Computers in Human Behavior 35 (2014) 444–454

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook

Ralf De Wolf*, Koen Willaert, Jo Pierson

iMinds – Digital Society Department, SMIT, Studies on Media, Information & Telecommunication, Vrije Universiteit Brussel, Pleinlaan 9, 2nd floor, B-1050 Brussel, Belgium

ARTICLE INFO

Article history:
Available online 4 April 2014

Keywords:
Privacy
Social network sites
Communication Privacy Management theory (CPM)
Facebook
Disclosure

ABSTRACT

Most research on privacy management within the context of social network sites (SNSs) treats users as individual owners of private information. Privacy, however, is beyond individual control and is also managed on a group level. This study applies the Communication Privacy Management theory (CPM) to explore the individual and group privacy management strategies in Facebook. We present a survey completed by 900 members of a youth organization regarding their online behaviors and membership. We found that women are more likely to employ individual privacy management strategies, while men are more likely to employ group privacy management strategies. For group privacy management, we found common bond and the role an individual is attributed within the youth organization to be the strongest predictors. The results generated from this study are a first but important step to illustrate the differences and similarities between individual and group privacy management. We argue that it is necessary to further study and understand group privacy to better approach users' privacy needs.

1. Introduction

Since social network sites (SNSs) began to bloom, privacy researchers have studied their impact on users' privacy. Psychological and sociological perspectives often study how the technical properties of SNSs create new dynamics and influence the privacy management of users (e.g. boyd, 2008; Litt, 2013; Stutzman, Capra, & Thompson, 2011; Tufekci, 2008; Vitak, 2012). Recently, academics and scholars have pled to broaden up the scope of privacy research by focusing on the *collective* next to the *individual* level of privacy (boyd, 2011; Lampinen, Lehtinen, Lehmuskallio, & Tamminen, 2011; Parks, 2010; Smith, Dinev, & Xu, 2011; Xu, 2012). Indeed, when information is disclosed to others, they become co-owners. Moreover, some types of information never belonged to the individual in the first place, but can be regarded as group property. In this study we have a closer look at how members of youth organizations manage this group property in Facebook. To do this, we draw on the Communication Privacy Management theory (CPM), as formulated by Petronio (2002). CPM treats privacy as a dialectic process, indicating that privacy is about opening and closing boundaries to others and optimizing the need of being both private and public. Following CPM, this regulation of boundaries is dependent of so-called privacy rules or privacy management strategies. People develop both individual and group privacy management strategies. For example, in Facebook users can employ settings that limit the audience to whom the information flow is directed or, together with others, agree on what type of information can be disclosed.

Throughout this article, we further discuss the basic principles of CPM, the general patterns in how people manage group boundaries and provide an overview of different privacy management strategies used in SNSs. The overall goal of this study is to move beyond an individual-centric notion of privacy. Specifically, we focus on the privacy management strategies of members ($n = 900$) of -Belgian youth organizations in Facebook. By means of hierarchical regression analyses, we determine the predictors of individual and group privacy management and its relationship with perceived privacy control.

2. Communication privacy management theory

2.1. Privacy as boundary coordination

Petronio (2002, p. 6) defines privacy, "as the feeling that one has the right to own private information, either personally or collectively." We manage our privacy through coordinating the boundaries of sharing certain information with particular people or groups. Indeed, she refers to *our* privacy because people have the feeling that they *own* private information and others become co-owners when the information is disclosed. People develop

* Corresponding author.
E-mail addresses: ralf.de.wolf@vub.ac.be (R. De Wolf), koen.willaert@vub.ac.be (K. Willaert), jo.pierson@vub.ac.be (J. Pierson).

http://dx.doi.org/10.1016/j.chb.2014.03.010
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

individual and group privacy management strategies or rules to coordinate disclosure behavior. As we create individual boundaries around the self, we also create group boundaries with others. Co-owners of information negotiate on privacy rules to optimize the dialectic between disclosing and withdrawing of information. When the negotiation fails privacy turbulence is likely to occur. For example, people intentionally violate the established rules or unwillingly disclose private information.

Petronio (2002) differentiates three general patterns in how people manage group boundaries: inclusive boundary coordination, intersected boundary coordination, and unified boundary coordination.

Inclusive boundary coordination refers to person A giving up privacy control to person B in order to get something in return (e.g., a patient talking about their eating habits to a doctor so the doctor can provide adequate consultation with regard to his or her health status). In intersected boundary coordination, the concealed information is perceived as comparable, and person A and B are considered as equals (e.g., two friends mutually disclosing the troubles they face at home). Unified boundary coordination is a pattern whereby everyone is in control of the private information, whilst no one really owns the information. Here, the power of person A over B or the equal sharing of information between person A and B is not the most important aspect (e.g., members of a sports club concealing that they have cheated during a game). Rather, "the body of private information typically found in this type of coordination often predates all members and new members make contributions, yet the information belongs to the body of the whole" (Petronio, 2002, p. 134). In this study we conceptualize group privacy management as coordinating unified boundaries. Individual privacy management we conceptualize as the coordination of privacy rules around the self.

2.2. Boundary coordination in SNSs

Many researchers have studied how users manage their privacy in SNSs. Most focus on how users employ the privacy settings available in SNSs (i.e. boyd & Hargittai, 2010; Kramer-Duffield, 2010; Lenhart, 2009; Lewis, Kaufman, & Christakis, 2008; Litt, 2013; Stutzman, Gross, & Acquisti, 2012; Vitak, 2012), such as deleting content form one's profile (Madden, 2012) or creating separate audience groups (Kramer-Duffield, 2010). Others also study the social and mental strategies in managing privacy in SNSs. For example, boyd and Marwick (2011) indicate that teenagers encrypt the meaning of the disclosed information in SNSs, so that it only becomes accessible to a particular segment of their friends. They labeled the latter with the term social steganography. Brandtzæg, Lüders, and Skjetne (2010) suggest that users adapt their disclosure behavior through only posting information that matches the attitudes and beliefs of all audiences. The latter goes hand in hand with the common denominator approach of Hogan (2010), whereby users treat SNSs as a front stage and only post information that is suitable for every public.[1]

CPM was developed before the emergence of SNSs as a widespread communication tool. In SNSs users are not only disclosing to other people, but also to SNS providers and other third parties. Raynes-Goldie (2010) defines "the control of information flow about how and when personal information is shared with other people" as social privacy, and access to and processing of individually identifiable personal information by SNS providers and other third parties as institutional privacy.

