Computers in Human Behavior 45 (2015) 158–167

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Privacy antecedents for SNS self-disclosure: The case of Facebook

Lili Nemec Zlatolas *, Tatjana Welzer, Marjan Heričko, Marko Hölbl

University of Maribor, Faculty of Electrical Engineering and Computer Science, Smetanova 17, 2000 Maribor, Slovenia

ARTICLE INFO

Article history:
Available online 23 December 2014

Keywords:
Social networking sites (SNSs)
Facebook
Privacy
Self-disclosure

ABSTRACT

In recent years, social networking sites have spread rapidly, raising new issues in terms of privacy and self-disclosure online. For a better understanding of how privacy issues determine self-disclosure, a model which includes privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns and self-disclosure was built. A total of 661 respondents participated in an online survey and a structural equation modeling was used to evaluate the model. The findings indicated a significant relationship between privacy value/privacy concerns and self-disclosure, privacy awareness and privacy concerns/self-disclosure, privacy social norms and privacy value/self-disclosure, privacy policy and privacy value/privacy concerns/self-disclosure, privacy control and privacy value/privacy concerns. The model from the study should contribute new knowledge concerning privacy issues and their shaping of self-disclosure on social networking sites. It could also help networking sites service providers understand how to encourage users to disclose more information.

1. Introduction

Social networking sites (SNSs) have become an important form of communication and have been a topic of interest for researchers in the last few years in a number of disciplines including technology, communications and sociology. SNSs were defined as services where (1) users can form public or semi-public profiles; (2) connect with other users; and (3) view lists of connections of their connections (boyd & Ellison, 2007). The SNS Facebook has all of the above-mentioned features. Users have their public profiles opened or closed, they interact with friends on Facebook and they can see the activities of friends and strangers on Facebook, depending on the openness of the user's profile.

This research addresses privacy issues and self-disclosure on Facebook. Privacy has been defined as a personal boundary regulation process to regulate the levels of privacy with others, depending on the context (Altman, 1975; Laufer & Wolfe, 1977). Self-disclosure was defined as the act of revealing personal information to others (Archer, 1980).

The motivation to start this study is years of interest in privacy issues and disclosure of personal information on SNSs, especially Facebook. Facebook was founded in 2004 and became the most popular SNS in 2009 (Cheung, Chiu, & Lee, 2011; Sheldon, 2008). As of September 2014, Facebook reported having 1.35 billion monthly active users (Facebook.com, 2014), which is about 18% of the world population (Worldometer.info, 2014). With that many people using Facebook every day, it is important to research privacy issues and self-disclosure levels of members of Facebook.

Studies researching privacy issues and self-disclosure on Facebook have already been published, but to the best of our knowledge, no studies examined the complex set of privacy issues and their effect on self-disclosure on Facebook. This study intends to fill this gap in research with a more comprehensive view of privacy and self-disclosure on SNSs by developing a model of relationships between different constructs.

The results of a survey on privacy concerns have shown that the more the users understand how their information is shared on Facebook, the more often they visit the SNS (Staddon, Huffaker, Brown, & Sedley, 2012). Another study has shown that some users are keen on SNSs, but are unfavorable to publishing things on SNSs on their own (McKnight, Lankton, & Tripp, 2011). A study reported that people are very unconfident about changing the privacy settings of their Facebook account and that 95% of frequent users of Facebook have changed their status update at least once a month (boyd & Hargittai, 2010). Another study on Internet users also reported that some users had inaccurate perceptions of their knowledge on privacy (Jensen, Potts, & Jensen, 2005).

Our research aims to establish a connection between privacy-related issues and self-disclosure. A set of constructs was selected for the model developed in this study. Privacy awareness, privacy social norms, privacy policy and privacy control are independent constructs. Privacy awareness measures to which extent users

* Corresponding author. Tel.: +386 2 220 7393; fax: +386 2 220 7272.
E-mail address: lili.nemeczlatolas@um.si (L. Nemec Zlatolas).

http://dx.doi.org/10.1016/j.chb.2014.12.012
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

are informed about privacy problems, violations and procedures in SNSs. Privacy social norms measure how other people or friends influence the users on keeping their information private on SNSs. Privacy policy measures how the users feel how the privacy policy of SNSs reflects the protection of their privacy and confidentiality of their information. Privacy control measures how much control do the users believe they have over who can access information on their profiles.

Constructs that are influenced by the above-mentioned constructs are privacy value, privacy concerns and self-disclosure. Privacy value measures how users feel about privacy, privacy threats and the importance of maintaining their privacy. Privacy concerns measure if the users are concerned about who will have access to the information they put on SNSs. Self-disclosure measures to what extent the users' profiles are filled with their personal information and how much information users reveal on Facebook.

The research model that was developed based on the above-described constructs will examine the relationships between the constructs by using structural equation modeling (SEM). Factor analysis, structural equations (regression) and path analysis are modeled in a picture for a clearer conceptualization in SEM (Byrne, 2010). The purpose of SEM is to assess model fit and the hypotheses of the research. The population of this study were Slovenian users of Facebook, aged between 18 and 65 and the sample was 661 users who filled out an online survey (administered using LimeSurvey).

The contributions of this study will be new knowledge concerning privacy issues and its influence on self-disclosure on SNSs. The study will also help SNSs providers understand how to get their users to disclose more information and inform the media about privacy issues that are important for users when disclosing information on SNSs.

The rest of the paper is organized as follows: Section 2 focuses on a review of existing literature on the subject and a theoretical foundation where selected works on privacy issues and self-disclosure are discussed. Section 3 defines the research model and hypothesis. The constructs used in the model are discussed. Section 4 explains data collection and who the participants of the survey were. It also explains the measures for the model, while Section 5 analyzes the data and presents the results. The paper concludes with Section 6, which includes a discussion and the practical implications of the findings.

2. Literature review and theoretical development

2.1. Privacy, self-disclosure and SNSs

Privacy issues among SNSs have already been the topic of research for many studies. A study done among college students during the early rise of Facebook showed that the social factor (friends having closed profiles) and time spent on SNS (more time) had an influence on more privately set profiles of users on Facebook (Lewis, Kaufman, & Christakis, 2008). Another study explained that the users of Facebook applications misunderstood what data the applications were gathering about them and that users were not always consistent with their privacy concerns (King, Lampinen, & Smolen, 2011). Sahinoglu, Akkaya, and Ang (2012) analyzed privacy and security risks for SNSs users and demonstrated how to manage those risks. Anderson and Stajano (2013) discussed how SNSs come into conflict with privacy, proposing a new architecture in order for users to have better control over their data. In a study by Frampton and Child (2013) participants indicated that mostly they primarily added their coworkers on Facebook, but that it also depended on the participants' privacy management practices. Feng and Xie (2014) found that (1) parents' educational influence, and (2) frequent SNS use are motivators for teens to increase their privacy concerns and disclose less information on Facebook.

