perceived behavioral control. Perceived behavioral control (PBC) is defined as the degree to which an individual believes how easy or difficult it would be to perform a behavior (Fishbein & Ajzen, 1975). If users are not confident in their ability to use privacy controls in ways that most fit their needs, they may shy away from the use. As hypothesized in the TPB, the individuals who believe themselves as having control over the use of privacy controls on Facebook are more likely to have an intention to use. Therefore,

H3. Perceived behavioral controls toward using Facebook privacy controls is positively related to intention to use Facebook privacy controls.

4.2. Beliefs about overall assessment of consequences of using or not using privacy controls

Fishbein and Ajzen (1975) argue about the role played by various variables other than the three proximal variables (attitude, social norm, and perceived behavioral control). According to them, an individual's attitude toward a behavior is influenced by his or her beliefs about behavior-related consequences. We adopt Bulgurcu's ISP compliance model to identify beliefs about overall assessment of consequences of using or not using privacy controls on Facebook.

4.2.1. Bulgurcu's ISP compliance model

In accordance with the study conducted by Bulgurcu et al. (2010), we conceive the notion of benefits and costs related beliefs about using privacy controls on Facebook to encompass three distinct beliefs. The first belief, perceived benefit of using privacy controls on Facebook is defined as the overall expected favorable consequence to a user for using privacy controls on Facebook. The second belief is perceived cost of not using privacy controls, which we define as the overall expected adverse consequences for not using Facebook privacy controls. The third belief, the perceived cost of using privacy controls on Facebook, is the overall expected adverse consequences for using Facebook privacy controls.

4.2.1.1. Perceived benefit of using privacy controls. The perceived benefit of using privacy controls is defined as the overall predicted favorable consequence to a user for using privacy controls. A user who believes that he or she will achieve expected and favorable outcomes from the use of privacy controls sees the benefit. Users will only take advantage of the mechanisms if they feel there is a real benefit from using them. According to the expectancy-value theory, behavior is a function of an individual's expectancies for success and value of the goal toward which one is working (Wigfield, 1994). When more than one behavior is possible, individuals are more likely to choose the behavior with the largest combination of expected success and value. Therefore, an individual forms a positive attitude toward behaviors leading to desirable consequences (Bulgurcu et al., 2010). The higher the perceived benefit, the more favorable the attitude toward the use of privacy controls. Therefore,

H4. Perceived benefit of using privacy controls is positively related to attitude toward using privacy controls.

4.2.1.2. Perceived cost of not using privacy controls. The perceived cost of not using privacy controls is defined as the overall expected unfavorable consequences for not using privacy controls. According to the expectancy-value theory, if an individual perceives that there will be some disadvantages for not using privacy controls, he or she will have a favorable attitude toward using privacy controls (Bulgurcu et al., 2010). The higher the perceived cost of not using privacy controls, the more favorable the attitude toward use of privacy controls. Therefore,

H5. Perceived cost of not using privacy controls is positively related to attitude toward using privacy controls.

4.2.1.3. Perceived cost of using privacy controls. The perceived cost of using privacy controls is defined as the overall expected unfavorable consequences for using privacy controls. The steps an individual must take in order to protect his or her information through privacy controls may cause a negative consequence to the user through things such as inconvenience, additional effort, or ineffective utilization of Facebook. Users may feel that, in addition to the benefits of controlling their personal information by toggling privacy controls on Facebook, there will be negative downsides as well. These downsides are the costs of using privacy controls. The higher the cost of using privacy controls, the lower the attitude toward use of privacy controls. Therefore,

H6. Perceived cost of using privacy controls is negatively related to attitude toward using privacy controls.

4.3. Drivers of beliefs about overall assessment of consequences of using or not using privacy controls

As noted by Bulgurcu et al. (2010), beliefs about overall assessment of consequences (i.e., costs and benefits) result from processing the beliefs about outcomes of performing or not performing a behavior. Therefore, individuals are expected to form beliefs about overall assessment of consequences (costs and benefits) of using or not using privacy controls by evaluating various outcomes that will follow from using or not using privacy controls. In order to identify individuals' salient beliefs about outcomes of using or not using privacy controls, we conducted a belief elicitation exercise in a free-response format (Fishbein & Ajzen, 2010) by soliciting responses from 35 students and grouping them into nine categories based on "theoretical grounding and practical empiricism" (Pavlou & Fygenson, 2006).

The intrinsic motivational models of human behavior emphasize individuals' preferences and desires as the fundamental drivers of behavior (Taylor & Todd, 1995). Intrinsic benefits are the internal gratifications felt by individuals, and these gratifications motivate them to perform a behavior (Lin & Hwang, 2014). Intrinsic benefits are found to motivate individuals to use computer mediated discussion forums (Hsu, Ju, Yen, & Chang, 2007), virtual communities (Hsu et al., 2007) and knowledge management systems (Lin & Hwang, 2014). Davis, Bagozzi, and Warshaw (1992) found that intrinsic factors affect the motivation to use information technology systems. In the context of Facebook, people have a sense of relief and satisfaction if they feel that their personal information is well-kept and protected from misuse and other harm because of using privacy controls available on Facebook. As such, we posit that intrinsic benefit is an outcome belief about the benefit of using privacy controls.

Intrinsic cost reflects an individual's negative feelings due to the consequence of performing a behavior. Bulgurcu et al. (2010) found that intrinsic cost (guilt, embarrassment, shame, and stress) is an outcome belief about information security policy noncompliance behavior. In the context of Facebook, individuals could feel guilty, embarrassment or shame if they think that the use of privacy controls will restrict others from knowing about them. Therefore, intrinsic cost is an outcome belief about the cost of using privacy controls.

According to the models of goal-directed behavior, individuals avoid activities which disrupt their desired goal or outcome (Viane, Crombez, Eccleston, Devulder, & De Corte, 2004). If an individual performs a behavior that results in the disruption of a desired goal, the individual feels unpleasant. Individuals formulate responses in ways which result in avoidance of such behaviors. Previous studies have found that ensuring information security may interfere with the goals of the business or individuals (Bulgurcu et al., 2010; Pahnila, Siponen, & Mahmood, 2007; West, 2008). We therefore postulate that work impediment is an outcome belief about the cost of using privacy controls.

The protection motivation theory (PMT) is considered as one of the most powerful theories for predicting an individual's intention to engage in protective behavior. According to the PMT, the motivation to self-protect from risks is a result of perceived severity (the magnitude of the threat), perceived vulnerability (the extent to which the individual is perceived to be susceptible to the threat), and perceived response efficacy (belief that the behaviors will be effective in reducing or eliminating the danger) (Rogers, 1975).

According to the health belief model (Rosenstock, 1974), perceived susceptibility refers to an individual's perception of the risk of acquiring an illness or disease. Prior literature has shown that the individuals who perceive vulnerability to the threat of virus attacks are more likely to engage in virus protection behaviors (Mohamed & Ahmad, 2012). The individuals who believe that their information resources will be vulnerable to harm and exploits in the absence of privacy controls will consider it as the cost of not using privacy controls. Therefore, resource vulnerability is an outcome belief about the cost of not using privacy controls.

According to the health belief model, perceived severity refers to a person's feelings on the seriousness of contracting an illness or disease. It is the primary component of a fear appeal that contributes to an individual's reaction and intensity of a response (Johnston & Warkentin, 2010; Rogers, 1975). The individuals who believe that the harm to their information resources will be severe if these are exploited in the absence of proper privacy controls will consider it as the cost of not using privacy controls. Therefore, perceived severity is an outcome belief about the cost of not using privacy controls.

Response efficacy is defined as the extent an individual believes that a recommended response will effectively reduce a threat (Witte, 1992) and is an important concept in several health information processing models, including the health belief model (Rosenstock, 1974). Previous studies have found that the motivation to adopt the protective behavior arises from the individual's expectation that it can reduce the likelihood or severity of harm (Cismaru & Lavack, 2006). We therefore surmise that response efficacy is an outcome belief about the benefit of using privacy controls.

