IDIS (2009) 2:39–63
DOI 10.1007/s12394-009-0019-1

Privacy concerns and identity in online social networks

Hanna Krasnova · Oliver Günther · Sarah Spiekermann · Ksenia Koroleva

Received: 18 November 2008 / Accepted: 9 July 2009 / Published online: 1 October 2009

Abstract Driven by privacy-related fears, users of Online Social Networks may start to reduce their network activities. This trend can have a negative impact on network sustainability and its business value. Nevertheless, very little is understood about the privacy-related concerns of users and the impact of those concerns on identity performance. To close this gap, we take a systematic view of user privacy concerns on such platforms. Based on insights from focus groups and an empirical study with 210 subjects, we find that (i) Organizational Threats and (ii) Social Threats stemming from the user environment constitute two underlying dimensions of the construct "Privacy Concerns in Online Social Networks". Using a Structural Equation Model, we examine the impact of the identified dimensions of concern on the Amount, Honesty, and Conscious Control of individual self-disclosure on these sites. We find that users tend to reduce the Amount of information disclosed as a response to their concerns regarding Organizational Threats. Additionally, users become more conscious about the information they reveal as a result of Social Threats. Network providers may want to develop specific mechanisms to alleviate identified user concerns and thereby ensure network sustainability.

Keywords Online social networks · Privacy concerns · Measures · Identity · Structural equation modeling

H. Krasnova (✉) · O. Günther · S. Spiekermann · K. Koroleva
Humboldt-Universität zu Berlin, Berlin, Germany
e-mail: krasnovh@wiwi.hu-berlin.de

S. Spiekermann
European Business School,
Schloss Reichartshausen,
Oestrich-Winkel, Berlin, Germany

Abbreviations

AVE	Average Variance Extracted
CFA	Confirmatory Factor Analysis
EFA	Exploratory Factor Analysis
FGQ	Focus Group Quotation
HR	Human Resources
MM	Measurement Model
OSN	Online Social Network
PCOSN	"User Privacy Concerns on OSNs" construct
SD	Standard Deviation
SEM	Structural Equation Model
SM	Structural Model

Introduction

Online Social Networks (OSNs) such as Facebook or StudiVZ have evolved into popular Web places where users communicate and share updates with friends. This facilitated exchange of information helps create social capital by bringing individuals closer together and maintaining existing relationships (Ellison et al. 2007). However, media-driven user privacy concerns might damage the self-sustainability of OSNs and ultimately ruin their public value. Motivated by these developments, this study identifies user privacy concerns specific to OSNs and explores their impact on self-disclosure dynamics.

Indeed, participation in OSNs is closely related to information disclosure, an integral part of the identity construction process on these sites. Building on the individual's desire to engage in impression management, OSN platforms induce users to report on their experiences, share news, and upload photos in their public space. For example, "*more than 1 billion pieces of content"* including links, news updates, photos, etc. are weekly shared on the Facebook platform (Facebook 2009). User-provided content is also an important determinant of the OSN commercial success (Krasnova et al. 2008). In fact, to remain sustainable, OSN providers must support user communication as without supply of fresh material, users may lose interest and refrain from coming back (Boyd and Heer 2006). On the other hand, mutual updates motivate users to return and stay active.

While users want to communicate and present themselves to others, many are becoming increasingly vigilant with regard to the information they disclose. A chain of privacy-related public scandals, along with related media coverage revealing questionable information handling practices, has started to increase user awareness with respect to the privacy threats users face (Wieschowski 2007). For example, the introduction of the Beacon application, which displays recent purchases, and the News Feed feature, which makes user actions public (Boyd 2008), have made more users aware of the scope and reach of the information they publish. As a consequence, OSN groups such as "Petition: Facebook, stop invading my privacy" or "Facebook Privacy Awareness Syndicate" emerged. Such developments can undermine the self-sustainability of the OSN platforms in the long term.

However, despite the importance of these developments for the OSNs' business and public value, researchers know little about the privacy concerns of users and how those concerns impact users' self-presentation and self-disclosure strategies.

Even though Acquisti and Gross (2006), Dwyer et al. (2007), Krasnova et al. (2009), Tufekci (2008), Stutzman (2006) have made the first steps to determine the impact of privacy concerns on behaviour, the findings remain limited and are often of controversial nature. What privacy threats concern users the most? How do privacy concerns impact individual self-communication? What can OSN providers do to minimize these concerns, ensure their long-term sustainability and maintain healthy impression management levels? These questions must be answered to ensure that the public value of OSNs—their ability to create social capital—is retained. Looking for answers to these questions, we take a systematic view of the user privacy concerns on OSNs and explore their impact on self-disclosure variables.