Self-disclosure on SNSs has also been researched in the past. Chang and Heo (2014) explored the factors that could influence information disclosure on Facebook, some of the factors being also time spent on Facebook, number of friends, perceived risks, and benefits. Different motives for Facebook use were explained by Special and Li-Barber (2012), some of them being passing time, entertainment and relationship maintenance. Hollenbaugh and Ferris (2014) similarly found factors influencing self-disclosure, some of them being social cohesion, Facebook motives and personality factors. Also Kwak, Choi, and Lee (2014) researched factors influencing self-disclosure on Facebook, some of them being enjoyment, curiosity and time-distortion.

There has been also research done on privacy and self-disclosure on SNSs, but not into the ways that privacy issues affect self-disclosure on Facebook. In the early stages of Facebook, research showed that individuals disclosed information almost irrespective of their privacy concerns (Acquisti & Gross, 2006; Gross & Acquisti, 2005). Kolek and Saunders (2008) found that many students did not have their Facebook accounts protected with restricted access, allowing random people to see their addresses or personal pictures. Another study found that users of Facebook knew how to manage their privacy controls, but were sometimes unaware of who the audience of their published posts will be (Johnson, Egelman, & Bellovin, 2012). Stutzman, Gross, and Acquisti (2012) also conducted privacy and disclosure research over time and explained that users have revealed more information and cared about privacy less within six years' time from the beginning to the end of the research. Taddei and Contena (2013) developed a model where they also indicated the direct effect of privacy concerns on self-disclosure behaviors on Facebook.

2.2. Communications privacy management and SNSs

The theory that was used as a baseline for the formation of the research model is the Communication Privacy Management (CPM) theory proposed by Petronio (2002). CPM defines privacy as the process of opening and closing boundaries to others. First, the ownership of the information is important in CPM, where the co-ownership rights for private information is extended to other users when individuals share their private information. The ownership is only transmitted when the information is shared with the owner's permission, not when it is taken without permission. Secondly, the control of private information is important for individuals in CPM theory, meaning that when individuals disclose information, they want the option of revealing or concealing private information. And thirdly, turbulence in CPM is considered to be when some information that should not be shared, has nevertheless been shared without the owner's permission. In the context of SNSs, users of Facebook can control, who has access to the information they publish and when they publish the information, their friends can also share their information further.

The CPM theory has been primarily used in interpersonal, family and health communications (Petronio & Durham, 2014), but it can also be found in the research of privacy and disclosure on SNSs (Courtney Walton & Rice, 2013; De Wolf, Willaert, & Pierson, 2014; Frampton & Child, 2013; Kisekka, Bagchi-Sen, & Rao, 2013; Lee, Park, & Kim, 2013). In the next section privacy and self-disclosure models are presented, some of them also based on CPM theory.

2.3. Privacy and self-disclosure models

In our study, we have included previous research that was found most suitable for explaining the relationship between privacy issues constructs and self-disclosure on Facebook. During this research, no paper with the same or similar model proposal was found. A summary of variables, user groups and references for all the papers that were thoroughly analyzed before developing the research model is in Table 1.

Dinev and Hart (2004) established the impact of perceived vulnerability and perceived ability to control on perceived privacy concerns, which was further divided into information finding and information abuse. An exploratory factor analysis supported the validity of the measures while a regression model analysis indicated that there is additional space for expanding the model with more constructs while doing further empirical research. The perceived ability to control had a non-significant, while perceived vulnerability had a significant and positive effect on information finding and information abuse, which are both part of perceived privacy concerns.

Xu, Dinev, Smith, and Hart (2008) proposed a model of formation of users privacy concerns – the study examines a complex set of privacy issues and was tested on users of e-commerce, social networking, finance and healthcare websites. The model is based on CPM theory. Partial least squares (PLS) analysis and hypotheses testing revealed 49% of the variance for social networking site users in the model. The model empirically supports the understanding of the formation of an individual's privacy concerns. The direct effects on privacy concerns are the perception of intrusion, privacy risk and privacy control, while the disposition to privacy has a direct effect on all three mentioned constructs. There is also a significant effect for the perceived effectiveness of privacy policy on privacy risk and privacy control. The privacy seal has a non-significant effect on privacy risk and a significantly positive effect on privacy control. Privacy awareness has a non-significant effect, whereas privacy social norms have a significantly positive effect on the disposition for privacy.

A paper on self-disclosure on SNSs by Krasnova, Kolesnikova, and Guenther (2009) presented a SEM model, tested on SNS users. The model indicated the connections between the proposed constructs. The model implied that the users cared about their privacy less than they should and that perceived enjoyment has a significantly positive and privacy concerns have a significantly negative impact on self-disclosure among SNSs. Wu, Huang, Yen, and Popova (2012) similarly researched the effect of online privacy policy on the willingness to provide personal information on websites mediated by consumer's privacy concern and trust. The privacy policy construct was further divided into notice, choice, access, security and enforcement and the impact of all individual connections on online privacy concern and trust was examined. The paper showed relationships between the constructs, also indicating the negative effect of privacy concerns on willingness to provide personal information.

Xu, Gupta, Rosson, and Carroll (2012) measured the information privacy concern of mobile users and developed a model, where the information privacy concern has sub constructs, which are: the secondary use of personal information, perceived surveillance and perceived intrusion. The model confirms that prior privacy experience has a negative impact on information privacy concern and that information privacy concern has a positive effect on behavioral intention, which also measures the disclosure of personal information on mobile applications.

Chen (2013) analyzed privacy self-disclosure behaviors among SNS users and proposed a theoretical model, indicating the impact of extroversion, perceived critical mass and perceived Internet risk on privacy self-disclosure behaviors, mediated by attitude. It also indicates that privacy value reduces the impact of attitude on privacy self-disclosure behaviors.

The model presented in this paper is based on the models in Table 1. When conducting this research we selected privacy awareness, privacy social norms, privacy policy, privacy value, privacy concerns, privacy control and self-disclosure constructs for building our model. These are the constructs that appeared in the described privacy and self-disclosure models often and already indicated some effects between oneself.