Privacy has been interpreted as the "boundary control process in which individuals regulate when, how, and to what extent information about them is communicated to others" (Mohamed & Ahmad, 2012). Information privacy issues are found to influence willingness to disclose personal information on the Internet (Mohamed & Ahmad, 2012). Perceived privacy risk is the expectation of losses associated with the disclosure of personal information and has been found to impact the decisions of individuals to disclose personal information (Li, Sarathy, & Xu, 2010). The individuals who believe that not using privacy controls will risk their privacy as their personal information can be disclosed to others will consider such risks as cost of not using privacy controls. Therefore, privacy risk is an outcome belief about cost of not using privacy controls.

Intrusion reflects undesirable interference of another's presence or activities on an individual and has been found to create discomfort and harm to individuals (Xu, Dinev, Smith, & Hart, 2008). The individuals who attribute the possibility of intrusion, unwanted access and interference with their personal lives to not using privacy controls will consider such intrusion to their privacy as cost of not using privacy controls. Therefore, privacy intrusion is an outcome belief about cost of not using privacy controls.

The quality in use integrated measurement model specifies that the usability of a system depends upon whether it ensures safety by limiting the risk of harm to people or other resources, such as stored information (Braz, Seffah, & M'Raihi, 2007). In the context of Facebook, if the individuals feel that privacy controls will contribute to the safety of their personal information, then they will appreciate the advantage of using privacy controls. Therefore, resource safety is an outcome belief about the benefit of using privacy controls.

In summary, we conceptualize nine outcome beliefs related to the use of privacy controls that provide the foundation for beliefs about overall assessment of consequences. These include intrinsic benefits, resource safety, and response efficacy (determinants of benefit of using privacy controls); resource vulnerability, threat severity, privacy risk, and privacy intrusion (determinants of cost of not using privacy controls); and intrinsic costs and work impediment (determinants of cost of using privacy controls). In the following sections, we discuss each of these beliefs about outcomes under the corresponding beliefs about overall assessment of consequences and formulate the related hypotheses.

4.3.1. Drivers of benefit of using privacy controls

Based on the above discussions, we model three outcome beliefs that drive individuals' assessments of the benefits associated with the course of action. These are (i) intrinsic benefits, (ii) resource safety, and (iii) response efficacy.

4.3.1.1. Intrinsic benefit. Intrinsic benefit is defined as an individual's positive feelings, such as satisfaction and fulfillment, about using privacy controls (Bulgurcu et al., 2010). People feel a sense of relief when they know their personal information is well-kept and protected from misuse and other harm. Knowing that outside users cannot access certain information unless they are granted permission may give one the satisfaction of knowing that he or she is able to really control who can see the information at hand. If users achieve positive feelings when they control the use of their personal information, they will be more likely to use them. The higher the intrinsic benefit, the higher an individual will perceive the benefit of using privacy controls. Therefore,

H7. Intrinsic benefit is positively related to the perceived benefit of using privacy controls.

4.3.1.2. Resource safety. Resource safety is defined as an individual's perception that that his or her content posted on Facebook is safeguarded (Bulgurcu et al., 2010) as a result of using privacy controls. If a user perceives that his or her content is susceptible to misuse or other possible harm, he or she may shy away from revealing enough information, thus resulting in a lower overall experience. Facebook privacy controls are made available to allow users to toggle what information is shared or can be seen or accessed. If users perceive that these controls can be used to reduce potential misuse of the content that is posted, resource safety is apparent. Resource safety is one of the benefits of using privacy controls. The higher the resource safety, the higher an individual will perceive the benefit of using privacy controls. Therefore,

H8. Resource safety is positively related to the perceived benefit of using privacy controls.

4.3.1.3. Response efficacy. Response efficacy is defined as a person's belief that the recommended behaviors are effective in reducing or eliminating the threat (Johnston & Warkentin, 2010; Keller, 1999). Threats to people's privacy become increasingly possible as users post their sensitive information online. Users of Facebook, who get the most out of their social experience by constantly posting information about them, are at risk of threats to this information. If users believe the privacy controls available on Facebook help to prevent these threats, then they will be more likely to toggle the controls to their suiting. Response efficacy is a benefit of using privacy controls, so users who believe in a stronger response efficacy see a clear advantage to using the mechanisms. According to the protection motivation theory, high levels of response efficacy are associated with positive inclination toward response mechanism (Johnston & Warkentin, 2010). The higher the response efficacy, the higher an individual will perceive the benefit of using privacy controls. Therefore,

H9. Response efficacy is positively related to the perceived benefit of using privacy controls.

4.3.2. Drivers of the cost of not using privacy controls

We model four outcome beliefs that drive individuals assessments of the cost associated with not following the course of action. These are (i) resource vulnerability, (ii) threat severity, (iii) privacy risk, and (iv) privacy intrusion.

4.3.2.1. Resource vulnerability. Resource vulnerability is defined as an individual's belief that his or her content posted on Facebook is exposed to privacy-related risks and threats as a consequence of not using privacy controls. Users post their personal information on Facebook in order to achieve the best possible experience. But the downside to this is risks and threats to their private information that can be accessed or misused by unauthorized users. As observed by Bulgurcu et al. (2010), missing or ineffectively administered safeguard mechanisms allows a threat to occur with a greater impact and/or frequency (Peltier, 2004). If users perceive that resource vulnerability is high, they are more likely to believe that the unfavorable consequences for not using privacy controls are high. The higher the resource vulnerability, the higher an individual will perceive the cost of not using privacy controls. Therefore,

H10. Resource vulnerability is positively related to the perceived cost of not using privacy controls.

4.3.2.2. Threat severity. Threat severity refers to the beliefs that a fear appeal's audience holds toward the significance of the threat related to their invasion of privacy (Johnston & Warkentin, 2010). It is the primary component of a fear appeal that contributes to an individual's reaction and intensity of a response (Johnston & Warkentin, 2010; Rogers, 1975). While sharing their information on Facebook, individuals are faced with the possibility of misuse of their information and invasion of privacy. As the threat of invasion of privacy is perceived to be severe, users will more likely believe that the unfavorable consequence for not using privacy controls is high. Therefore,

H11. Threat severity is positively related to the perceived cost of not using privacy controls.

4.3.2.3. Privacy risk. Privacy risk is defined as the expectation of losses associated with the disclosure of personal information on Facebook (Xu et al., 2008). Perceived risk to privacy is a salient belief in information privacy contexts (Miyazaki & Fernandez, 2000). Extant literature has confirmed the negative effect of perceived privacy risk on willingness to disclose personal information due to the expectation of losses (Li et al., 2010).

Users may realize that posting their personal information on Facebook could have negative consequences. Once an individual posts content about himself or herself on Facebook, it is put toward a risk of the content flowing over the Internet. Facebook users face the risk of personal losses from their content being misused once it is disclosed on the website. These repercussions can be avoided through the use of Facebook privacy controls. The higher the perceived privacy risk, the higher the perceived cost of not using privacy controls. Therefore,

H12. Privacy risk is positively related to the perceived cost of not using privacy controls.

4.3.2.4. Privacy intrusion. Privacy intrusion is defined as invasive acts disturbing an individual's privacy by involving undesirable interference of another's presence or activities (Solove, 2006; Xu et al., 2008). Intrusion requires protection as it has been found to create discomfort and harm to individuals (Xu et al., 2008). People who perceive the possibility of the invasion of their privacy may be willing to take actions that induce protection against it. Facebook privacy controls are an example of protection against the intrusion of users' privacy. The higher the perceived privacy intrusion, the higher the perceived cost of not using privacy controls. Therefore,

H13. Privacy intrusion is positively related to the perceived cost of not using privacy controls.