This paper is structured as follows: In the "Identity Construction and Privacy Concerns" section, we provide a detailed review of relevant studies. We show that state of the art literature does not have a precise answer on how user privacy concerns impact OSN participation. This may be partly due to a lack of validated measurement instruments addressing OSN specifics. To close this gap, in the next section, "Stage 1: Understanding User Privacy Concerns," we analyze the results of two focus groups we conducted to capture relevant dimensions of individual privacy concerns particular to OSN platforms. Identified dimensions were operationalized and validated in a survey with 210 subjects described in the section "Stage 2: Validating 'User Privacy Concerns on OSNs' Construct". We find that (i) Organizational Threats and (ii) Social Threats stemming from the user environment constitute two underlying dimensions of the construct "Privacy Concerns in Online Social Networks". Building on these insights, in the section "Stage 3: Identity Construction and Privacy Concerns," we examine the impact of these two types of privacy concerns on three dimensions of self-disclosure: Amount, Honesty, and Conscious Control. Our findings reveal interesting dynamics in the self-disclosure behaviour of users. Additionally, we provide insights relevant for the OSN provider, who can then develop specific mechanisms to alleviate identified user concerns and thereby ensure network sustainability.

Identity construction and privacy concerns

Boyd and Ellison (2007) describe OSNs as online environments in which people create public or semi-public self-descriptive profiles and make links to other people. Public self-presentation is a central part of OSN participation. The abundance of impression management activities (Goffman 1959) on OSNs is related to the asynchronous nature of communication on these platforms (Walther 1996). Furthermore, due to their emphasis on the *verbal and linguistic cues,* OSNs enable individuals with significant control over the impression they produce on others—an important advantage over face-to-face communication where *nonverbal* communication cues play a critical role (Ellison et al. 2006). These capabilities allow users not only to express their identity more fully, but also to express their latent and nested identities (Schau and Gilly 2003). In their profiles, users can report on their

experiences and achievements, upload photos, and display their list of connections, thereby projecting desirable associations and impressions. Apart from their profile, OSN participants are given opportunities to construct their identity by using applications, participating in discussions, blogging, or posting comments in public areas.

The content of self-presentation can be broadly referred to as self-disclosure (Schau and Gilly 2003). The information disclosure strategies an individual uses on the platform depend on that individual's particular goals (Gibbs et al. 2006). For example, those looking for *new* relationships might strategically disclose information to facilitate search for others, help to find the common ground and transmit desired signals (Lampe et al. 2007). Overall, OSNs allow users to pre-select what information they publish, giving them the opportunity to construct a public identity that may be closer to their "*ideal self*" (Higgins 1987). Boyd (2007) notes that user behaviour on OSNs is to a large extent determined by the desire to self-present, as OSNs allow users to unfold the most salient facets of their identity in front of significant others. Nevertheless, most users maintain a tightly integrated social network that consists primarily of real-life friends. This, combined with the non-anonymous nature of the platform, invisibly controls users' statements and thereby prevents them from engaging in exaggerated self-enhancement and misrepresentation—a phenomenon often observed in anonymous online forums, dating platforms, and chats (e.g. Brym and Lenton 2001). In this sense, identity created in OSNs is an idealized projection of the real-life "*actual self*".

However, rising privacy concerns have begun to compel users to reconsider their approach to self-communication on social networking sites. Boyd and Ellison (2007) argue that perceived privacy threats are changing the way users disclose information about themselves by undermining their ability to control and manage impressions and social contexts. This dynamics may have drastic negative consequences for the sustainability of OSNs. Unable to construct their identity in the desired way, users may in the end reduce their participation level or even leave the network—a scenario in which both commercial and public value of the OSN platforms gets destroyed.

Current research findings provide controversial insights into how privacy concerns shape user behavior on OSNs. Whereas several studies find support for a dichotomy between stated privacy concerns and actual revelation behavior (e.g. Acquisti and Gross 2006; Stutzman 2006; Tufekci 2008), Krasnova et al. (2009) show that users do reduce the amount of information they disclose in response to their privacy concerns. Due to transferability of the privacy risks to the offline world, Lusoli and Miltgen (2009) argue that young users may even abstain from using the appropriate electronic identity services to which OSNs belong.