Different components have been identified as reasons for users to disclose information to SNS providers and third parties, including financial rewards and personalization (Smith et al., 2011; Xu, Teo, Tan, & Agarwal, 2009; Yang & Wang, 2009). When disclosing information to other people, Petronio (2002, p. 6) indicates, "Individuals may wish to relieve a burden, gain control, enjoy self-expression, or possibly develop intimacy." Over the years, researchers have studied why users disclose information towards other people in SNSs and especially found it be of value for bridging and bonding social capital (Ellison, Steinfield, & Lampe, 2011; Steinfield, Ellison, & Lampe, 2008; Vitak & Ellison, 2012) and presenting the self (boyd, 2008; Papacharissi, 2012; Parks, 2010; Zhao, Grasmuck, & Martin, 2008). Although users disclose information towards multiple audiences at once in SNSs, research indicates that users disclose to achieve interpersonal benefits, rather than paying heed to the harm SNS providers and other third parties might cause (Brandtzæg et al., 2010; Raynes-Goldie, 2010; Tufekci, 2008; Young & Quan-Haase, 2013).

In this study we limit ourselves to studying individual and group privacy management with respect to other people in SNSs and do not focus on how users deal with the collection and processing of personal information by SNS providers and other third parties.

3. Predictors and hypotheses in the model

CPM theory outlines different decision criteria that influence the development of privacy management strategies. In this section we discuss and substantiate different criteria we included in the research model and formulate our hypotheses. A body of literature has studied the individual privacy management in SNSs. To our knowledge, the predictors of group privacy management in Facebook have not been studied so far. We differentiate between group and individual privacy management to obtain a holistic view on managing privacy boundaries. In Appendix A we give an overview of the individual privacy management strategies we measured. We include preventive, corrective, social and structural privacy management strategies.

3.1. Predictors of individual privacy management strategies

When people grow older their social environment expands. This makes it possible to develop a multi-layered self. It also requires being able to control multiple boundaries and information flows. CPM theory indicates that during the adolescent stage individuals begin to develop stricter privacy rules (Petronio, 2002). In adulthood the privacy rules must increase to manage privacy boundaries. Litt (2013) notices that while popular media often suggests that young users do not care about their online privacy, studies conclude quite the reverse: young users are stricter than older users. The research of Brandtzæg et al. (2010) indicate that young users are more aware of strategies to manage their privacy than adults. It also seems that young users employ different privacy management strategies. boyd and Marwick (2011) state that teenagers use social strategies as social steganography in managing their privacy, whilst Quinn (2012) mentions other privacy strategies used by mid-adults, such as not filling out profiles fully or providing false information.

CPM states that adults establish stricter privacy rules than children and adolescents (Petronio, 2002). Research on privacy management in SNSs suggests the opposite. We therefore find it difficult to specify a direction regarding the relationship between age and privacy management in SNSs. As such, our first hypothesis expects a significant difference between age and privacy management but does not specify its relationship.

[1] For a synthesis of the different strategies used for boundary coordination, we refer to work of Lampinen et al. (2011).

H1. Age is related to individual privacy management.

CPM suggests that men and women define their privacy boundaries differently and develop a distinct set of privacy management strategies (Petronio, 2002). Research in SNSs has found that women use more privacy settings to manage their privacy, such as un-tagging photos or setting their profiles to private (boyd et al., 2010; Lewis et al., 2008; Litt, 2013).

H2. Women apply more individual privacy management strategies than men.

Our third hypothesis studies the relationship between occupation and privacy management. We conceptualize occupation as one's regular performed activity, and differentiate between secondary school students, college students, employees and those looking for a job. Hargittai and Litt (2013) indicate that employers are increasingly using SNSs to scan their current and potential employees. Not coordinating privacy boundaries might damage their reputation and put (future) jobs on the line. Therefore, we could assume that employees and those looking for a job employ stricter privacy management strategies than college and secondary school students. Moreover, CPM indicates that when the audience expands, the boundaries also have to expand to accommodate increasing privacy needs (Petronio, 2002). Research, however, indicates that many users fail to create separate professional and non-professional identities (DiMicco & Millen, 2007) or lack the skills to present the self optimally online while searching for a job (Hargittai & Litt, 2013). We propose following hypotheses:

H3. One's regularly performed activity is related to individual privacy management.

CPM indicates that people employ stricter privacy rules when having higher concerns, although not all research indicates that privacy concerns influence privacy management (e.g., Acquisti & Gross, 2006; Tufekci, 2008). Sometimes people fail in coordinating their privacy boundaries, and turbulence occurs. In online environments, privacy turbulence has been proven to be an important predictor for privacy management (Child & Petronio, 2011; Child, Petronio, Agyeman-Budu, & Westermann, 2011; Litt, 2013). We hypothesize that privacy concern and turbulence will positively influence privacy management.

H4. Individuals who have a higher privacy concern apply more individual privacy management strategies.

H5. Individuals who have experienced individual privacy turbulence apply more individual privacy management strategies.

3.2. Predictors of group privacy management strategies

CPM states that groups are fundamental to our lives and also develop privacy rules to coordinate boundaries. In this study, we focus on the unified boundary coordination of members of the KSJ-KSA-VKSJ,[2] a youth organization in Flanders (Belgium) that is comparable to the Boy or Girl Scouts of America. KSJ[3] consists of 30,293 members, spread over more than 276 local groups in different districts of Flanders, Belgium.[4] Each local group has *members* (children and adolescents) and *leaders* (young adults), who are classified into different bans or sections. Children from primary schools are subdivided into three bans: gnomes (6–8 years old), jumpers (8–10 years old), and young lads (10–12 years old). Adolescents are also subdivided into three bans: lads (12–14 years old), young renewers (14–16 years old), and renewers (16+). Although these are the official divisions, each local group has its own interpretation and structure. KSJ is originally founded on Christian values, but nowadays mainly seeks to let young adults educate adolescents and children on a weekly basis, in an informal way, by means of playing recreational and educational games. Within KSJ, both gender-segregated groups (boys and girls only) and mixed groups exist.