4.3.3. Drivers of the cost of using privacy controls

We model two outcome beliefs that drive an individual's assessment of the cost associated with following the course of action. These are (i) intrinsic cost and (ii) work impediment.

4.3.3.1. Intrinsic cost. Intrinsic cost is defined as an individual's negative feelings such as stress, guilt, shame, and embarrassment due to the consequence of using privacy controls. Self-imposed punishment in the form of embarrassment and shame can motivate employees to refrain from corporate crimes (Bulgurcu et al., 2010; Paternoster & Simpson, 1996). Users may feel that using privacy controls can make others think that they have something to hide or do not have enough to share. For this reason, users could feel negatively about controlling how their content is shared, accessed, and used on Facebook. Intrinsic cost is therefore a downside of using Facebook privacy controls for many individuals. The

Table 1
Measurement items.

Construct	Items
Attitude	Using privacy controls available on Facebook is ___ • Unnecessary (*strongly disagree/strongly agree*) • Important (*strongly disagree/strongly agree*) • Good (*strongly disagree/strongly agree*)
Benefit using privacy control	Using privacy controls available on Facebook would_______ • Be favorable to me (*Not at all/very much*) • Result in benefit s to me (*Not at all/very much*) • Create advantages for me. (*Not at all/very much*)
Cost not using privacy control	If I do not use privacy controls available on Facebook • It would impact me negatively (*Not at all/very much*) • It would create disadvantages for me (*Not at all/very much*) • It would generate losses for me (*Not at all/very much*)
Cost using privacy control	Using privacy controls available on Facebook is _____ for me • Time consuming (*Not at all/very much*) • Burdensome (*Not at all/very much*) • Costly (*Not at all/very much*)
Intention	I intend to use privacy controls on Facebook to _____________ in the future • Selectively block people from interacting with me or seeing my information on Facebook. (*strongly disagree/strongly agree*) • Control who can see the photos and videos I am tagged in that appear on my profile (*strongly disagree/strongly agree*) • Control whether things I've specifically chosen to share with everyone show up in searches on and off Facebook. (*strongly disagree/strongly agree*)
Intrinsic benefit	My use of privacy control on Facebook would make me feel ____: • Satisfied (*Not at all/very much*) • Comfortable (*Not at all/very much*) • Clever (*Not at all/very much*)
Intrinsic Cost	My use of privacy control on Facebook could reflect that I have ___: • A negative social approach (*Not at all/very much*) • Things to hide (*Not at all/very much*) • Not much to show (*Not at all/very much*)
PBC	• If I want to, I can use privacy controls available on Facebook (*strongly disagree/strongly agree*) • Using privacy controls available on Facebook is entirely up to me (*strongly disagree/strongly agree*) • Taking the necessary steps to protect the privacy of my personal information on Facebook is entirely under my control (*strongly disagree/strongly agree*)
Privacy intrusion	I feel that as a result of personal information posted on Facebook,_____ • Others could know more than I am comfortable with (*Not at all/very much*) • The information about me that I consider private could be more readily available to others than I would want to (*Not at all/very much*) • The information about me out there, if used, could invade my privacy (*Not at all/very much*)
Privacy risk	• In general, it would be risky to post personal information on Facebook (*strongly disagree/strongly agree*) • Personal information posted on Facebook could be inappropriately used (*strongly disagree/strongly agree*) • Posting personal information on Facebook could involve many unexpected problems (*strongly disagree/strongly agree*)
Resource safety	• Using privacy controls available on Facebook would_______ • Enhance safety of my personal information (*not at all/very much*) • Protect my personal information (*not at all/very much*) • Reduce the risk of potential misuse of my personal information (*not at all/very much*) • Reduce potential problems associated with the misuse of my personal information (*not at all/very much*)
Resource vulnerability	If I do not use privacy controls available on Facebook, _____ • My posted information will be at risk (*not at all/very much*) • My posted information can be exploited (*not at all/very much*) • My posted information can be misused (*not at all/very much*)
Response efficacy	• Privacy controls available on Facebook works for information protection (*strongly disagree/strongly agree*) • Privacy controls available on Facebook are effective for information protection (*strongly disagree/strongly agree*) • When using privacy controls available on Facebook, my information is more likely to be protected (*strongly disagree/strongly agree*)
Social norm	_______would think that I should use privacy controls on Facebook • My friends (*strongly disagree/strongly agree*) • My family (*strongly disagree/strongly agree*) • People important to me who use Facebook (*strongly disagree/strongly agree*)
Threat severity	• If my information posted on my Facebook account is misused, its effect would be severe (*strongly disagree/strongly agree*) • If my information posted on my Facebook account is misused, its effect would be serious (*strongly disagree/strongly agree*) • If my information posted on my Facebook account is misused, its effect would be significant (*strongly disagree/strongly agree*)
Work impediment	Using privacy controls available on Facebook would_______ • Hold me back from using Facebook effectively (*not at all/very much*) • Hinder my use of Facebook (*not at all/very much*) • Restrict my use of Facebook (*not at all/very much*)

higher the intrinsic cost, the higher the perceived cost of using privacy controls. Therefore,

H14. Intrinsic cost is positively related to the perceived cost of using privacy controls.

4.3.3.2. Work Impediment. Work impediment is defined as a detriment to an individual's tasks and activities resulting from using privacy controls. Complying with security policies that conflict with the employee's primary tasks and hinders his or her work is associated with the cost of complying with such policies (Paternoster & Simpson, 1996). Individuals post and share their content in order to enjoy the social networking experience on Facebook. In some cases, if individuals use privacy controls to limit their information, they might not be able to get connected with their old friends or find new friends. Therefore, work impediment is a cost of using privacy controls. The higher the work impediment, the higher the cost of using privacy controls. Therefore,

H15. Work impediment is positively related to the perceived cost of using privacy controls.

5. Research methodology

5.1. Sample & data collection

We collected data by drawing a sample from accessible population of undergraduate students in a north-eastern public college in the United States. The use of students as subjects is a common practice across various domains and is pertinent to the subject matter of this research, since teenagers and young adults compose the majority of Facebook users (Christofides et al., 2009).

Out of 282 surveys that were distributed in the classes, 261 (92.5%) of them were completed and returned. Response to the filter questions allowed us to confirm students' use of Facebook before analysis and 5 surveys in which respondents claimed to be non-users of Facebook were removed from the dataset. Seven surveys with more than 5 missing values were also removed, thereby resulting in 249 (88.3%) usable responses. We achieved a high response rate as the sample frame was carefully selected and based on relevance to research goals, the anticipated importance of the survey content to respondents was high.[1]

The respondents were almost equally distributed in terms of gender, with 135 males (54.2%) and 112 females (45%). In terms of age, 131 (52.6%) respondents were between the age of 18 and 20, while 82 (33%) were between 21 and 23 years. There were 81 freshmen, 33 sophomores, 53 juniors and 80 seniors. The respondents' main uses for Facebook included keeping in touch with people, showing others pictures, publicizing events and news, and informing family members and friends about changes in life.

5.2. Measures

We adapted existing validated items from prior studies where possible and made minor modifications to fit the context of our study by using standard scale development procedures (Boudreau, Gefen, & Straub, 2001). In our survey, privacy controls on Facebook were referred to as the settings one can choose to control which people and apps can see users' information on Facebook.

The items for constructs were adapted with the help of validated items from literature whenever possible by making minor changes to fit the context of our study. The measures for attitude, intention, benefit of using privacy controls, cost of using privacy controls, cost of not using privacy controls, intrinsic benefit, intrinsic cost, resource safety, resource vulnerability, and work impediment were adopted from Bulgurcu et al. (2010). The questions for social norm and perceived behavioral control (PBC) were adopted from Taylor and Todd (1995) and Ajzen, Joyce, Sheikh, and Cote (2011). The measures for privacy intrusion and privacy risk were adopted from Xu et al. (2008), and the items for response efficacy and threat severity were derived from Johnston and Warkentin (2010). All items were measured using a seven-point Likert scale. Filter questions were used in the survey to determine if the respondents used Facebook or not to determine their participation eligibility.