Existing disagreement between research findings can also be partly due to the lack of validated measurement instruments addressing the unique character of OSNs. This deficiency is particularly evident for privacy concern scales. Overall, privacy concern is typically viewed and measured as a multidimensional construct (e.g. Malhotra et al. 2004; Smith et al. 1996). In the organizational context, Smith et al. (1996) have developed a "Concern For Information Privacy" (CFIP) Framework in which they differentiate between *collection, secondary use, improper access,* and *errors* concerns in the organizational context. Building on the CFIP, Malhotra et al.

(2004) have pointed out *collection, control,* and *awareness* of *the privacy practices* as dimensions of the Internet Users' Information Privacy Concerns (IUIPC).

Both CFIP and IUIPC have been widely applied in various settings. However, when exploring the social networking context, we notice that scholars tend to view concern for privacy in a distinctive manner. For example, apart from asking general questions related to accessibility and secondary use of information, Acquisti and Gross (2006) test a specific set of situations implying possible outcomes of profile accessibility, such as, for example, stalking. Furthermore, Gürses et al. (2008) distinguish between four categories of OSN-specific privacy breaches encompassing issues of indeterminate visibility of user profile information, separation of identities and aggregation as well as misappropriation and contested ownership of user data. Finally, Tufekci (2008) argues that the main source of privacy risks on OSNs lies in the inability of users to control the audience both spatially and temporally.

Hence, in addition to the common online privacy concerns typical for the E-commerce context arising as part of the interaction between a user and an OSN provider, OSN members are subject to the *specific* privacy-related risks rooted in the public and social nature of OSNs. For this reason, we argue that existing measures (e.g. Malhotra et al. 2004; Smith et al. 1996) are not sufficient to capture all relevant dimensions of user concerns in the OSN context.

Hogben (2007) has taken the first step to address this deficit by developing a broad overview of privacy threats specific to OSNs; these include digital dossier aggregation by third parties, online stalking, bullying, reputation slander, just to name a few. Furthermore, a recent report of the Internet Safety Technical Task Force (2008) elaborates on the privacy threats young people face on social networking platforms, which include online harassment and cyberbullying, sexual solicitation and exposure to problematic content. However, despite the encompassing nature of these studies as well as their contribution to the field, a user perspective on these and other privacy threats—user privacy concerns—has still received limited attention.

Summarizing, we find that only a limited number of studies examine the impact of user privacy concerns on the dynamics of self-presentation and self-disclosure. Discovered controversies between the obtained results from these studies may be partly due to the lack of valid instruments, which measure privacy concerns in the distinctive OSN context. We fill this gap by developing a taxonomy for users' privacy-related concerns and by examining their impact on various self-disclosure strategies.

Research approach

As shown in Fig. 1, the study involved three stages. Due to the lack of validated measurement instruments for capturing privacy concerns of OSN users, we first focused our effort on developing, operationalizing, and validating the construct "*User Privacy Concerns on OSNs*" (PCOSN) in the first two parts of our study. In the third part, we examined how identified concern dimensions influence various aspects of individual self-disclosure. As a whole, the study provides relevant insights into the dynamics of identity construction in the light of privacy concerns.