We argue that the demographic measures as formulated in Section 3.1 are also applicable for group privacy management. As members become older they are likely to manage multiple boundaries. We hypothesize that older members of a youth organization employ stricter group privacy management strategies.

H6. Age is positively related to group privacy management.

The way men and women develop privacy rules is also dependent of an individual's environment. According to CPM, women disclose more in small groups, while men disclose more in dyads. Moreover, women tend to reveal more than men do in small groups. CPM indicates gendered differences as decision criteria used to develop privacy rules, but does not specify its relationship (Petronio, 2002).

H7. Gender is related to group privacy management.

As employees and job seekers are confronted with current and potential employees, they would also benefit from scoring higher on group privacy management strategies. Group information after all is also part of the self, which can also be subject to a scanning from employers. We formulate following hypothesis:

H8. Employees and job seekers are more likely to employ group privacy management strategies than secondary school and college students.

The unified boundary coordination is determined by membership in a group (Petronio, 2002). We therefore include different group measures. To measure membership in a group we study why people identify with one's group. Following Prentice, Miller, and Lightdale (1994) we differentiate between common identity and common bond. While the former refers to the feeling of being attached to the group as a whole, the latter refers to the feeling of being attached to individual members of that particular group. Antecedents of common identity are social categorization, interdependence, and out-group presence, whereas those of common bond are social interaction, personal information, and interpersonal similarity (Ren, Kraut, & Kiesler, 2007). We assume that the higher the score on common bond and common identity – a higher identification with one's group – the more likely members will possess greater group privacy management strategies in Facebook. Next to determining why people identify with one's group, we also take into account the role one plays in their group and its composition (gendered-segregated and gender-mixed groups), as predictors. We hypothesize that those attributed with an educative role (leaders) will make more use of group privacy management strategies. In line with the view of CPM on gender we expect the composition of the group to be significantly related with group privacy management. Thus, we state the following hypotheses:

[2] KSJ (Katholieke Studerende Jeugd), KSA (Katholieke Studentenactie), VKSJ (Vrouwelijke Katholieke Studerende Jeugd). Throughout the article we use the abbreviation KSJ.

[3] Throughout the article we use the abbreviation KSJ for KSJ-KSA-VKSJ.

[4] We retrieved this information from the employees of KSJ National on the 25th of March 2013.

H9. Members who identify highly with their group apply more group privacy management strategies.

H10. Members who are attributed with an educative role in their group apply more group privacy management strategies.

H11. The composition of the group (gendered-segregated and gender-mixed groups) is related to group privacy management.

In line with CPM we hypothesize that privacy concern will be positively related with group privacy management. Because information belongs to everyone it may happen that groups fail to coordinate their privacy boundaries. When groups have experienced turbulence it is likely that they try re-negotiating their boundaries.

H12. Members who have a higher privacy concern apply more group privacy management strategies.

H13. Members who have experienced group privacy turbulence apply more group privacy management strategies.

3.3. Privacy management and perceived privacy control

As people develop both individual and group privacy management rules, an adequate combination of both will likely lead to a higher feeling of control over private information: "When boundary coordination works in synchronicity, the members successfully regulate privacy" (Petronio, 2002, p. 176). Therefore, we also look at the relation between privacy management and perceived control. We speak of *perceived* privacy control, because users tend to magnify the degree of control they exert (Xu, 2012).

H14. Individual privacy management is positively related to perceived individual privacy control.

H15. Group privacy management is positively related to perceived group privacy control.

H16. Individual group privacy management and group privacy management are positively related with one another.

In the following sections we describe the research model, sample, and the operationalized measures we use in the regression models. We developed, changed, and employed different Likert-scales to operationalize the measures. Fig. 1 summarizes the research model of this study. Specifically, we measure the relationship between the predictors and individual privacy management in Section 5.1; do the same for group privacy management in Section 5.2; and study the relationship between privacy management and perceived privacy control in Section 5.3.

4. Method

4.1. Research sample

To test the formulated hypotheses, a survey was administered. Based on literature study, we developed an online survey that measured group and individual privacy management strategies and its predictors. We focused on individual and group privacy management of members of the KSJ as described in Section 3.1.

In the spring of 2013, and in collaboration with the national holding of KSJ the survey was ad randomly distributed among 150 local groups.[5] The survey was sent out electronically to the three oldest bans and all leaders of a local group.[6] The original sample consisted of 1011 people. After data cleaning, we were left with 900 valid responses. The 111 responses that were deleted contained a high amount of missing data (i.e. respondents who only filled in the demographic measures). Participants ranged from 13 to 37 years old ($M = 18.93$, $SD = 3.08$). 531 women (59%) and 369 men (41%) filled in the survey. Most respondents were either secondary school students (35.78%) or attending college (54.67%). Considering their role within the youth organization, 31% were members and 69% leaders. Regarding the composition of the youth organization, 25.44% girls and 16.44% boys belonged to segregated groups, whereas the majority reported a gendered-mixed group (58.11%) (see Table 1).

4.2. Measures

In this section, we operationalize all the measures. In all scales mentioned, the respondents were asked to rate items on a 7-point Likert scale, ranging from "strongly disagree" to "strongly agree". Where needed, we included the option "I don't know" or "not applicable" to prevent a bias from occurring.[7] We investigated the internal structure of the scales using exploratory factor analyses (EFA) and measured the reliability of the scales using Cronbach's alpha. The different items of the scales are listed in Appendix A. In the factor matrix tables we present the factor loadings (after Varimax rotation) of the factors that were retained and left out factor loadings that were .3 or less.