The instrument was tested for content validity by getting feedback from two faculty and five students not involved in the study to ensure that the instrument was not vague, and respondents easily comprehended the questions. They were also asked to indicate whether these measurement items needed to be deleted or reworded and if any new items should be added. Next, a pilot study was conducted to improve the psychometric properties of the instrument by administering the survey to 20 students using the same procedure that was subsequently used for the main study. The actual items used in the research along with their constructs are shown in Table 1.

6. Data analysis and results

We conducted Partial Least Square (PLS) analysis to validate our model. Using Smart-PLS (Ringle, Wende, & Will, 2005), we first examined our measurement model to evaluate the validity and reliability of the measurement items. Then we examined the structural model to evaluate the significance for each of the hypotheses.

6.1. Measurement model

We used the thresholds suggested in the literature to assess the validity and reliability. As shown in Table 2, internal consistency of the items was ascertained by seeing that the composite reliabilities were above the threshold of 0.70 (Hair, Black, Babin, Anderson, & Tatham, 2006; Hulland, 1999) and Cronbach's alpha for all constructs was above 0.70 (Hair et al., 2006). Also, the average vari-

Table 2
Psychometric properties for constructs.

	AVE (threshold 0.5)	Composite reliability (threshold 0.7)	Cronbachs alpha (threshold 0.7)
Attitude	0.65	0.85	0.73
Benefit using privacy control	0.83	0.94	0.90
Cost not using privacy control	0.89	0.96	0.94
Cost using privacy control	0.77	0.91	0.84
Intention	0.77	0.91	0.86
Intrinsic benefit	0.80	0.92	0.88
Intrinsic cost	0.75	0.90	0.84
PBC	0.70	0.88	0.80
Privacy intrusion	0.83	0.93	0.90
Privacy risk	0.82	0.93	0.89
Resource safety	0.83	0.95	0.93
Resource vulnerability	0.88	0.96	0.93
Response efficacy	0.79	0.92	0.87
Social norm	0.72	0.89	0.82
Threat severity	0.88	0.96	0.93
Work impediment	0.89	0.96	0.94

[1] We wish to thank the reviewer for this insight.

Table 3
Loadings and cross loadings.

	Attitude	Benefit using	Cost not using	Cost using	Intent	Intrin benefit	Intrin cost	PBC	Privacy intr	Privac risk	Res safty	Res vuln	Resp effic	SN	Threat sev	Work imp
Attitude-01	**0.797**	0.472	0.258	−0.388	0.291	0.480	−0.182	0.314	0.194	0.275	0.351	0.274	0.334	0.400	0.053	−0.221
Attitude-02	**0.743**	0.354	0.299	−0.260	0.325	0.271	−0.181	0.032	0.166	0.181	0.124	0.296	0.016	0.260	0.131	−0.277
Attitude-03	**0.871**	0.397	0.356	−0.205	0.441	0.463	−0.078	0.115	0.315	0.370	0.284	0.417	0.092	0.381	0.149	−0.172
Benefits using-01	0.506	**0.904**	0.312	−0.231	0.319	0.474	−0.222	0.258	0.371	0.160	0.671	0.385	0.374	0.367	0.090	−0.368
Benefits using-02	0.453	**0.940**	0.262	−0.228	0.257	0.452	−0.154	0.232	0.389	0.200	0.587	0.339	0.357	0.345	0.110	−0.263
Benefits using-03	0.428	**0.894**	0.267	−0.268	0.225	0.457	−0.194	0.225	0.273	0.176	0.552	0.258	0.380	0.326	0.039	−0.288
Cost not using-01	0.370	0.297	**0.943**	−0.106	0.253	0.326	−0.125	0.068	0.344	0.344	0.210	0.481	0.006	0.427	0.402	−0.187
Cost not using-02	0.354	0.316	**0.951**	−0.139	0.227	0.303	−0.099	0.036	0.338	0.358	0.249	0.443	0.054	0.457	0.340	−0.160
Cost not using-03	0.346	0.260	**0.941**	−0.145	0.224	0.317	−0.072	0.007	0.306	0.318	0.198	0.409	0.003	0.441	0.373	−0.165
Cost using-01	−0.259	−0.211	−0.088	**0.906**	−0.015	−0.196	0.310	−0.211	−0.048	−0.197	−0.144	−0.077	−0.208	−0.183	−0.024	0.283
Cost using-02	−0.333	−0.232	−0.116	**0.924**	−0.085	−0.219	0.296	−0.261	−0.027	−0.168	−0.173	−0.079	−0.284	−0.187	−0.013	0.320
Cost using-03	−0.333	−0.249	−0.154	**0.789**	−0.160	−0.234	0.295	−0.304	−0.047	−0.130	−0.309	−0.097	−0.243	−0.136	0.040	0.270
Intention-01	0.352	0.231	0.262	−0.109	**0.844**	0.299	−0.074	0.133	0.249	0.188	0.154	0.265	0.067	0.293	0.153	−0.194
Intention-02	0.435	0.255	0.182	−0.095	**0.909**	0.343	−0.070	0.217	0.215	0.205	0.248	0.296	0.119	0.366	0.103	−0.149
Intention-03	0.359	0.293	0.225	−0.062	**0.886**	0.310	−0.079	0.113	0.273	0.190	0.246	0.300	0.066	0.346	0.196	−0.214
IntrinsicBenefits-01	0.518	0.468	0.329	−0.253	0.363	**0.943**	−0.129	0.279	0.317	0.239	0.411	0.258	0.424	0.414	0.153	−0.306
IntrinsicBenefits-02	0.490	0.535	0.327	−0.248	0.362	**0.935**	−0.203	0.265	0.360	0.225	0.434	0.294	0.392	0.387	0.182	−0.308
IntrinsicBenefits-03	0.326	0.313	0.221	−0.143	0.218	**0.803**	0.021	0.179	0.288	0.234	0.230	0.134	0.297	0.345	0.171	−0.241
IntrinsicCost-01	−0.177	−0.201	−0.166	0.354	−0.091	−0.155	**0.905**	−0.152	0.009	0.010	−0.205	−0.104	−0.151	−0.208	0.116	0.252
IntrinsicCost-02	−0.193	−0.198	−0.079	0.273	−0.129	−0.113	**0.874**	−0.090	−0.011	0.023	−0.137	−0.101	−0.069	−0.154	0.113	0.191
IntrinsicCost-03	−0.092	−0.140	−0.003	0.254	0.012	−0.074	**0.825**	−0.173	0.053	0.090	−0.092	−0.021	−0.088	−0.092	0.124	0.156
PBC-01	0.233	0.222	0.001	−0.264	0.157	0.291	−0.093	**0.859**	0.019	0.099	0.246	0.077	0.526	0.226	−0.109	−0.052
PBC-02	0.144	0.241	0.079	−0.228	0.184	0.190	−0.174	**0.915**	0.062	0.042	0.222	0.149	0.455	0.229	−0.019	−0.054
PBC-03	0.107	0.197	0.001	−0.293	0.090	0.234	−0.135	**0.732**	−0.061	−0.006	0.238	0.016	0.588	0.135	−0.080	−0.187
PrivacyIntrusion-01	0.256	0.336	0.310	−0.064	0.263	0.308	0.052	0.036	**0.877**	0.258	0.251	0.320	0.104	0.297	0.330	−0.203
PrivacyIntrusion-02	0.244	0.349	0.306	−0.024	0.253	0.356	0.017	0.020	**0.941**	0.292	0.266	0.406	0.045	0.304	0.355	−0.266
PrivacyIntrusion-03	0.268	0.348	0.334	−0.037	0.236	0.323	−0.017	0.011	**0.909**	0.357	0.231	0.406	0.012	0.359	0.394	−0.220
PrivacyRisk-01	0.341	0.194	0.352	−0.156	0.217	0.246	0.040	−0.006	0.209	**0.881**	0.075	0.301	−0.022	0.303	0.295	−0.058
PrivacyRisk-02	0.298	0.163	0.284	−0.197	0.187	0.178	0.012	0.079	0.350	**0.908**	0.076	0.341	−0.038	0.211	0.354	-0.155
PrivacyRisk-03	0.297	0.171	0.333	−0.163	0.195	0.263	0.058	0.102	0.361	**0.928**	0.090	0.344	0.017	0.244	0.390	−0.127
ResourceSafety-01	0.297	0.565	0.230	−0.210	0.241	0.347	−0.165	0.213	0.275	0.105	**0.849**	0.211	0.373	0.314	0.036	−0.226
ResourceSafety-02	0.259	0.608	0.187	−0.225	0.222	0.398	−0.163	0.256	0.266	0.043	**0.934**	0.127	0.465	0.216	−0.003	−0.252
ResourceSafety-03	0.313	0.620	0.197	−0.227	0.217	0.398	−0.146	0.238	0.229	0.079	**0.941**	0.147	0.491	0.215	−0.039	−0.219
ResourceSafety-04	0.303	0.627	0.233	−0.213	0.230	0.374	−0.159	0.288	0.233	0.100	**0.923**	0.185	0.489	0.225	−0.003	−0.232
ResourceVuln-01	0.426	0.361	0.434	−0.071	0.329	0.270	−0.113	0.128	0.386	0.336	0.200	**0.902**	0.022	0.439	0.297	−0.150
ResourceVuln-02	0.366	0.337	0.414	−0.109	0.296	0.237	−0.097	0.119	0.387	0.334	0.154	**0.958**	−0.012	0.377	0.265	−0.140
ResourceVulny-03	0.361	0.319	0.474	−0.093	0.295	0.249	−0.049	0.068	0.397	0.348	0.160	**0.953**	−0.035	0.347	0.288	−0.134
ResponseEfficacy-01	0.172	0.344	0.015	−0.233	0.096	0.351	−0.027	0.597	0.082	0.028	0.427	−0.008	**0.898**	0.113	−0.133	−0.175
ResponseEfficacy-02	0.182	0.395	0.024	−0.270	0.120	0.403	−0.136	0.519	0.043	−0.014	0.453	−0.021	**0.922**	0.133	−0.186	−0.177
ResponseEfficacy-03	0.151	0.340	0.019	−0.249	0.043	0.366	−0.164	0.475	0.032	−0.054	0.458	0.005	**0.851**	0.089	−0.175	−0.150
SN-01	0.338	0.295	0.394	−0.134	0.422	0.320	−0.093	0.179	0.253	0.227	0.172	0.315	0.077	**0.894**	0.174	−0.132
SN-02	0.381	0.307	0.378	−0.165	0.229	0.344	−0.206	0.250	0.326	0.232	0.259	0.365	0.130	**0.773**	0.195	−0.217
SN-03	0.423	0.392	0.433	−0.217	0.269	0.457	−0.210	0.221	0.362	0.276	0.284	0.406	0.139	**0.876**	0.231	−0.193
ThreatSeverity-01	0.138	0.079	0.365	0.034	0.129	0.198	0.129	−0.074	0.358	0.355	0.004	0.261	−0.176	0.208	**0.942**	−0.059
ThreatSeverity-02	0.070	0.053	0.350	0.001	0.136	0.158	0.134	−0.028	0.360	0.374	−0.028	0.267	−0.160	0.192	**0.958**	−0.060
ThreatSeverity-03	0.171	0.112	0.388	−0.030	0.199	0.169	0.115	−0.105	0.392	0.343	0.012	0.318	−0.183	0.239	**0.910**	−0.065
WorkImpediment-01	−0.281	−0.334	−0.167	0.304	−0.254	−0.310	0.203	−0.090	−0.226	−0.125	−0.248	−0.102	−0.164	−0.185	−0.073	**0.938**
WorkImpediment-02	−0.266	−0.330	−0.170	0.331	−0.172	−0.290	0.240	−0.055	−0.243	−0.092	−0.244	−0.128	−0.195	−0.197	−0.051	**0.962**
WorkImpediment-03	−0.231	−0.291	−0.176	0.311	−0.163	−0.313	0.222	−0.124	−0.246	−0.130	−0.229	−0.196	−0.172	−0.181	−0.064	**0.931**