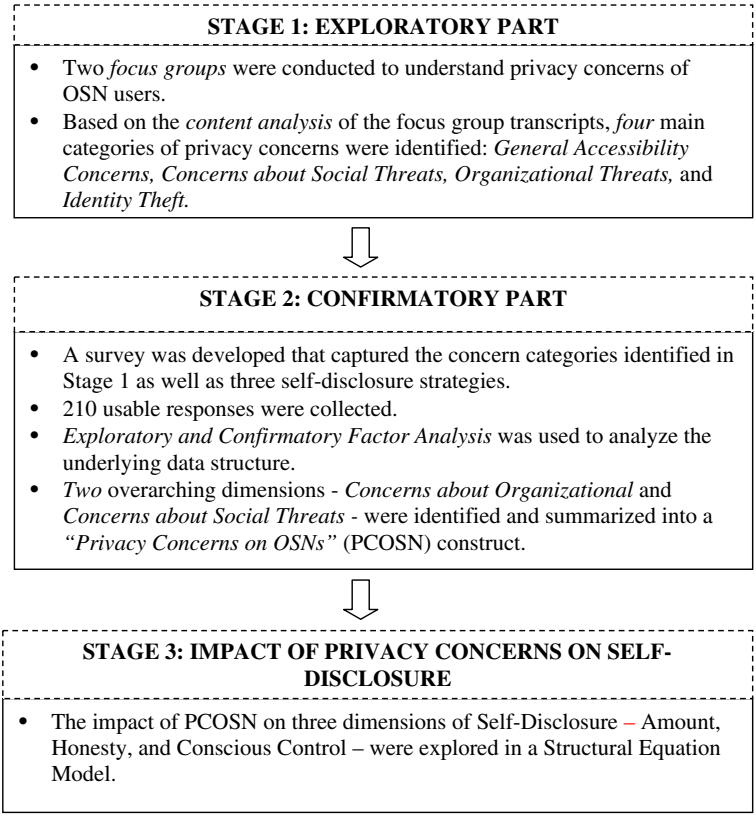

Fig. 1 Research framework

STAGE 1: Understanding user privacy concerns

Since few past studies have dealt with OSN-specific privacy concerns, two focus groups comprised of OSN users—all students—were assembled at the Institute of Information Systems in Berlin, Germany. A focus group is a popular method of exploratory research used to gain an understanding of consumer impressions, structure information, and generate empirically testable hypotheses (Churchill and Iacobucci 2002).

Both focus groups revolved around the same set of questions dealing with factors—motivators and impediments—behind OSN participation. In this paper, however, we concentrate mainly on user privacy concerns as a major impediment of OSN participation. With the help of the focus groups we aimed to identify which threats users are concerned about and how they affect the process of identity construction. We did not prompt participants about any specific threats which OSNs might involve, but rather asked open questions such as: "Do you feel safe when giving out your information on a social network? Why yes, Why not?".

As a result of privacy-related content analysis of the focus group transcripts, *four* main categories involving twelve sub-categories of privacy concerns were tentatively identified and grouped into a codebook: *General Accessibility Concerns, Concerns about Social Threats, Organizational Threats,* and *Identity Theft.* It is important to

Table 1 Results of the focus group content analysis: inter-coder agreement

Coder 1 / Coder 2	Agreement between both coders	Relative Importance
GENERAL ACCESSIBILITY		
• *By People*	**23**	**56,5%**
• *By Organizations*	**15**	
• *Improper Access*	**5**	
SOCIAL THREATS FROM USER ENVIRONMENT		
• *Uncontrollable Actions*	**10**	**21,1%**
• *Bullying*	**4**	
• *Stalking*	**2**	
ORGANIZATIONAL THREATS		
• *Collection by OSN Provider*	**2**	**21,1%**
• *Secondary Use by OSN Provider*	**4**	
• *Collection by Third Parties*	**1**	
• *Secondary Use by Third Parties*	**3**	
• *Marketing (Banners and Emails)*	**6**	
IDENTITY THEFT		
• *Identity Theft*	**1**	**1,3%**

note that whereas a tentative structure for our codebook involved some concern categories prompted by Hogben (2007) as well as Smith et al. (1996), most themes (categories and sub-categories) were deduced from the focus groups transcripts in the process of their analysis, as suggested by Ryan and Bernard (2000).

At the next step, two coders independently assigned 96 extracted keywords to the pre-defined codebook sub-categories. A resulting inter-coder reliability constituted 0.756 ($p<0.000$), which shows an acceptable level of agreement between the coders (Landis and Koch 1977). Table 1 provides a summary of the coding procedure: From the column "Agreement between both coders," one can infer for how many keywords both coders agreed that a keyword belonged to the same particular sub-category (76 keywords it total). The "Relative Importance" column provides the weight of a particular category, which can be interpreted as the relevance of a particular group of concerns.

General Accessibility was the most frequently mentioned concern. It refers to fears connected to *unwanted* access of the information provided on an OSN. Specifically, due to the public nature of these platforms, the information users provide can be potentially viewed by other parties for whom this information was not initially intended: fellow students, supervisors, subordinates, parents, just to name a few (Hewitt and Forte 2006). For example, in a longitudinal study, Lampe et al. (2008) show that an increasing number of users believe that future employers accessed their profile. At the same time less and less users perceive Facebook purely as a student space.

Focus group respondents differentiated between various dimensions of the *General Accessibility concern. Accessibility by People* (e.g. parents, a teacher) was the most prominent one: *"other people can really check the Internet and they will find everything about you"* (focus group quotation (FGQ). It was followed by a

concern about information *Accessibility to Organizations* (an HR agency, an insurance company):"*If you apply for a job, human resources department checks"* or *"all this information is available to CIA"* (FGQ). Respondents also mentioned concern over *Improper Access*, the notion that data might become available to unauthorized parties: *"it is easy to crack the account and they do that"* (FGQ).