The dependent variables self-disclosure in our model have different antecedent variables in the models presented in Table 1 then in our proposed model. The self-disclosure antecedents in the models presented were privacy concerns, trust and attitude. Privacy concerns were indicated to have a significant negative impact on self-disclosure in papers by Krasnova et al. (2009) and Wu et al. (2012). Trust has a significantly positive impact on self-disclosure (Wu et al., 2012) while attitude also has a significantly positive impact on self-disclosure, although it is weakened by privacy value (Chen, 2013).

There are no antecedents for the privacy value variable in researched models whereas our model proposes this variable as a mediator variable. The variable privacy concerns is also a mediator variable in our model and there are different antecedents predicting this variable in researched models. Dinev and Hart (2004) indicated that perceived vulnerability and the ability to control have an impact on privacy concerns. The model by Xu et al. (2008) indicates the positive impact of perception of intrusion and privacy risk and negative impact of privacy control on privacy concerns. Krasnova et al. (2009) indicated the positive impact of perceived likelihood and perceived damage on privacy concerns for SNSs users. Wu et al. (2012) indicated the negative impact of privacy

Table 1
Summary of models on privacy and self-disclosure.

Independent variables	Mediator variables	Dependent variables	Tested on users of	Reference
Perceived vulnerability, perceived ability to control		Perceived privacy concerns (information finding and information abuse)	Internet	Dinev and Hart (2004)
Privacy awareness, privacy social norm, perceived effectiveness of privacy policy, perceived effectiveness of privacy seal	Privacy risk, disposition to privacy[a], privacy control, perception of intrusion	Privacy concerns	Electronic commerce, financial and healthcare websites and SNSs	Xu et al. (2008)
Perceived likelihood, perceived damage, privacy enjoyment	Privacy concerns	Self-disclosure	SNSs	Krasnova et al. (2009)
Privacy policy (notice, choice, access, security, enforcement)	Online privacy concern, trust	Willingness to provide information[b]	Internet	Wu et al. (2012)
Prior privacy experience	Mobile users information privacy concern (secondary use of personal info, perceived surveillance, perceived intrusion)	Behavioral intention	Mobile users	Xu et al. (2012)
Extroversion, perceived critical mass, perceived Internet risk, privacy value	Attitude	Privacy self-disclosure behaviors	SNSs	Chen (2013)

[a] Termed privacy value in our proposed model.
[b] Termed self-disclosure in our proposed model.

policy access, security and enforcement on online privacy concerns, and did not find any significant impact for privacy policy notice and choice on online privacy concerns. Xu et al. (2012) indicated the negative impact of prior privacy experiences on mobile users' information privacy concern.

The independent variables in our model are privacy awareness, privacy social norms, privacy policy and privacy control. The constructs privacy awareness and privacy social norm have no antecedents in analyzed studies, but the latter has significantly positive impact on disposition to privacy (Xu et al., 2008). Privacy policy construct is also explained in the same paper as the perceived effectiveness of privacy policy and has a positive impact on privacy control and negative impact on privacy risk. And privacy control is explained by perceived effectiveness of privacy policy and seal, both having a positive impact on privacy control. Privacy policy construct is also explained by Wu et al. (2012), divided into notice, choice, access, security and enforcement and indicated impact on trust and online privacy concerns.

Our model is based on previously developed models that were tested not only on SNSs users, but also on general Internet users, website users and mobile users. The primary goal of this paper was to develop a model for SNSs users with the analysis of how privacy effects on self-disclosure.

3. Research model and hypotheses

The research model of this study is presented in Fig. 1, and was developed based on previous research on privacy issues and self-disclosure online. It was developed from the CPM theory and models, both presented in the previous section. The constructs selected for this model were selected by frequency of appearance and indicated significance of paths in existing models.

While controlling for gender, age and education, the model in Fig. 1 proposes that privacy awareness, privacy social norms, privacy policy and privacy control have a direct impact on privacy value, privacy concerns and self-disclosure. Furthermore, the model proposes that all four independent variables are interrelated to each other. Moreover, the model also proposes that privacy value and privacy concerns have a direct impact on self-disclosure on Facebook. Below all the constructs in the research model are discussed in more detail, followed by the hypotheses.

3.1. Privacy value

Privacy value is an important topic in SNSs, explaining how users feel about privacy, privacy threats and the importance of maintaining their privacy. A study on information disclosure showed that some users do not worry about posting their personal information, but most users do worry about their identity on Facebook, which also influences their level of self-disclosure (Tow, Dell, & Venable, 2010). Acquisti and Gross (2006) carried out research among undergraduate students and the mean on a 7-point Likert scale for members of Facebook, when asked how concerned they were about threats to their personal privacy, was 4.81 whereas for non-members of Facebook it was 5.41. This implies that, already in the early days of the Facebook site, non-members were more aware of privacy threats, and consequentially had a higher privacy value. Chen (2013) reported that privacy value attenuates the relationship between attitude and privacy self-disclosure behaviors on SNSs.

The literature suggests that privacy value and self-disclosure are two strongly related constructs. Therefore, this study proposes the following hypotheses:

H1. Privacy value has a positive impact on self-disclosure on SNSs.

3.2. Privacy concerns

The privacy concerns construct is a widely used construct in the research of privacy and users behavior associated with privacy concerns. Information that the user puts on SNS is collected by Facebook and the users are often not acquainted with this, although media is increasing the awareness of information collected by Facebook. CPM indicates that when people have higher privacy concerns, they will want to more strictly manage their disclosed information (Petronio, 2002). A study showed that the mean for the statement of how users felt if a stranger would know where they lived was 5.78 on a 7-point Likert scale. Number 7 was labeled as being "very worried" and was chosen by 46% of respondents (Acquisti & Gross, 2006). Another study revealed that 56% of Internet users have concerns about online privacy (Paine, Reips, Stieger, Joinson, & Buchanan, 2007). A study on risk taking, trust and privacy concerns among SNSs implied that non-SNS users are more concerned about the consequences of sharing identity information than SNS users and that SNS users are more likely to share their identity information online in the future than non-SNS users (Fogel & Nehmad, 2009). Furthermore, a study where interviews with students who use Facebook were held presented answers where students revealed that they did not want to have their information exposed on Facebook because of concerns about, who could access this information (Young & Quan-Haase, 2009).