4.2.1. Individual and group privacy management measures

Individual privacy management (IPM) represents one of the dependent measures in this study. The factor analysis differentiates three factors which together account for 52.18% of the total variance Table 2. The first factor includes items as "I am careful with who I accept friend request from" and "I make sure that only friends can see my profile." We label this first factor as *basic privacy management*, the second factor we label as *advanced privacy management* (e.g. "I make use of Facebook lists when posting information") and the third and final factor we label as *appearance management* (e.g. "I review photos friends tag me in before they appear on my timeline"). After the reliability testing we noticed that factor two ($\alpha = .539$) and three ($\alpha = .275$) had a rather low to very low internal consistency. We only included factor one for further analyses ($\alpha = .723$, $M = 5.67$, $SD = .980$), consisting of seven items Table 2.

Group privacy management (GPM) presents the other dependent measure in this study. Because we focus on the unified boundary coordination of youth organizations we look at how members coordinate privacy rules. In the questionnaire we asked for different group strategies, such as agreeing on rules of thumb on what content can be disclosed or collectively defining the appropriate audience when disclosing shared information. The factor analysis differentiated three factors and together accounted for 61.79% of the total variance (see Table 3). We label the first factor as *group privacy guidelines* (i.e. "Our youth organization has

[5] The employees of the KSJ National electronically sent out the survey to the persons in charge of a local group. We did not have direct contact with the youth organizations for privacy reasons. They sent out the survey to 150 out of 276 groups only because they also planned other surveys and did not want to completely exhaust their population.

[6] Facebook requires everyone to be at least 13 years old to create an account.

[7] Exploratory interviews with Facebook users indicated that many did not know about Facebook lists. Not including the option "I don't know" would lead to biased results.

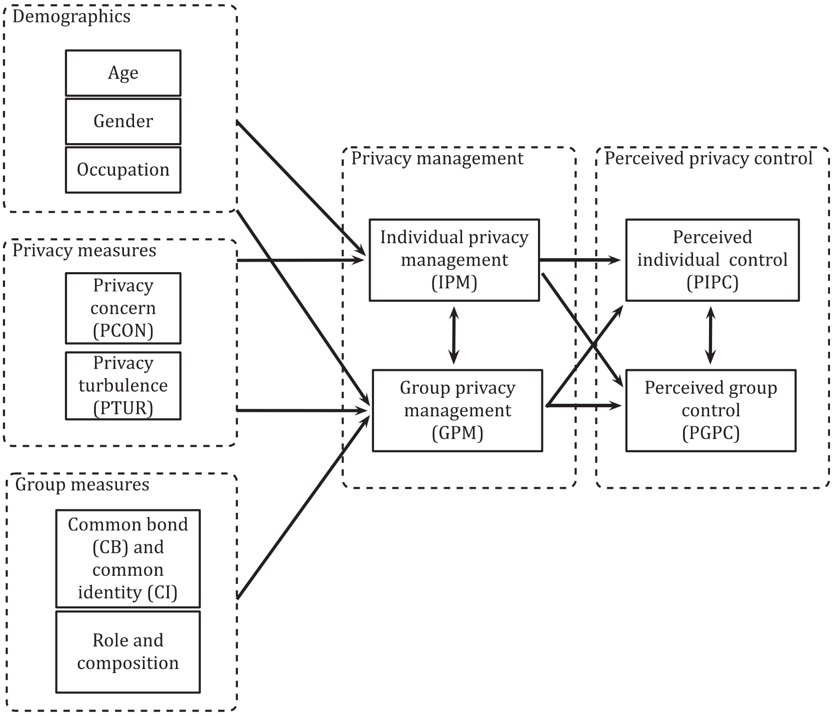

Demographics
Age
Gender
Occupation
Privacy measures
Privacy concern (PCON)
Privacy turbulence (PTUR)
Group measures
Common bond (CB) and common identity (CI)
Role and composition
Privacy management
Individual privacy management (IPM)
Group privacy management (GPM)
Perceived privacy control
Perceived individual control (PIPC)
Perceived group control (PGPC)

Fig. 1. Proposed research model.

Table 1
Respondents' demographics.

Demographics	Percent	*N*
Age	*M* 18.93 (SD 3.08)	900
Women	59	531
Men	41	369
Occupation		
Secondary school student	35.9	323
College student	54.8	493
Employed	8.2	74
Job seekers	1.1	10
Group variables		
Organization role		
Members	31	279
Leaders	69	621
Composition of organization		
Boys only	16.44	148
Girls only	25.44	229
Mixed	58.11	523

Table 2
Individual privacy management factor matrix (IPM).

Items	Factor 1 basic privacy management	Factor 2 advanced privacy management	Factor 3 appearance
Item 3	**.504**		
Item 4	**.538**		.420
Item 8	**.647**		
Item 10	**.407**		
Item 7	**.651**		
Item 5	**.433**	.312	
Item 6	**.371**	.423	
Item 2		.502	.394
Item 9		.469	
Item 1			
Eigen value	2.972	1.186	1.060
% of variance	29.71	11.86	10.60
KMO	.813		
Bartlett's test (approx. chi square)	781.025***		

Note: Factor loadings for items included in the regression models appear in bold.
*** P < 0.001.

guidelines with regard to what information can be posted in Facebook''). The items in the second factor all refer to *information management* (i.e. ''I don't fill in all information that is requested by Facebook'') and the last factor refers to *encryption* (''On the newsfeed we talk in a language so only fellow members can understand''). Factor two has low internally consistency ($\alpha = .480$). We only included factor one, consisting of four items, in further analyses ($\alpha = .857$, $M = 3.79$, SD = 1.75) (Table 3).

4.2.2. Demographic measures

In the regression models we included three demographic variables: gender, age, and occupation. We considered age a continuous variable and gender a dummy variable (women = 1). For occupation we used secondary school students as the baseline category to which the other occupation-types are compared in the regression models. We merged the employed and job seekers categories because both are confronted with an employer audience.

4.2.3. Group measures

4.2.3.1. Role and composition. The youth organization differentiates between ''leaders'' and ''members''. The former category applies to those who are attributed an educative role within the organization. The latter are not. Regarding the composition of the organization, we made a distinction between gender-segregated (boy or girl only) and gender-mixed groups. In the regression models, leaders and male organizations are treated as the baseline category for comparison.