Note: Loading values greater than 0.7 are shown in bold.

Table 4
Correlation matrix and average variance extracted for principal constructs.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Attitude	**0.805**															
2	Benefit using privacy control	0.508	**0.913**														
3	Cost not using privacy control	0.378	0.308	**0.945**													
4	Cost using privacy control	−0.354	−0.265	−0.137	**0.875**												
5	Intention	0.438	0.294	0.249	−0.100	**0.880**											
6	Intrinsic Benefit	0.509	0.506	0.334	−0.248	0.362	**0.896**										
7	Intrinsic Cost	−0.181	−0.209	−0.106	0.344	−0.084	−0.136	**0.869**									
8	PBC	0.197	0.262	0.040	−0.297	0.180	0.275	−0.159	**0.839**								
9	Privacy Intrusion	0.282	0.379	0.349	−0.046	0.276	0.362	0.018	0.024	**0.910**							
10	Privacy Risk	0.346	0.196	0.360	−0.188	0.222	0.256	0.042	0.062	0.334	**0.906**						
11	Resource Safety	0.321	0.664	0.232	−0.240	0.249	0.416	−0.173	0.273	0.274	0.089	**0.912**					
12	Resource Vulnerability	0.409	0.361	0.472	−0.097	0.327	0.269	−0.091	0.111	0.416	0.362	0.183	**0.938**				
13	Response Efficacy	0.190	0.406	0.022	−0.282	0.099	0.420	−0.123	0.594	0.058	−0.015	0.500	−0.010	**0.891**			
14	Social Norm	0.435	0.380	0.467	−0.193	0.383	0.426	−0.181	0.243	0.353	0.282	0.264	0.412	0.126	**0.849**		
15	Threat Severity	0.137	0.088	0.394	0.001	0.167	0.187	0.134	−0.075	0.396	0.381	−0.003	0.303	−0.185	0.228	**0.937**	
16	Work Impediment	−0.275	−0.338	−0.181	0.334	−0.207	−0.322	0.236	−0.094	−0.253	−0.122	−0.255	−0.150	−0.188	−0.199	−0.066	**0.944**

Note: The diagonal element (in bold) represents the square root of the AVE

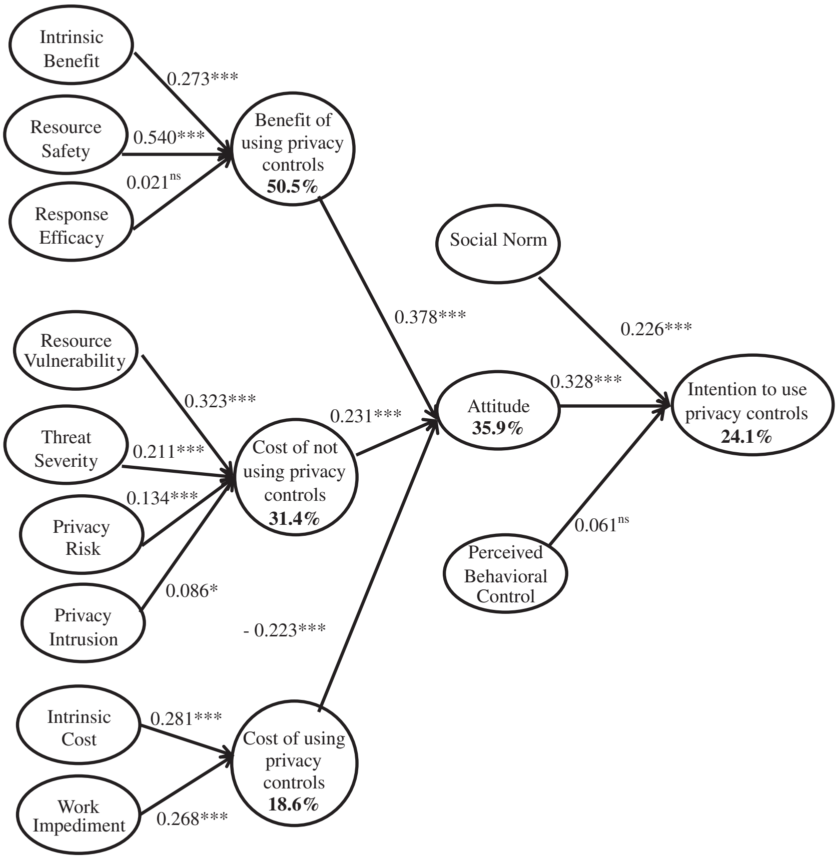

Fig. 3. Structural model analysis.