According to a model where the effect of privacy concerns on willingness to provide personal information was examined, the

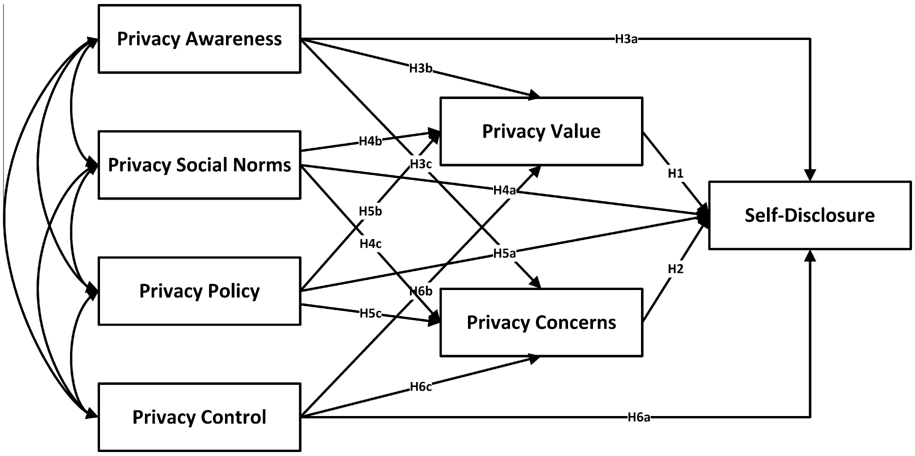

Fig. 1. The research model of privacy issues and self-disclosure on social networking sites.

negative impact between the constructs was indicated (Wu et al., 2012). Another study on self-disclosure for SNSs indicated the negative relationship between privacy concerns and self-disclosure (Krasnova et al., 2009).

Based on previous research, the impact of privacy concerns on self-disclosure is supported and the research shows that the more users are concerned about privacy, the less information they are going to disclose on SNSs. Therefore, this study proposes the following hypotheses:

H2. Privacy concerns have a negative impact on self-disclosure on SNSs.

3.3. Privacy awareness

Privacy awareness is a construct that measures how much a person is informed about privacy practices in SNSs. Media coverage plays an important part in raising privacy awareness (Dinev & Hart, 2006). Research conducted in 2009 and 2010 showed that students became more and more aware of privacy issues on Facebook in the time between the two studies (boyd & Hargittai, 2010). Another study done among students also showed that 10.3% of students in the study were unaware of their privacy settings on Facebook (Nemec, Brumen, Welzer, & Hölbl, 2011). A study on social phishing also found that SNSs users were more keen on giving information to someone who seemed to be a real-life friend than to strangers, suggesting that the collaborators of this study were aware of potential threats (Jagatic, Johnson, Jakobsson, & Menczer, 2007).

The literature suggests that privacy awareness is related to self-disclosure, privacy value and privacy concerns. This study proposes the following hypotheses:

H3a. Privacy awareness has a negative impact on self-disclosure.

H3b. Privacy awareness has a positive impact on privacy value.

H3c. Privacy awareness has a negative impact on privacy concerns.

3.4. Privacy social norms

Privacy social norms is a construct that incorporates how other people or friends influence the user into keeping their information privacy. Altman (1977) already indicated cultural effect on individuals privacy. Laufer and Wolfe (1977) suggested that public opinion is very important for privacy value. Another study also suggested that users change their privacy on Facebook depending on what they perceive others are expecting (Christofides, Muise, & Desmarais, 2009). The results of a study by Camacho, Minelli, and Grosseck (2012) showed that 26% of participants were somewhat influenced by their contacts on SNS and 46% of the respondents claimed not to be influenced by their contacts on SNS. A study with a model of individuals' privacy concerns has also indicated a positive effect for privacy social norms on privacy value (Xu et al., 2008).

Evidence was found in the literature that privacy social norms is an important construct and is related to self-disclosure, privacy value and privacy concerns. Therefore, this study proposes the following hypotheses:

H4a. Privacy social norms have a negative impact on self-disclosure.

H4b. Privacy social norms have a positive impact on privacy value.

H4c. Privacy social norms have a positive impact on privacy concerns.

3.5. Privacy policy

Privacy policy is a construct that incorporates users' opinions on how their privacy is protected with regards to SNS privacy policy and if their information is confidential. Acquisti and Gross (2006) tested the users' opinions on the importance of privacy policy on a 7-point Likert scale and the mean was 5.41, meaning it is highly important. Also the users who are more acquainted with the privacy policy of a website tend to disclose less information (Stutzman, Capra, & Thompson, 2011). A model tested by Xu et al. (2008) also indicated that privacy policy increases individuals' perceived privacy control. In another study of the privacy practices of Internet users, 86% of the respondents did not read the privacy policy of websites that do not ask any information from them and 43% of users re-check the privacy policy before buying anything online (Jensen et al., 2005). Stutzman et al. (2011) indicated a negative impact for privacy policy consumption on disclosure on Facebook, meaning that the people who read more of the privacy policy will disclose less information. Wu et al. (2012) indicated a negative impact for privacy policy on online privacy concerns among Internet users.

As explained in the literature, previous research suggests that privacy policy has had an influence on self-disclosure, privacy values and privacy concerns. This study proposes the following hypotheses:

H5a. Privacy policy has a negative impact on self-disclosure.

H5b. Privacy policy has a negative impact on privacy value.

H5c. Privacy policy has a negative impact on privacy concerns.

3.6. Privacy control

Privacy control is a construct widely used in privacy models. It explains how much control users have over who can see their information. CPM implies that the possibility of managing private information should be possible. For example, when an individual's relationship with a friend on Facebook changes, they might change the privacy settings of their disclosed information or even unfriend someone (Petronio & Durham, 2014). Studies have determined that it is necessary to have individual and group privacy rules to gain better control over the data (De Wolf et al., 2014; Petronio, 2002). A collaborator in research by Wang et al. (2011) explained that he has created another account on Facebook to self-check how others see his account even though Facebook has a feature of checking the profile from a different user already integrated. Dinev and Hart (2004) and Xu et al. (2008) indicated a negative relationship between the perceived ability to control and privacy concerns. Another study also showed that 71% of mobile SNS users would prefer determining who can access the information they share (Christin, Sánchez López, Reinhardt, Hollick, & Kauer, 2013).

As explained in other studies, privacy control has an influence on self-disclosure, privacy values and privacy concerns. Therefore, this study proposes the following hypotheses:

H6a. Privacy control has a negative impact on self-disclosure.

H6b. Privacy control has a negative impact on privacy value.

H6c. Privacy control has a negative impact on privacy concerns.