4.2.3.2. Common bond and common identity. In our analysis we included the reasons for identifying with one's group. We adapted the scales of Prentice et al. (1994) to measure common bond (CB)

Table 3
Group privacy management factor matrix (GPM).

Items	Factor 1 group privacy guidelines	Factor 2 information management	Factor 3 encryption
Item 2	**.784**		
Item 4	**.761**		
Item 9	**.836**		
Item 1	**.572**	.488	
Item 7		.430	
Item 8		.386	
Item 6			.739
Item 5			
Item 3			
Eigen value	3.629	1.290	1.002
% of variance	36.32	14.33	11.14
KMO	0.816		
Bartlett's test (approx. chi square)	1011.376***		

Note: Factor loadings for items included in the regression models appear in bold.
*** $P < 0.001$.

Table 4
Common bond and common identity factor matrix (CB and CI).

Items	Factor 1 common bond	Factor 2 common identity
Item 6	**.842**	
Item 8	**.683**	
Item 7	.364	.303
Item 5	.440	**.429**
Item 1	.481	**.444**
Item 4		**.572**
Item 2		**.570**
Item 3		**.555**
Eigen value	3.226	1.165
% of variance	40.33	14.56
KMO	0.805	
Bartlett's test (approx. chi square)	1704.474***	

Note: Factor loadings for items included in the regression models appear in bold.
*** $P < 0.001$.

Table 5
Privacy concern factor matrix (PCON).

Items	Factor 1 privacy concern
Item 1	**.798**
Item 2	**.790**
Item 3	**.912**
Item 4	**.899**
Item 5	**.701**
Eigen value	3696
% of variance	73,92
KMO	.805
Bartlett's test (approx. chi square)	1704.474***

Note: Factor loadings for items included in the regression models appear in bold.
*** $P < 0.001$.

and common identity (CI) and used a 7-point Likert scale instead of a 9-point Likert scale, to obtain uniform scales throughout the entire survey. The factor analysis of all the items also revealed a two-factor solution: common identity ($\alpha = .707$, $M = 5.54$, SD = .80) and common bond ($\alpha = .766$, $M = 6.02$, SD = .95). After testing for internal consistency, we left out item seven (Table 4).

4.2.4. Privacy measures

4.2.4.1. Privacy concern. To measure privacy concern (PCON), we used the privacy concern scale, as developed by Xu, Dinev, Smith, and Hart (2011) and operationalized it for social privacy issues in Facebook. Because one factor was extracted, the analysis only shows the non-rotated results (Table 5). This single factor accounts for 73.92% of the total variance. Our analysis proves PCON, a five-item scale, to be one-dimensional and very consistent ($\alpha = .911$, $M = 4.07$, SD = 1.53).

4.2.4.2. Perceived privacy control. For privacy control we focused on individual and group-perceived privacy control. The factor analysis confirms this distinction and revealed a two-factor solution: *perceived individual privacy control* (PIPC) ($\alpha = .758$, $M = 5.70$, SD = 1.18), consisting of items three, four and five and *perceived group privacy control* (PGPC) ($\alpha = .715$, $M = 4.86$, SD = 1.38), consisting of items one and two (Table 6).

4.2.4.3. Privacy turbulence. According to CPM, people who have experienced privacy turbulence will have stricter privacy rules in managing their privacy. We operationalized four dimensions of privacy turbulence, following two axes: who is the perpetrator and who is the victim? We asked the participants whether they had experienced turbulence (i.e. "Have you ever experienced an embarrassing incident in Facebook, caused by someone else?"). As the reported turbulence experienced by the local groups caused by themselves ($n = 6$) was very low, we only focused on individual turbulence caused by others ($n = 157$) and by themselves ($n = 96$), and group turbulence caused by others ($n = 53$). In the regression models, not having experienced turbulence is considered the baseline category.

5. Results

Our analyses follows the model outlined in Fig. 1. We first measure the effect of the predictors on individual privacy management (IPM). Next, we measure the effects on group privacy management (GPM). We end by exploring the association between privacy management and perceived privacy control.

To determine the quality of the predictors, we made use of a hierarchical regression method, which allowed us to analyze the effect of predictors after controlling for other variables and account for the increment in variance. The change in the R^2 at each step in the analyses will be provided. To explain the variance in IPM, two linear regression models were run (see Table 7). Model 1 includes demographic variables, whereas model 2 incorporates privacy specific variables. To understand how the different predictors influence GPM, we also incorporated a model with only group variables (see Table 8). We found no violations testing the assumptions of linear regression.

5.1. Individual privacy management

H1 and H2 asked about the relationship between age and gender and IPM. The data indicates a positive relationship, where older individuals are more likely to make use of individual privacy management strategies. The positive gender coefficient indicates that women are more likely to make use of individual privacy management strategies than men. When controlling for privacy concerns and turbulence, in model 2 the effects remain. No significant effects were found between the occupation of the respondents and IPM (H3). Our model supports for H4 but not entirely for H5. Individuals who have a higher privacy concern engage with more privacy management strategies. The same cannot be said about individuals who have experienced turbulence caused by others.

Table 6
Perceived individual and group privacy control factor matrix (PGPC and PIPC).

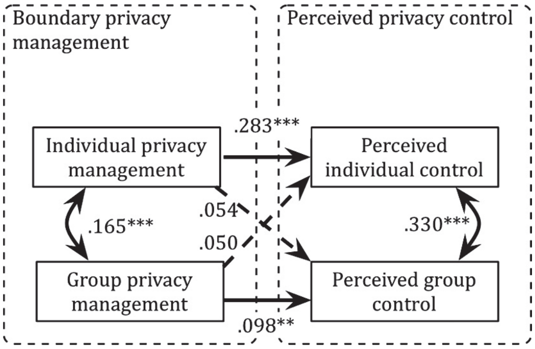
Items	Factor 1 perceived individual privacy control	Factor 2 perceived group privacy control
Item 3	**.705**	
Item 4	**.750**	
Item 5	**.524**	
Item 1		**.694**
Item 2		**.860**
Eigen value	2.467	1.127
% of Variance	49,34	22.55
KMO		.676
Bartlett's test (approx. chi square)		999.161***

Note: Factor loadings for items included in the regression models appear in bold.
*** $P < 0.001$.