ance extracted (AVE) for all constructs was above 0.50 (Fornell & Larcker, 1981), thereby demonstrating the convergent validity.

Following Gefen and Straub (2005), discriminant validity was ascertained by evaluating that (i) the loading of an indicator on its assigned latent variable was higher (greater than 0.7) than its loading on all other latent variables (Table 3), and (ii) the square root of the construct's AVE was larger than its correlations with other constructs (Table 4). The results confirmed the discriminant validity of the items.

Overall, we were able to ascertain the psychometric properties of the items, thereby allowing us to test our proposed structural model.

6.2. Structural model

In this study, we build the PLS structural model in SmartPLS and used path coefficients to test our hypotheses and R square value to evaluate the explanatory power of the model (Pi, Chou, & Liao, 2013). The bootstrapping method with 1000 samples was used to compute the test statistic (t-values) for determining the significance of path coefficients and test the hypotheses. The significance of the coefficient can be reached in different levels with different t-values for a one-tail test as direction is specified in the hypotheses ($p < 0.01$ when $t > 1.96$; $p < 0.05$ when $t > 1.64$; $p < 0.10$ when $t > 1.28$).

Table 5
Path coefficient analysis.

		Coefficient	Standard error	T-statistic
H1	Attitude → intention	0.328	0.104	3.147***
H2	Social norm → intention	0.226	0.078	2.908***
H3	Perceived behavioral control → intention	0.061	0.059	1.035ns
H4	Benefit of using privacy control → attitude	0.378	0.066	5.734***
H5	Cost of not using privacy control → attitude	0.231	0.060	3.834***
H6	Cost of using privacy control → attitude	−0.223	0.068	3.261***
H7	Intrinsic benefit → benefit of using privacy control	0.273	0.064	4.291***
H8	Resource safety → benefit of using privacy control	0.540	0.076	7.123***
H9	Response efficacy → benefit of using privacy control	0.021	0.044	0.480ns
H10	Resource vulnerability → cost of not using privacy control	0.323	0.084	3.864***
H11	Threat severity → cost of not using privacy control	0.211	0.064	3.280***
H12	Perceived privacy risk → cost of not using privacy control	0.134	0.069	1.934**
H13	Perceived privacy intrusion → cost of not using privacy control	0.086	0.059	1.454*
H14	Intrinsic cost → cost of using privacy control	0.281	0.079	3.389***
H15	Work impediment → cost of using privacy control	0.268	0.069	4.092***

*** Significant at $p < 0.01$.
** Significant at $p < 0.05$.
* Significant at $p < 0.1$.
ns Not significant.

The proposed research model was found to explain 24.1% of the variance for intention, 35.9% of the variance for attitude, 50.5% for the benefit of using privacy controls, 31.4% for the cost of not using privacy controls, and 18.6% for the cost of using privacy controls. Fig. 3 shows the results of structural model analysis with significance level highlighted next to the path coefficients.

The relationship between attitude and intention was found to be significant ($\beta = 0.328$, $t = 3.147$, $p < 0.01$), verifying hypothesis 1. The relationship between social norm and intention was found to be significant ($\beta = 0.226$, $t = 2.908$, $p < 0.01$), verifying hypothesis 2. However, the relationship between perceived behavioral control and intention was found to be non-significant ($\beta = 0.061$, $t = 1.035$), implying that hypothesis 3 was not supported.

The relationship between benefit of using privacy controls and attitude was found to be significant ($\beta = 0.378$, $t = 5.734$, $p < 0.01$), verifying hypothesis 4. The relationship between cost of not using privacy controls and attitude was found to be significant ($\beta = 0.231$, $t = 3.834$, $p < 0.01$), verifying hypothesis 5. The relationship between cost of using privacy controls and attitude was found to be significant ($\beta = -0.223$, $t = 3.261$, $p < 0.01$), verifying hypothesis 6.

The relationship between intrinsic benefit and benefit of using privacy controls was found to be significant ($\beta = 0.273$, $t = 4.291$, $p < 0.01$), verifying hypothesis 7. The relationship between resource safety and benefit of using privacy controls was found to be significant ($\beta = 0.540$, $t = 7.123$, $p < 0.01$), verifying hypothesis 8. The relationship between response efficacy and benefit of using privacy controls was found to be non-significant ($\beta = 0.021$, $t = 0.480$), implying that hypothesis 9 was not supported.

The relationship between resource vulnerability and cost of not using privacy controls was found to be significant ($\beta = 0.323$, $t = 3.864$, $p < 0.01$), verifying hypothesis 10. The relationship between threat severity and cost of not using privacy controls was found to be significant ($\beta = 0.211$, $t = 3.280$, $p < 0.01$), verifying hypothesis 11. The relationship between perceived privacy risk and cost of not using privacy controls was found to be significant ($\beta = 0.134$, $t = 1.934$, $p < 0.05$), verifying hypothesis 12. The relationship between perceived privacy intrusion and cost of not using privacy controls was found to be significant ($\beta = 0.086$, $t = 1.454$, $p < 0.1$), verifying hypothesis 13.

The relationship between intrinsic cost and cost of using privacy controls was found to be significant ($\beta = 0.281$, $t = 3.389$, $p < 0.01$), verifying hypothesis 14. The relationship between work impediment and cost of using privacy controls was found to be significant ($\beta = 0.268$, $t = 4.092$, $p < 0.01$), verifying hypothesis 15.

The result of our structural model analysis shows support for all hypotheses except H3 & H9. Table 5 summarizes the results of path coefficient analysis.

7. Conclusions

7.1. Discussions

This study investigates the rationality-based beliefs affecting individual's attitudes and intention to use privacy controls available on Facebook. We adopted Bulgurcu's ISP compliance model in the context of Facebook privacy controls to develop and test a model that further theorizes salient beliefs about outcomes of using or not using privacy controls available on Facebook. While Bulgurcu's study pertains to adoption of a behavior (ISP compliance) which, depending on the organization, could be mandatory or not strictly mandatory, and whose effect impacts organization's resources, our research focuses on adoption of a behavior (using Facebook privacy controls) which is entirely voluntary, completely under users' discretion, and whose effect impacts an individual's own information resources.

The results of our study show that intention to use Facebook privacy controls depends on attitude and social norm, and attitude is driven by an individual's beliefs regarding the benefits of using, cost of using, and cost of not using privacy controls available on Facebook. Contrary to the theory of planned behavior, our results indicate that the relationship between perceived behavioral controls and intention was not significant. A possible explanation for this finding is that individuals realize that if they want to use privacy controls mechanisms available on Facebook, they are capable of using if they desire.