In the following chapters we will describe the research methods used in this survey, data analysis and the results of the study.

4. Research methods

The study used an online questionnaire that was designed to test 14 hypotheses. Survey questions measuring each construct – privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns and self-disclosure – were designed based on existing literature and discussion with fellow faculty members.

4.1. Data collection and participants

This research targeted users of Facebook in Slovenia. Facebook penetration in Slovenia was 39.9% in May 2014 (Allin1Social.com, 2014). On average there are 50% male and 50% female users and the majority of Facebook users in Slovenia are between 18 and 44 years old, while the largest group are users aged between 25 and 34 years old (29.6%), followed by the age group 18 to 24 (24.7%) and the age group 35 to 44 (19.0%) (SocialBakers.com, 2014).

The participants of this particular study were aged between 18 and 65. A convenience sampling was used to recruit the participants, posting a call for participation on different Facebook groups, web forums and sent via e-mail to researcher's home institution students. The welcome page of the questionnaire notified the participants about the title of the research, protection of their data and their treatment. There were 47 questions in total in the survey.

The total number of participants was 828. After a case screening 155 cases were excluded, because they did not use Facebook. Also if the standard deviation for responses of each person were less than 0.5, the case was excluded, because there is no variance in these cases. A total of 12 such unengaged responses were deleted. The variables age and education were tested for outliers with boxplots and no cases were excluded after this step, because there were no outliers found. After the complete screening was done, 661 cases were valid. A detailed sample of demographics for valid cases is in Table 2.

4.2. Measures

Measurement items for the constructs were combined from existing measures to ensure validity. A 5-point Likert-scale ranging from (1) strongly disagree to (5) strongly agree was used to evaluate the items in each construct. The detailed constructs with items and references used to build the constructs are in Table 3. There were 26 items in the survey. The survey instruments were pretested with 25 users of Facebook and then refined and validated for statistical properties.

Table 2
Sample of demographics ($n = 661$).

Variable	Sample results
Gender	Male 43.1% Female 56.9%
Education	High school 45.5% Bachelor's degree 46.6% Master's degree or higher 7.9%
Age mean	*M* 26.76 SD 6.91
Number of Facebook friends	*M* 302.98 SD 191.79
Frequency of Facebook use	Less than once a day 16.0% 10 min or less per day 11.5% 30 min or less per day 25.7% 60 min or less per day 26.9% More than 60 min per day 19.8%

5. Data analysis and results

A data analysis was performed with the use of IBM SPSS Statistics 20.0 and AMOS 19.0 software. A structural equations modeling was used and hypothesis testing was done.

5.1. Model analysis

First, variable screening for missing data was done, and then factor loadings analysis was conducted and it was iterated until the results arrived at a clean pattern matrix. Two variables, SD5 (Variable 5 for the Self-disclosure construct) and PCt3 (Variable 3 for the Privacy control construct) were dropped because of a loading lower than 0.5. Two variables with a loading lower than 0.5 were left in the model to avoid under-dependency, which may occur when there are not enough items to define a construct (Hair, 2010). Altogether 24 items were left in the model.

Convergent validity was evaluated with Cronbach's alpha, a commonly used measure testing the extent to which multiple items for a construct belong together. The coefficient ranges from 0 to 1. Cronbach's alpha in the research model presented ranged from 0.711 to 0.894, which is within the acceptable reliability coefficient above 0.7 (Nunnaly, 1978). Cronbach's alpha was calculated for each construct, considering all the items that were left after the exclusion of two items. All values are presented in Table 4.

The factor loadings for the final set of items in the model are also presented in Table 4. The bolded items in the table exceed the recommended values. The results show that the instrument of research has a high internal consistency and factor loadings and is therefore reliable.

Next, a confirmatory factor analysis was done to validate the model. The results of the model fit for the initial model (after two construct items were already deleted) can be seen in Table 5. The following fit indices were included: the chi-square statistic ($C_{\min}/df$), the root mean square error of approximation (RMSEA), the goodness-of-fit (GFI), the normed fit index (NFI) and the comparative fit index (CFI). The recommended values in the table were adapted from Segars and Grover (1993), Chin and Todd (1995) and Hair (2010).

In the resulting set of measurement items the composite reliability (CR), average variance extracted (AVE) and factor correlations matrix are presented in Table 6. The composite reliability values are between 0.737 and 0.902, and the average variance extracted values are between 0.501 and 0.677, all surpassing the minimum value of 0.7 and 0.5 respectively (Hair, 2010). The discriminant validity criteria is confirmed when the AVE value exceeds the squared correlation between different constructs (Fornell & Larcker, 1981). As in Table 6, there is good discriminant validity for all constructs. To sum up, there are no reliability or validity concerns in the model.

Further on, a common method bias approach was done to define whether anything external to questions may have influenced the responses by the user (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Evidence of common method bias was found in privacy policy and privacy concern factor so the common latent factor was retained in the model, meaning the model is using common method bias adjusted variables.

Table 3
Measurement of variables.

Constructs	Code	Items	References
Privacy awareness	PA1	I am aware of problems and procedures concerning privacy in our society	Xu et al. (2008)
	PA2	I follow news and the development of problems and violations concerning privacy	
	PA3	I follow news on what companies and government do to ensure our privacy	
Privacy social norms	PSN1	People who have influence on me believe that it is very important to keep my personal information private	Xu et al. (2008)
	PSN2	My friends believe that I need to take care about my privacy	
	PSN3	People who are important to me believe that I should be careful with exposing my information online	
Privacy policy	PP1	I am convinced that the privacy policy of Facebook reflects that my privacy is protected	Wu et al. (2012) and Xu et al. (2008)
	PP2	Considering the privacy policy of Facebook, I believe that my personal information will be kept private and confidential	
	PP3	I believe that the privacy policy of Facebook reflects respect for the privacy of an individual	
Privacy control	PCt1	I believe that I have control over who can access my personal information that I post on Facebook	Xu et al. (2008)
	PCt2	I believe that I have control over which of my personal information is visible to others on Facebook	
	PCt3	I believe that I have control over how Facebook uses my personal information	
	PCt4	I believe that I have control over which information I provide to Facebook	
Privacy value	PV1	In comparison with others, I believe privacy is very important	Chen (2013) and Xu et al. (2008)
	PV2	It is very important to me that I keep my online privacy	
	PV3	In comparison with others, I am more sensitive about threats to my privacy	
Privacy concerns	PC1	It bothers me when I have to put much personal information on SNSs	Dinev and Hart (2004), Wu et al. (2012) and Xu et al. (2008, 2012)
	PC2	I am concerned that SNSs are collecting too much personal information about me	
	PC3	I am concerned that unauthorized people could access my personal information	
	PC4	I am concerned that SNSs use my personal information for purposes that I am not being notified of	
	PC5	I am concerned when I have to post personal information on SNSs	
Self-disclosure	SD1	I have a detailed profile on Facebook[a]	Chen (2013), Krasnova et al. (2009) and Wu et al. (2012)
	SD2	My Facebook profile tells a lot about me[a]	
	SD3	I reveal a lot of information about me on Facebook[a]	
	SD4	I don't mind putting personal information on SNSs[a]	
	SD5	I am forced to provide personal information on SNSs	

[a] Reverse coded item.