We found the opposite of the direction predicted by H5 to be true. No significant effect between turbulence caused by oneself and IPM was observed. In total, the model accounts for about 12% of the variance in IPM (Table 7).

5.2. Group privacy management

When looking at the relationship between age, gender and GPM, the data indicates a different outcome than with IPM. Model 1 indicates a positive relationship between age and GPM (H6). When controlling for group variables in Model 2, we see the relationship has disappeared. Instead, a strong relationship is found between the role one is attributed and the usage of group privacy management strategies. We found a negative relationship between being a member and GPM. Hence, leaders are more likely to use group privacy management strategies than members (H10). As for gender (H7), we found a negative relationship with GPM, even when we controlled for group and privacy variables. As with IPM, no effects were found for occupation (H8) and composition (H11). Considering H9, the data indicates that common bond (attachment to individual members) positively influences GPM. No effects were found between common identity and GPM. Model 3 confirms H12 that members with more privacy concern score higher on GPM. Lastly, no effects were found between privacy turbulence caused by others and GPM (H13). Looking at the proportion of the variance in GPM explained by the dependent variables, we notice that especially the group variables exert an influence (Table 8).


Boundary privacy management
Perceived privacy control
Individual privacy management
Perceived individual control
Group privacy management
Perceived group control
.283***
.165***
.054
.050
.330***
.098**

***P < 0.001 **P < 0.01 *P < 0.05

Fig. 2. The relationship between privacy management and perceived privacy control (standardized coefficients, β).

5.3. Privacy management and perceived control

In the previous two sections we looked at the predictors of individual and group privacy management. In this section we solely look at the relationship between privacy management and perceived privacy control, both on the individual and group level (see Fig. 2).

The results show a clear relationship between IPM and perceived individual privacy control (PIPC) ($\beta = .283$, $p < .001$) (H14) and group privacy management and perceived group privacy control (PGPC) ($\beta = .098$, $p < .001$) (H15). No significant relationships were found between IPM and PGPC on the one hand and GPM and PIPC the other hand. When looking at the relationship between IPM and GPM we found a mutual relationship, indicating an indirect effect between IPM and PGPC on the one hand and GPM and PIPC on the other hand (H16).

6. Discussion

6.1. Focus of study

For adequate privacy management, Petronio (2002) indicates that people both need to develop privacy rules around the self and groups. The goal of this study was to investigate which variables influence individual and group privacy management in Facebook. As far as we know, no research has been done that studies the predictors of group privacy management or studies its relationship with individual privacy management on SNSs.

Table 7
Summary of hierarchical regression analysis for variables predicting individual privacy management ($n = 900$).

	Model 1		Model 2	
	B (S.E.)	β	*B* (S.E.)	β
Demographics				
Age	.073 (.016)***	.232***	.062 (.016)***	.197***
Women	.399 (.068)***	.202***	.288 (.069)***	.146***
College student	.081 (.093)	.042	.093 (.091)	.048
(un)employed	−.214 (.170)	−.066	−.189 (167)	−.058
Privacy variables				
Privacy concern			.093 (.022)***	.147***
Ind. turbulence (self)			−.109 (.086)	−.045
Ind. turbulence (others)			−.423 (.105)***	−.142***
Constant	4.018 (.281)***		3.979 (.280)***	
R^2	.08		.12	

*** $P < 0.001$.

Table 8
Summary of hierarchical regression analysis for variables predicting group privacy management (n = 900).

	Model 1		Model 2		Model 3	
	B (S.E.)	*β*	*B* (S.E.)	*β*	*B* (S.E.)	*β*
Demographics						
Age	.140 (.033)***	.228***	−.012 (.037)	−.019	−.023 (.038)	−.038
Women	−.329 (.125)**	−.092**	−.527 (155)**	−.148**	−.556 (.156)***	−.156***
College student	.288 (.179)	.082	.134 (.174)	.038	.159 (174)	.045
(un)employed	−.209 (.317)	−.035	.036 (.307)	.006	.095 (307)	.016
Group variables						
Member			−1.334 (.186)***	−.339***	−1.332 (.186)***	−.339***
Girls only			.400 (.239)	.101	.376 (.240)	.095
Gendered mixed			.289 (188)	.082	.285 (.188)	.081
Common bond			.209 (.069)**	.113**	.220 (.070)**	.119**
Common identity			.071 (.085)	.032	.071 (.084)	.032
Privacy variables						
Privacy concern					.094 (.039)*	.083*
Privacy turbulence (others)					−.071 (.763)	−.010
Constant	1.188 (.561)*		2.704 (.820)**		2.480 (.824)**	
R^2	.08		.16		.17	

* $P < 0.05$.
** $P < 0.01$.
*** $P < 0.001$.

6.2. Findings and reflections

In line with the CPM we found a positive relationship between age and IPM, meaning that older people are more likely to make use of individual privacy management strategies in Facebook. In line with the results of Lewis et al. (2008) and Litt (2013), we found that women are also more likely to score higher on IPM in comparison with men. CPM indicates privacy concern and turbulence as predictors of privacy management (Petronio, 2002). Indeed, we found a positive relationship between privacy concern and IPM and privacy concern and GPM. However, the data is in disagreement with the CPM theory considering privacy turbulence. For IPM and GPM, we differentiated between turbulence caused by oneself and by others. Our results do not support a relationship between privacy turbulence caused by oneself and IPM and turbulence caused by others and GPM, but does support a relationship for privacy turbulence caused by others and IPM. The latter relationship, in contrast with the CPM theory, was negative. Several explanations are plausible: users might think their efforts are futile to fix turbulence caused by others or think they lack the skills to adapt their privacy management strategies, Future research is necessary to investigate these relationships. Potentially, our results could also be biased, because only a small number of people reported individual privacy turbulence caused by others (17.4%).