Attitude was found to exert the strongest effect on intention followed by the social norm. It shows that the use of privacy controls as positively valued was found to be an important factor in influencing individuals' intentions to use privacy controls. Use of Facebook to connect with friends is often based on common interests with individuals sharing information with each other (Pempek et al., 2009). It can be concluded from this study that the users are more likely to use privacy controls if it is considered acceptable to their referent groups. This finding is in contrast with Venkatesh et al. (2003) who found that social norms influence intention only when it is mandatory (not voluntary) to adopt the system. Our finding is consistent with the theory of planned behavior (Fishbein & Ajzen, 1975) and shows that social norms are an important aspect of hedonic systems like Facebook. Individuals tend to make attempts at fitting in with others, and so they tend to do what is expected of them. On the other hand, if friends and family members expect them to freely share information and not use privacy controls to restrict the information, they are less likely to use privacy controls. It is therefore important for individuals to not only utilize privacy controls, but also to encourage their friends to do so because in the absence of privacy controls, their personal information (photos, etc.) available on their friends' unprotected Facebook account could be compromised.

Our results indicate that the benefit of using privacy controls exerts the strongest effect on attitude followed by the cost of not using privacy controls and next by the cost of using privacy controls. As users are likely to perform a cost-benefit analysis, it is therefore important to emphasize to them the advantages for using and also the disadvantages of not using privacy controls on Facebook. Additionally, it may be important to describe how the advantages for using outweigh any disadvantages of using privacy controls.

The results provide support for a negative relationship between the cost of using privacy controls and attitude. Some users may feel that there is more annoyance and confusion involved in spending time to understand and configure privacy settings on Facebook (Brandtzæg et al., 2010). Also, the use of privacy controls could lead to the loss of enjoyment of Facebook use (Thambusamy, Church, Nemati, & Barrick, 2010) as users might not be able to connect to people or use the app which they like using. Enjoyment is an important factor contributing to a website's success and also the use of Facebook (Paris, Lee, & Seery, 2010). Hence, the results suggest that if it is not burdensome to use privacy controls, or it does not require much time, the individual will form a favorable attitude toward the use of privacy controls. Therefore, if an individual experiences less unfavorable consequences for using privacy controls, the individual will have favorable perception toward the use of privacy controls.

The major conclusion of this study is determining a series of salient beliefs about outcomes that can drive an individual's beliefs about the overall assessment of consequences of using or not using Facebook privacy controls. The findings indicate that the safety of resources exerts the strongest effect on the benefit of using privacy controls followed by the intrinsic benefit of the use of privacy controls. It shows that usability of Facebook privacy controls depends upon whether it ensures safety by limiting the risk of harm to stored information (Braz, Seffah, & M'Raihi, 2007). Also, the individuals who feel comfortable and satisfied knowing that they are able to control who can see their information due to the use of privacy controls will acknowledge the benefits of using privacy controls.

Our findings indicate that resource vulnerability has a strong positive relationship with the cost of not using privacy controls, followed by threat severity, privacy risk, and privacy intrusion. As Facebook allows the members little control over who may eventually see material they have posted in the absence of privacy controls (MacDonald et al., 2010), a high level of vulnerability is engendered as individuals post their information which can be exploited (Debatin et al., 2009). Individuals who believe that their posted information could be exploited or misused if they do not use privacy controls understand the possibility of high unfavorable consequences for not using privacy controls.

Privacy issues are found to affect how adults disclose information and open their profiles (Walrave et al., 2012) and Facebook has been found for being used as a medium for knowing where an individual lives (Fogel & Nehmad, 2009), stalking (Chaulk & Jones, 2011), etc. An individual who feels that he or she would be severely or seriously impacted by the misuse of information posted on Facebook will associate high unfavorable consequences for not using privacy controls. Prior literature has found that perceived risk determines whether users are willing to disclose personal information on social networking sites (Li et al., 2010; Lo, 2010). If an individual believes that it is risky to post personal information on Facebook because it can be inappropriately misused, or he or she could get into unexpected problems, such a person will associate high unfavorable consequences for not using privacy controls.

One way social networking sites like Facebook are used is through browsing, or passive observation, known as "lurking" (Pempek et al., 2009). Individuals who use Facebook to browse other users' profiles are said to be lurking. Lurkers browse things such as other users' wall posts, pictures, friends' lists, recent activity, current location, and much more. If the users believe that the availability of information on Facebook could intrude his or her privacy, he or she will associate unfavorable consequences with not using privacy controls. Individuals who realize that their profiles can be lurked by others, can use privacy controls to filter out what others can see in their profiles.

The results found evidence that intrinsic cost was more strongly related to the cost of using privacy controls as compared to the work impediment. Negative feelings such as guilt, shame, and embarrassment reduce the possibility that individuals perform a behavior (Tong, Wang, & Teo, 2007). Individuals often use Facebook to share information, to keep up with trends, or to show off their popularity (Waters & Ackerman, 2011). If an individual perceives that the use of privacy controls will imply that the he or she has things to hide, does not have much to show, or is not social because he or she is not sharing information, he or she may feel that there are costs associated with the use of Facebook privacy controls mechanisms.

An individual who believes that the use of privacy controls available on Facebook and not allowing others access to personal information restricts the use of Facebook for his or her intended purposes (Hoadley et al., 2010), will perceive the presence of costs associated with the use of privacy controls. It could be because the individual wants to make new friends or to find a date, but could not do so because other users will not be able to find information about him or her. Since businesses use Facebook to investigate potential employees (Peluchette & Karl, 2009), this finding is especially important for students because they might feel that their prospective employers will not think highly of them if their information availability is blocked on Facebook. It is important to make students realize that the employers could be granted friend access if it is asked by them (Smith & Kidder, 2010).

7.2. Implications

The findings of the current study have important implications for both academics and practitioners. To the best of our knowledge, this is the first study that draws on the rational choice theory and the theory of planned behavior to examine the influence of the consequences of using or not using privacy controls on attitude toward using privacy controls on Facebook. While Bulgurcu's study pertains to adoption of a behavior (ISP compliance) which, depending on the organization, could be mandatory or not strictly mandatory, and has consequences directed toward organization's resources, this study contributes to the academic literature by developing and empirically validating a research model related to adoption of a behavior (use of Facebook privacy controls) which is entirely voluntary, completely under a user's discretion, and has consequences directed toward an individual's own information resources. It next contributes by identifying individuals' salient beliefs about outcomes of using or not using privacy controls available on Facebook. Lastly, it contributes by showing that social norms are an important aspect of using hedonic systems, even though the behavior is entirely voluntary and completely under users' discretion.

Our study indicates that the impact of the cost of using privacy controls on attitude is as strong as the cost of not using privacy controls. The results are similar to Bulgurcu et al. (2010)'s finding regarding the cost of compliance in the context of security policies. It further provides support for the inclusion of the construct related to the cost of conforming to protective behaviors in the information security and online privacy based research. Our results suggest for excluding the construct related to perceived behavior from research focusing on the adoption of technologies commonly used in our daily lives. However, more support for this finding by other studies is needed.

The findings of our study also offer useful insights for practitioners. The results suggest that schools, colleges, and public libraries should develop appropriate awareness programs and training interventions to reinforce individuals' beliefs related to information resource safety, information resource vulnerability, privacy concern, threat severity, privacy intrusion, work impediment, and intrinsic cost associated with the use of privacy controls. As individuals perceive work impediments to be costly, the cost of not using privacy controls and associated repercussions should be reinforced to them. The support for threat severity shows that users are aware of the possibility of varying levels of harm to their personal information. Practitioners can pinpoint common causes of threats to Facebook information, such as Facebook services and apps, and investigate ways to reduce or eliminate the potential harm to personal information required for the services and apps to function. The support for the social norm construct shows that users want to do what other users are doing; therefore, it is important to emphasize that privacy overrules popularity. Practitioners can develop posters and slogans that show users they should not worry about "being cool" and instead practice protective control mechanisms rather than post revealing information about themselves in order to get popular.