Table 4
Factor loadings and Cronbach's alpha.

Item	Factor loading	Constructs	No. of items	Cronbach's α
PA1	**0.462**	Privacy awareness	3	0.776
PA2	0.977			
PA3	0.772			
PSN1	0.645	Privacy social norms	3	0.815
PSN2	0.804			
PSN3	0.867			
PP1	0.718	Privacy policy	3	0.856
PP2	0.765			
PP3	0.948			
PCt1	0.697	Privacy control	3	0.711
PCt2	0.890			
PCt4	**0.372**			
PV1	**1.002**	Privacy value	3	0.850
PV2	0.734			
PV3	0.619			
PC1	0.654	Privacy concerns	5	0.894
PC2	0.865			
PC3	0.820			
PC4	0.811			
PC5	0.835			
SD1	0.717	Self-disclosure	4	0.837
SD2	0.835			
SD3	0.894			
SD4	0.521			
Overall			24	0.793

5.2. Structural equations model results

The results of the model fit for the final model are in Table 7 and can be compared to Table 5 where the results of the model fit for the initial model are presented. All the values for the final model were within the frame of the recommended criteria so the overall model fit is acceptable and the paths can be used to test the hypotheses.

Table 5
The results of testing the overall model fit (initial model).

Notation	Recommended value	Initial model
χ^2/df	$\leqslant$3.0	2.289
RMSEA	$\leqslant$0.10	0.044
GFI	$\geqslant$0.90	0.929
NFI	$\geqslant$0.90	0.918
CFI	$\geqslant$0.90	0.952

5.3. Testing research hypothesis

The model was tested for the overall model fit, while individual paths in the model were also tested. The results of the path analysis for the links between different groups of factors are in Fig. 2.

The path coefficient analysis and the results of the *t*-statistic explain the hypotheses that were developed. The strength and significance of each path is evaluated by the standardized coefficient (β) and by a *t* value higher than 2.0 or lower than −2.0 (Al Omoush, Yaseen, & Atwah Alma'aitah, 2012). The results of the path analysis and hypotheses testing are in Table 8. The results indicate that three paths are insignificant – (1) privacy awareness does not have a significant effect on privacy value, (2) privacy control does not have a significant relationship on self-disclosure and (3) privacy social norms do not have a significant effect on privacy concerns. Privacy social norms and privacy control have a significant effect on privacy value at a p value lower than 0.01 and standardized coefficient values of 0.116 and −0.147 respectively, with *t* values higher than 3 and lower than −3 respectively. All the other path effects in the model are significant at p lower than 0.001. Privacy concerns, privacy awareness, privacy social norms, and privacy policy have a significant effect on self-disclosure and standardized values −0.340, −0.340, −0.125, −0.425 respectively, with *t* values

Table 6
Composite reliability (CR), average variance extracted (AVE) and factor correlations matrix.

	CR	AVE	Privacy value	Privacy policy	Privacy concerns	Self-disclosure	Privacy awareness	Privacy social norms	Privacy control
Privacy value	0.862	0.677	**0.823**						
Privacy policy	0.860	0.672	−0.090	**0.820**					
Privacy concerns	0.902	0.648	0.615	−0.262	**0.805**				
Self-disclosure	0.844	0.577	0.432	−0.121	0.291	**0.759**			
Privacy awareness	0.801	0.586	0.272	−0.094	0.151	0.032	**0.766**		
Privacy social norms	0.818	0.600	0.266	0.195	0.191	0.097	0.122	**0.775**	
Privacy control	0.737	0.501	−0.047	0.590	−0.275	0.032	0.087	0.133	**0.707**

The diagonal elements in bold represent square root of AVE.

Table 7
The results of testing the overall model fit (final model).

Notation	Recommended value	Final model
$\chi^2/\mathrm{d}f$	$\leqslant$3.0	2.618
RMSEA	$\leqslant$0.10	0.050
GFI	$\geqslant$0.90	0.986
NFI	$\geqslant$0.90	0.966
CFI	$\geqslant$0.90	0.978

Table 8
The results of the hypotheses testing.

H	Path			Standardized coefficient β	t-Statistic	The result
H1	PV	–	SD	.418***	10.449	Accepted
H2	PC	–	SD	−.340***	−7.257	Accepted
H3a	PA	–	SD	−.340***	−9.851	Accepted
H3b	PA	–	PV	.063^{NS}	1.670	Rejected
H3c	PA	–	PC	−.120***	−3.702	Accepted
H4a	PSN	–	SD	−.125***	−3.848	Accepted
H4b	PSN	–	PV	.116**	3.219	Accepted
H4c	PSN	–	PC	.036^{NS}	1.165	Rejected
H5a	PP	–	SD	−.425***	−9.431	Accepted
H5b	PP	–	PV	−.246***	−5.119	Accepted
H5c	PP	–	PC	−.338***	−8.242	Accepted
H6a	PCt	–	SD	−.080^{NS}	−1.840	Rejected
H6b	PCt	–	PV	−.147**	−3.185	Accepted
H6c	PCt	–	PC	−.361***	−9.177	Accepted

** $p < 0.01$.
*** $p < 0.001$.
^{NS} $p \geqslant 0.05$ (not significant).

lower than −3. Privacy value has a significant effect on self-disclosure and a standardized value of 0.418 with t value higher than 10. Privacy policy has a significant effect on privacy value with β −0.246, for t value lower than −5. Privacy awareness, privacy policy and privacy control have a significant effect on privacy concerns with β −0.120, −0.338, −0.361 respectively and t values lower than −3.

6. Discussion and conclusions

SNSs, particularly Facebook, are a part of the everyday life of many individuals. Facebook is gaining new members daily as well as new posts and information on profiles are published by users daily. The spread of SNSs has opened new issues in privacy and self-disclosure online.