What was particularly intriguing about our results was the difference between the demographic predictors and individual and group privacy management. The data suggests that men are more likely to make use of group privacy management than women, the opposite of what we found for IPM. Another intriguing difference is the relationship between age and GPM. When controlling for the role one is attributed in their youth organization we found that the effect of age disappeared, indicating that group measures are more important than age in explaining the variance in GPM.

The data indicates a positive relationship between common bond and GPM. Thus, people who score higher on common bond are more likely to use group privacy management strategies in Facebook. No such relationship was found for common identity. Ren et al. (2007) indicate that the design of online communities influence people's interactions in that community. Research has shown that SNSs are a place to meet with your offline friends (e.g., Ellison et al., 2011). Our own data confirms this too, 84.89% of the respondents indicate that they use Facebook to maintain contact with their offline friends. Therefore we do not find it surprising that identifying with your friends within a group (common bond) is important for GPM in Facebook.

Lastly, we explored the relationship between privacy management and perceived privacy control. The CPM theory claims that it is necessary to develop individual and group privacy rules for adequate privacy management (Petronio, 2002). Our data confirms this claim and found a positive indirect relationship between GPM and PIPC and IPM and PGPC. Moreover, the data indicates a positive mutual effect between PIPC and PGPC. Hence, for adequate privacy management and feeling of control, it is necessary to focus beyond the individual.

6.3. Strengths and weaknesses

In this study we solely focused on how people share information with other people. Hence, we did not include—using the concept of Stutzman et al. (2012)—*silent listeners*, such as SNSs themselves, third-party apps, and advertisers, as an audience when disclosing in SNSs. We consider this to be both a strength and weakness. One the one hand, we control for the audience one has in mind when disclosing. On the other hand, we do not take into account these silent listeners or study how the co-presence of silent listeners and other SNS users, as an audience, influences users' disclosure behaviors.

Many authors have studied the variety of privacy management strategies of users in SNSs (e.g., boyd, 2008; Raynes-Goldie, 2010; Tufekci, 2008; Braendtzæg et al., 2010; boyd et al., 2011; Kramer-Duffield, 2010; Lampinen et al., 2011; Lewis et al., 2008; Litt, 2013; Young & Quan-Haase, 2013). When operationalizing the items for our two main dependent variables, individual and group privacy management, we included different sorts of strategies discussed in previous research: preventive and corrective, and social and structural. After investigating the internal structure of the scales, however, we left out certain items in the regression models. We did include the mean and standard deviation of each item in Appendix A, which also gives an overview of the different strategies and to what extend these are used.

Recently, there has been a push for studying privacy on a *collective* level. Within our research, we studied the individual and group privacy management strategies of a youth organization. People, however, belong to many different groups and therefore develop different sets of privacy rules. We only took into account one youth organization to study group privacy management, hereby limiting the strengths of our results. Different groups might define information ownership differently or individual and group privacy management strategies might contradict one another. Also, because we did not send out the survey ourselves and had no direct contact with the youth organizations, we were not able to take into account the hierarchical character of the data and study the data on different levels (members (level one) and the local group (level two)) by means of multi-level analysis (MLA). For example, we found differences between gender and group privacy management. This can be paradoxical because those men and women could belong to the same group. It might as well be, however, that men score higher on group privacy management and behold a different interpretation on managing privacy on a group level than women, even when belonging to the same group.

6.4. Recommendations

Individuals develop personal privacy rules to manage the personal information flow. Group information is connected to the self but is often beyond individual control. Therefore people develop group privacy rules together with others. This study sought to understand the predictors of individual and group privacy management of members of a youth organization and its relationship with perceived privacy control.

We argue that it is necessary for users of SNSs to negotiate privacy boundaries together with others. This is likely to facilitate privacy management and prevent privacy turbulence from occurring. We included different group measures in our analyses and found common bond and role (member or leader) to be the strongest predictors of group privacy management. Based on the results, we advise youth organizations to negotiate privacy boundaries with all members and underline the importance of being attached to individual members for group privacy management.

Different dimensions of privacy management remain to be studied. For example, do groups apply the same privacy rules in offline settings, in other SNSs, in non-technological settings, and so on? Overall, the findings indicate the importance of studying privacy on a group level. When we solely focus on how people manage individual privacy rules around the self we ignore the group privacy rules and deprive ourselves of understanding the relationship between both. Comparing the predictors of IPM and GPM we found some surprising differences—for example the relationship between age and IPM on the one hand and age and GPM on the other hand—that cannot be explained by the variables we integrated in our survey, leaving us with some unanswered questions. We argue that it is necessary to continue studying how individuals and groups manage their privacy in order to obtain a holistic view on privacy management, and turn away from individual-centric notions of privacy.

Acknowledgement

The research leading to these results has received funding from the Strategic Basic Research (SBO) Program of the Flemish Agency for Innovation through Science and Technology (IWT) in the context of the SPION project (www.spion.me) under grant agreement number 100048. The authors thank Carina Veeckman, Paulien Coppens, Bram Lievens, Sarah Talboom, members of the SPION project, and the anonymous reviewers for their constructive feedback and suggestions regarding this study.

Appendix A

Below privacy measures focus on how information is shared with other people. In this study we do not focus on institutional privacy and the respondents' relationship with SNS providers and other third parties.