7.3. Limitations and future research directions

As with other research, this study also has some limitations and the results should be interpreted accordingly. As we have used a student sample from a north-eastern state college in the United States, the results may have a limited generalizability to other groups. Second, our study design uses cross-sectional data, rather than longitudinal data. Third, we have measured intention to use privacy controls instead of observing actual use. It was not practical to observe how individuals are using privacy controls mechanisms because of the large sample size and privacy related issues. However, these limitations are typical of similar studies done in the past.

One possible direction for future research is to investigate other beliefs that could influence attitudes toward the use of privacy controls, the benefits and costs of using privacy controls, and not using. Also, the role of perceived behavioral control in commonly used technology adoption research needs more scrutiny. Another interesting avenue for future research is to explore the beliefs influencing social norm. As individuals not only post their information, they also share information and pictures about their friends and family on their account which could become available to third parties and compromise the privacy of their friends. A possible research direction would be to investigate the role of morality, values and concern for others' privacy on individual's use of privacy controls on Facebook.

Acknowledgements

We would like to acknowledge our colleagues Anil Singh, George Mangalaraj, Jill Gerhardt, Saralyn Mathis and Tara Ronda for their valuable insights, and many students in our classes who participated in this research.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Proceedings of the 6th Workshop on Privacy Enhancing Technologies* (pp. 36–58). Robinson College, Cambridge, United Kingdom: Springer.

Ajzen, I., Joyce, N., Sheikh, S., & Cote, N. G. (2011). Knowledge and the prediction of behavior: The role of information accuracy in the theory of planned behavior. *Basic and Applied Social Psychology, 33*(2), 101–117.

Bornoe, N., & Barkhuus, L. (2011). Privacy management in a connected world: Students' perception of Facebook privacy settings. In *Proceedings of the ACM conference on Computer Supported Cooperative Work* (pp. 19–23). Hangzhou, China.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151–164.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 1–16.

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

Brandtzæg, P. B., Luders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction, 26*(11–12), 1006–1030.

Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a trade-off between usability and security: A metrics based-model. In *Proceedings of the Human-Computer Interaction–INTERACT 2007* (pp. 114–126). Rio de Janeiro, Brazil: Springer.

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.

Chaulk, K., & Jones, T. (2011). Online obsessive relational intrusion: Further concerns about Facebook. *Journal of Family Violence, 26*(4), 245–254.

Cheung, C. M., Chiu, P.-Y., & Lee, M. K. (2011). Online social networks: Why do students use Facebook? *Computers in Human Behavior, 27*(4), 1337–1343.

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 & Behavior, 12*(3), 341–345.

Cismaru, M., & Lavack, A. M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making. *International Review on Public and Nonprofit Marketing, 3*(2), 9–24.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology, 22*(14), 1111–1132.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108.

Dwyer, C., Hiltz, S.R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the 13th Americas Conference on Information Systems* (pp. 339). Colorado, USA.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143–1168.

Fernandez, P. (2009). Balancing outreach and privacy in Facebook: Five guiding decision points. *Library Hi Tech News, 26*(3/4), 10–12.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160.

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

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*(1), 109.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71–80). Alexandria, VA, USA: ACM.

Guo, Y.Y. (2010). The privacy issue on social network sites: Facebook. *3pm Journal of Digital Research & Publishing*, 83.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., & Tatham, R.L. (2006). *Multivariate data analysis* (6th ed.): New Jersey: Prentice-Hall.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications, 9*(1), 50–60.

Hsu, M.-H., Ju, T. L., Yen, C.-H., & Chang, C.-M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies, 65*(2), 153–169.

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology, 13*(4), 289–302.

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

Hung, S.-Y., Ku, C.-Y., & Chang, C.-M. (2003). Critical factors of WAP services adoption: An empirical study. *Electronic Commerce Research and Applications, 2*(1), 42–60.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.

Joinson, A.N. (2008). Looking at, looking up or keeping up with people? Motives and use of facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1027–1036). Florence, Italy: ACM.

Keller, P. A. (1999). Converting the unconverted: The effect of inclination and opportunity to discount health-related fear appeals. *Journal of Applied Psychology, 84*(3), 403.

Kim, J. H., Kim, M.-S., & Nam, Y. (2010). An analysis of self-construals, motivations, Facebook use, and user satisfaction. *International Journal of Human-Computer Interaction, 26*(11–12), 1077–1099.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1), 79–100.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62.

Lin, H., & Hwang, Y. (2014). Do feelings matter? The effects of intrinsic benefits on individuals' commitment toward knowledge systems. *Computers in Human Behavior, 30*, 191–198.

Liu, Y., Gummadi, K.P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In *Proceedings of the Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 61–70). Berlin, Germany: ACM.

Lo, J. (2010). Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites. In *Proceedings of the 16th Americas Conference on Information Systems* (pp. 110). Lima, Peru.

Lo, J., & Riemenschneider, C. (2010). An examination of privacy concerns and trust entities in determining willingness to disclose personal information on a social networking site. In *Proceedings of the 16th Americas Conference of Information Systems*. Lima, Peru.

MacDonald, J., Sohn, S., & Ellis, P. (2010). Privacy, professionalism and Facebook: A dilemma for young doctors. *Medical Education, 44*(8), 805–813.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 2*(3), 173–191.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, 54–61.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366–2375.

Nagle, F., & Singh, L. (2009). Can friends be trusted? Exploring privacy in online social networks. In *Proceedings of the 2009 Advances in Social Network Analysis and Mining* (pp. 312–315). IEEE: Athens, Greece.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior, 26*(3), 406–418.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences* (pp. 156b–156b). Hawaii, USA: IEEE.

Paris, C. M., Lee, W., & Seery, P. (2010). The role of social media in promoting special events: Acceptance of Facebook 'events'. In *Proceedings of the Information and Communication Technologies in Tourism* (pp. 531–541). Lugano, Switzerland: Springer.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*(2), 103–127.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549–583.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 115–143.

Peltier, T.R. (2004). Information security policies and procedures: A practitioner's reference. CRC Press.

Peluchette, J., & Karl, K. (2009). Examining students' intended image on Facebook:"What were they thinking?!". *Journal of Education for Business, 85*(1), 30–37.

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology, 30*(3), 227–238.

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.

Ringle, C.M., Wende, S., & Will, S. (2005). SmartPLS 2.0 (M3) Beta. In. Hamburg.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93–114.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education & Behavior, 2*(4), 328–335.

Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. *Journal of Computer Information Systems, 49*(4).

Smith, W. P., & Kidder, D. L. (2010). You've been tagged!(Then again, maybe not): Employers and Facebook. *Business Horizons, 53*(5), 491–499.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477–564.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590–598.

Taylor, S., & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing, 12*(2), 137–155.

Thambusamy, R., Church, M., Nemati, H., & Barrick, J. (2010). Socially exchanging privacy for pleasure: Hedonic use of computer-mediated social networks. In *Proceedings of the International Conference on Information Systems*. St. Louis, USA.

Tong, Y., Wang, X., & Teo, H.-H. (2007). Understanding the intention of information contribution to online feedback systems from social exchange and motivation crowding perspectives. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (pp. 28-28)*. Hawaii, USA: IEEE.

Van der Heijden, H. (2004). User acceptance of hedonic information systems. *MIS Quarterly*, 695–704.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Viane, I., Crombez, G., Eccleston, C., Devulder, J., & De Corte, W. (2004). Acceptance of the unpleasant reality of chronic pain: Effects upon attention to pain and engagement with daily activities. *Pain, 112*(3), 282–288.

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1).

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(1), 101–115.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–40.

Wigfield, A. (1994). Expectancy-value theory of achievement motivation: A developmental perspective. *Educational Psychology Review, 6*(1), 49–78.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329–349.

Xu, H., Dinev, T., Smith, H.J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the International Conference on Information Systems*. Paris, France.