The goal of the study was to develop a model of how privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns and self-disclosure are interconnected with each other. To the best of our knowledge, it is the first work that jointly considers all constructs in one model. The model was built based on previous research done in the field of privacy and self-disclosure. Online methods were used to collect data to validate the model. 661 respondents aged between 18 and 65, who both use Facebook and are from Slovenia, participated in the survey.

Our results provided an empirical model with the following constructs – privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns and self-disclosure, tested on users of SNS Facebook. The research model was confirmed via SEM analysis and the results of the path analysis accepted 11 out of 14 hypotheses tested. Privacy awareness, privacy social norms, privacy policy, privacy values and privacy concerns were indicated as being important in affecting self-disclosure on Facebook. The results also showed that privacy social

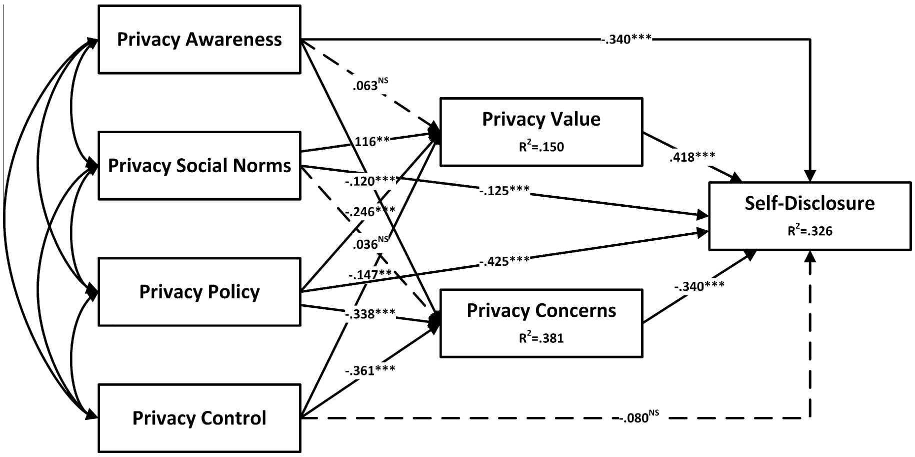

Fig. 2. The path coefficient analysis.

norms, privacy policy and privacy control have an effect on privacy value. And privacy awareness, privacy policy and privacy control have an effect on privacy concerns.

To place our results in context, privacy value was found to have a significantly positive impact on self-disclosure on a SNS. This indicates that the higher the user will value privacy, the more the user will disclose on Facebook. In a study by Stutzman et al. (2011) a similar hypothesis was confirmed, indicating that the users who had customized privacy settings for published content, were less likely to disclose more information on Facebook. A study by Lampe, Ellison, and Steinfield (2008) showed that user perception could change over time, meaning that if the persons' privacy value increases, they will want to disclose their information more carefully.

Privacy concerns were found to have a negative impact on self-disclosure, meaning that the higher the users' concern for privacy will be, the less information the user will disclose on SNSs. This path has already been supported by Krasnova et al. (2009) and Wu et al. (2012).

Privacy awareness was indicated to have a significantly negative impact on self-disclosure and on privacy concerns. This means that the more the users are informed about privacy, the less they will want to self-disclose and that the privacy concerns of the users will be higher. The privacy awareness of visitors of online websites has already driven companies to deal with privacy concerns by changing privacy policies (Cranor, Egelman, Sheng, McDonald, & Chowdhury, 2008). The impact of privacy awareness on privacy value in our model was not significant. This impact was also not significant for social networking users in a study by Xu et al. (2008), but it was significantly positive for the users of e-commerce, financial and healthcare websites.

Privacy social norms were indicated to have a negative impact on self-disclosure and positive impact on privacy value. The latter relationship was also supported by Xu et al. (2008). This relationships indicate that the bigger the influence of friends in raising the privacy awareness of the user is, the less the user will disclose and the user will have a lower value of privacy. The impact of privacy social norms does not have any significant impact on privacy concerns and this path was not presented in any other study found. This implies that the influence of friends in raising the privacy awareness of the user is not relevant for users' privacy concerns.

Privacy policy was indicated to have a negative impact on self-disclosure, privacy value and privacy concerns. Likewise, the first and the last relationships were similarly supported by Stutzman et al. (2011) and Wu et al. (2012) respectively. All the indicated paths imply that the more the user will read the privacy policy, the higher control over self-disclosure the user will want to have. As well as raising the privacy value of the user, the user will also be more concerned about privacy issues when reading more of the privacy policy. Based on these results policy makers are advised to provide users with more information that can help a user understand their concerns.

Privacy control was indicated to have a negative impact on privacy value and privacy concerns. To explain, the users who feel that they have a good control over their privacy settings on Facebook will show a higher value for privacy than others and will have more concerns about the privacy as well. The impact of privacy control on self-disclosure in the proposed model was not significant. Another study, however, implied that the impact between privacy behavior and disclosure is positive (Stutzman et al., 2011), although the privacy behavior construct is not exactly the same as the privacy control in our model. The path in our model implies that privacy control does not have any significant effect on what the user will self-disclose.

As explained in this section, our results are consistent with previous findings from research in the field of privacy and self-disclosure in the majority of instances. The results confirm and add new meaning to research in the field of the formation of self-disclosure on SNSs.

6.1. Limitations and future research directions

This study has some limitations. Facebook penetration in Slovenia is 39.9% (Allin1Social.com, 2014), which is about 820,000 people. The sample size in this study was 661 Slovenian users of Facebook, which is statistically valid with a 95 confidence level and 3.81% margin of error. Due to the convenience sampling method the study cannot be generalized to Slovenian users of Facebook or to all Facebook users. Future research should strive to collect a larger and more representative sample.

The next limitation were the constructs in the model. Even though an extensive analysis of existing studies was conducted, potential constructs might have been left unselected. Future studies should identify and incorporate potentially significant constructs for privacy issues and self-disclosure.

A statistical limitation was also that common method bias was found in privacy policy and privacy concern constructs so that common latent factor was retained in the model, meaning that model used common method bias adjusted variables. Future studies should avoid using the common method bias.

Future studies may need to develop a measurement scale specific to SNS users. The constructs in this study were adapted from models with users of Internet, electronic commerce, financial and healthcare websites, mobile users and SNS users.