No.	Details of items	*M*	S.D.
IPM	*Individual privacy management*		
Item 1	I make use of private communication channels (e.g., Facebook chat) when I want to talk about sensitive subjects	4.76	2.054
Item 2	I review photos friends tag me in before they appear on my timeline	4.34	2.298
Item 3	I make sure that only friends can see my profile	5.95	1.602
Item 4	I only post information in Facebook that is suitable for everyone that can see	6.21	1.194
Item 5	I untag myself from photos I don't find appropriate	5.87	1.659
Item 6	When I install an application in Facebook, I make sure that I am the only who can see this	5.24	1.837
Item 7	I don't fill in all the information that is requested by Facebook	6.14	1.239
Item 8	I am careful with who I accept friend requests from	6.13	1.202
Item 9	I make use of Facebook lists when posting information	3.66	1.896
Item 10	I defriend those I no longer want to see my status updates	5.39	1.670
GPM	*Group privacy management*		
Item 1	Our youth organization has guidelines with regard to what information can be posted in Facebook	4.50	1.876
Item 2	Our youth organization has rules about accepting parents in Facebook	3.65	1.931
Item 3	We make use of Facebook groups to share information about our youth organization	6.43	.992
Item 4	In our youth organization we have rules about accepting members/leaders in Facebook	4.37	2.127
Item 5	In our youth organization we make use of Facebook lists to share information	3.87	1.952
Item 6	On the newsfeed we talk in a language so only fellow members can understand	1.93	1.213
Item 7	We ask to delete damaging information about our youth organization	4.27	2.091
Item 8	Our youth organization makes use of multiple (social network) sites to separate information	3.74	2.043

Appendix A (*continued*)

No.	Details of items	*M*	S.D.
Item 9	Our organization has worked out various agreements in Facebook	4.08	1.923
CI & CB	*Common identity and common bond* (Prentice et al., 1994)		
Item 1	How important is belonging to your youth organization to you?	6.13	.916
Item 2	How accurate would it be to describe you as a typical member of your club?	4.77	1.290
Item 3	How often do you acknowledge the fact that you are a member of your youth organization?	5.31	1.295
Item 4	How good would you feel if you were described as a typical member of your youth organization?	5.79	1.282
Item 5	How often do you talk about your youth organization?	5.70	1.040
Item 6	How close do you feel to the other members of your youth organization?	5.94	.990
Item 7	How many members of your youth organization have influenced your thoughts and behaviors?	4.87	1.249
Item 8	How many people in your youth organization do you consider friends?	6.09	1.119
PCON	*Privacy concern (based on* Xu et al., 2011)		
Item 1	I am worried that others misuse the information I post in Facebook	4.14	1.739
Item 2	I am worried that others find private information about me in Facebook	3.91	1.751
Item 3	I am worried about posting information in Facebook, because of what others might do with it	4.14	1.742
Item 4	I am worried about posting information in Facebook, because it might be used in ways I had not foreseen	4.32	1.742
Item 5	I am worried about others placing embarrassing information about me in Facebook	4.28	1.767
PCTL	*Perceived privacy control (based on* Xu et al., 2011)		
Item 1	I believe that I control who has access to my personal information in Facebook	5.56	1.351
Item 2	I believe that I control the information I post in Facebook	5.95	1.166
Item 3	I believe that our youth organization controls what information leaders post in Facebook	5.33	1.549
Item 4	I believe that our youth organization controls what information members post in Facebook	3.98	1.924
Item 5	I believe that our youth organization controls who has access to information that is of our concern	5.57	1.446

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle, & G. Danezis (Eds.), *Privacy Enhancing Technologies Workshop* (pp. 36–58). Cambridge, UK.

boyd, d. (2008). *Taken out of context: American teen sociality in networked publics*. University of California, Berkely, California. Doctoral dissertation.

boyd, d. (2011). Networked privacy. In *Personal democracy forum*. New York. <http://www.danah.org/papers/talks/2011/PDF2011.html> Retrieved 29.07.13.

boyd, d., & Marwick, A. (2011). Social steganography: Privacy in networked publics. In *International Communication Association*. Boston, MA.

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

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

Child, J. T., Petronio, S., Agyeman-Budu, E., & Westermann, D. A. (2011). Blogg scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior, 27*(5), 2017–2027.

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). New York: Peter Lang.

Dimicco, J. M., & Millen, D. R. (2007). Identity management: Multiple presentations of self in Facebook. In *International ACM conference on Supporting group work* (pp. 383–386). New York, USA.

Ellison, N., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society, 13*(6), 873–892.

Hargittai, E., & Litt, E. (2013). Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy, 11*(3), 38–45.

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society, 30*(6), 377–386.

Kramer-Duffield, J. (2010). *Beliefs and uses of tagging among undergraduates*. University of North Carolina, Chapel Hill. Doctoral dissertation.

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). We're in it together: Interpersonal management of disclosure in social network services. In *Annual conference on human factors in computing systems* (pp. 3217–3226). New York, USA.

Lenhart, A. (2009). *Adults and social network websites*. Washington, DC: Pew Internet & American Life Project.

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.

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*(4), 1649–1656.

Madden, M. (2012). *Privacy management on social media sites*. Washington, DC: Pew Internet & American Life Project.

Papacharissi, Z. (2012). Without you, I'm nothing: Performances of the self on twitter. *International Journal of Communication, 6*(1), 1989–2006.

Parks, M. R. (2010). Social network sites as virtual communities. In Z. Papacharissi (Ed.), *A networked self. Identity, community, and culture on social network sites* (pp. 105–123). New York, Routledge.

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

Prentice, D. A., Miller, D. T., & Lightdale, J. R. (1994). Asymmetries in attachments to groups and to their members: Distinguishing between common-identity and common-bond groups. *Personality and Social Psychology Bulletin, 20*(5), 484–493.

Quinn, K. (2012). Understanding online privacy at midlife: Privacy management as an ecosystem. In *Amsterdam privacy conference* (pp. 1–11). Amsterdam.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1).

Ren, Y., Kraut, R., & Kiesler, S. (2007). Applying common identity and bond theory to design of online communities. *Organization Studies, 28*(3), 377–408.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Steinfield, C., Ellison, N., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology, 29*(6), 434–445.

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), 7–41.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36.

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media, 56*(4), 451–470.

Vitak, J., & Ellison, N. (2012). 'There's a network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media & Society, 15*(2), 243–259.

Xu, H. (2012). Reframing privacy 2.0 in online social networks. *University of Pennsylvania Journal of Constitutional Law, 14*(14), 1077–1102.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(2), 798–824.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push–pull technology in pirvacy calculus: The case of location-based services. *Journal of Management Information Systems, 24*(3), 135–174.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *The Data Base for Advances in Information Systems, 40*(1), 38–51.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479–500.

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior, 24*(5), 1816–1836.