6.2. Conclusion

In conclusion, this research explains the privacy dynamics behind self-disclosure on SNSs. The model presented in our study was built upon previously developed models but extended with the missing connections between privacy variables and self-disclosure among SNSs users. This model attempted to present a more holistic view on the issue of self-disclosure on Facebook and privacy variables that have a significant impact on self-disclosure.

The contribution of this study is to better understand the privacy dynamics and self-disclosure of users on SNS Facebook, given that earlier studies have not incorporated some of the important privacy variables in self-disclosure models among Facebook users. This study combined privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns and self-disclosure into one model. The study could help SNS providers publish more information for their users. With the media coverage of the findings of this study, a better understanding of privacy issues and self-disclosure on Facebook could also be presented. The developed model could also serve as a basis for other models to be developed and the model could also be extended to some other platform, not only SNSs.

Acknowledgements

This work was supported by the Slovenian Research Agency under the Grant 1000-10-310259 and by the research group P2-0057. We would also like to acknowledge participants of this research.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.). *Privacy enhancing technologies* (Vol. 4258, pp. 36–58). Berlin, Heidelberg: Springer.

Al Omoush, K. S., Yaseen, S. G., & Atwah Alma'aitah, M. (2012). The impact of Arab cultural values on online social networking: The case of Facebook. *Computers in Human Behavior, 28*(6), 2387–2399.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Brooks/Cole Pub. Co.

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

Anderson, J., & Stajano, F. (2013). Must social networking conflict with privacy? *IEEE Security and Privacy, 11*(3), 51–60.

Archer, J. L. (1980). The self in social psychology. In D. Wegner & R. Vallacher (Eds.), *Self-disclosure* (pp. 183–204). London: Oxford University.

boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1).

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8).

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). New York: Routledge.

Camacho, M., Minelli, J., & Grosseck, G. (2012). Self and identity: Raising undergraduate students' awareness on their digital footprints. *Procedia – Social and Behavioral Sciences, 46*, 3176–3181.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior, 30*, 79–86.

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems, 55*(3), 661–668.

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

Chin, W. W., & Todd, P. A. (1995). On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution. *MIS Quarterly, 19*(2), 237–246.

Christin, D., Sánchez López, P., Reinhardt, A., Hollick, M., & Kauer, M. (2013). Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications. *Information Security Technical Report, 17*(3), 105–116.

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.

Courtney Walton, S., & Rice, R. E. (2013). Mediated disclosure on Twitter: The roles of gender and identity in boundary impermeability, valence, disclosure, and stage. *Computers in Human Behavior, 29*(4), 1465–1474.

Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., & Chowdhury, A. (2008). P3P deployment on websites. *Electronic Commerce Research and Applications, 7*(3), 274–293.

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior, 35*, 444–454.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – Measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422.

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

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33*, 153–162.

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, 18*(1), 39–50.

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior, 29*(6), 2257–2264.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks (the Facebook case). In *ACM workshop on privacy in the electronic society (WPES)*. Alexandria, Virginia, USA.

Hair, J. F. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Hollenbaugh, E. E., & Ferris, A. L. (2014). Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior, 30*, 50–58.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human–Computer Studies, 63*(1–2), 203–227.

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: It's complicated. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1–15). Washington, DC: ACM.

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is there an app for that? In *Symposium on usable privacy and security*. Pittsburgh, PA.

Kisekka, V., Bagchi-Sen, S., & Rao, H. R. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in Human Behavior, 29*(6), 2722–2729.

Kolek, E. A., & Saunders, D. (2008). Online disclosure: An empirical examination of undergraduate Facebook profiles. *NASPA Journal, 45*(1).

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). It won't happen to me!'': Self-disclosure in online social networks. In *Americas conference on information systems*.

Kwak, K. T., Choi, S. K., & Lee, B. G. (2014). SNS flow, SNS self-disclosure and post hoc interpersonal relations change: Focused on Korean Facebook user. *Computers in Human Behavior, 31*, 294–304.

Lampe, C., Ellison, N. B., & Steinfield, C. (2008). Changes in use and perception of Facebook. In *Cscw: 2008 Acm conference on computer supported cooperative work, conference proceedings* (pp. 721–730).

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human–Computer Studies, 71*(9), 862–877.

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.

McKnight, D. H., Lankton, N., & Tripp, J. (2011). Social networking information disclosure and continuance intention: A disconnect. In *44th Hawaii international conference on system sciences (HICSS), 2011* (pp. 1–10).

Nemec, L., Brumen, B., Welzer, T., & Hölbl, M. (2011). Privacy awareness among students whilst using the social networking site 'Facebook'. In *ISIT* (pp. 11–17). Dolenjske Toplice, Slovenia.

Nunnaly, J. (1978). *Psychometric theory*. New York: McGraw-Hill.

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human–Computer Studies, 65*(6), 526–536.

Petronio, S. (2002). *Boundary of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

Petronio, S., & Durham, W. (2014). Communication privacy management theory: Significance for interpersonal communication. In D. O. Braithwaite & P. Schrodt (Eds.), *Engaging theories in interpersonal communication: Multiple perspectives* (2nd ed., pp. 335–347).

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.

Sahinoglu, M., Akkaya, A. D., & Ang, D. (2012). Can we assess and monitor privacy and security risk for social networks? *Procedia – Social and Behavioral Sciences, 57*, 163–169.

Segars, A. H., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quarterly, 17*(4), 517–525.

Sheldon, P. (2008). Student favorite: Facebook and motives for its use. *Southwestern Journal of Mass Communication*.

Special, W. P., & Li-Barber, K. T. (2012). Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior, 28*(2), 624–630.

Staddon, J., Huffaker, D., Brown, L., & Sedley, A. (2012). Are privacy concerns a turn-off?: Engagement and privacy in social networks. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1–13). Washington, DC: ACM.

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

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality, 4*(2).

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821–826.

Tow, W. N. F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology, 25*(2), 126–136.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). ''I regretted the minute I pressed share'': A qualitative study of regrets on Facebook. In *Proceedings of the seventh symposium on usable privacy and security* (pp. 1–16). Pittsburgh, Pennsylvania: ACM.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897.

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

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In F. G. Joey (Ed.), *International conference on information systems: Association for information systems 2012*.

Young, A. L., & Quan-Haase, A. (2009). Information revelation and Internet privacy concerns on social network sites: A case study of Facebook. In *C&T '09 (communities and technologies)* (pp. 265–274). ACM New York, NY, USA: The Pennsylvania State University, PA, USA.