Concerns about Social Threats, defined as fears stemming from the OSN user environment, were also mentioned frequently. These threats range from tagging a user in unwanted photos and leaving inappropriate comments about the user on their Wall or other public areas to user harassment or denigration on the platform. Within this category, respondents were mostly concerned about actions they could not control (*Uncontrollable Actions*): "*...somebody makes a picture and then links it... then people might see the picture I do not want [them] to [see]"* (FGQ). Bullying, defined by Hogben (2007, p. 4) as "*purposeful acts of harm"* which can take the form of harassment, offensive behaviour, secret sharing, public embarrassment and humiliation, emerged as another important concern: "*some people can really do revenge online"* (FGQ). By placing humiliating messages in the public areas of user's profile, bullies can denigrate a user in the eyes of relevant others and, hence, intrude into one's private sphere. Stalking, defined as threatening behaviour in which a perpetrator repeatedly contacts a victim, emerged as a concern of little importance: *"what if somebody is being not psychologically normal finds me somehow in the social network and gets obsessed"* (FGQ) and was excluded from the subsequent analysis.

Furthermore, participants were concerned about the C*ollection and Secondary Use* of their information *by Organizations*; discussing this concern, participants differentiated between *the OSN Provider, Third Parties*, and a generic category we call *Marketing*. Urged on by extensive media coverage and often guided by distorted rumours, focus group participants feared the collection and misuse of their information by *OSN providers*: *"you remove everything from there, but the provider keeps the history, it's violation of your privacy"*, "*they make just billions of dollars, these companies, how do they make this money? ... They do something with the content we provide on the site...*", "*… they will now start to make money from the network and sell the information of the users to third parties, to marketing firms or whatever"* (FGQ). *Collection and Use* of the information *by the Third Parties* was also viewed as a source of concern: *"But the third parties, for example in marketing, […] are selling the databases of contact information of other people"*, *"companies who are just selling private data to other companies so they are able to send you like personal advertising stuff"* (FGQ). The generic *Marketing* category encompassed concerns regarding the use of personal information to personalize banners or emails on the network: "*I always think that if I put all my hobbies and everything then all these marketing firms will be running after me"* (FGQ) or *"There is definitely a potential of using my information and then bombarding me with emails"* (FGQ).

Concern regarding Identity Theft was mentioned only once. Nevertheless, this threat can have very serious consequences if it actually takes place. We therefore include it into our subsequent analysis.

Analysis of the focus groups helped us to get an in-depth understanding of user privacy concerns. In addition, we gained important insights about the dynamics of user self-communication on these platforms. On the one hand, despite perceived privacy risks, users are willing to provide information about themselves on a social

network to gain various benefits of communication. On the other hand, focus group participants argued that they restrict how much information they reveal about themselves, viewing it as an important strategy to address their privacy concerns. Information disclosed on OSNs is often subject to cognitive control prior to its publication. Theoretical findings show that OSN users try to control their audience in order to mitigate their privacy concerns (Tufekci 2008). However, whereas users may find it difficult to correctly assess the breadth and the kind of their audience and, hence, feel unsure regarding the visibility of their information, they may choose to control the information they are about to publish. Confirming this rationale, our focus groups have shown that even when users reveal information on an OSN, they claim to *consciously control* what exactly they disclose, accounting for the privacy threats they perceive—a phenomenon we refer to as "Conscious Control" in the next sections of our study. Thus, w*hat* participants reveal is often a result of what they feel is harmless to them: "*I don't want to reveal information harmful to me in the future"* (FGQ). This phenomenon, expressed in the self-imposed restriction on the information revealed, has already been observed in the context of blogs, where bloggers tend to place constraints on the information they published accounting for possible future repercussions for them or others (Gumbrecht 2004). Furthermore, our focus groups have shown that, when participants decided to reveal their information, its content was abundant in impression management. Naturally, participants tended to present mostly positive information about themselves: "*I reveal information which […] is praiseworthy"* (FGQ).

Publishing dishonest or inaccurate information might be another strategy individuals use to address privacy risks. However, it is of low importance in accordance with the focus group results.

From our qualitative analysis of the focus groups, we can already conclude that OSN participants are aware of and concerned about multiple privacy risks they face on an OSN platform. As a result, they try to mitigate these risks by relying on various self-disclosure strategies. In the next sections, we will empirically investigate the validity of the focus group results and their implications for individual self-disclosure.

STAGE 2: Validating "User Privacy Concerns on OSNs" construct

Development of measurement scales

The categories identified through the focus groups served as a basis for the questionnaire items. Pre-tested scales were used where possible. Nevertheless, due to the explorative nature of the study, most items were self-developed. Table 8 in Appendix 1 summarizes the scales used for the study.

As one can see, many items used to operationalize the PCOSN construct start with an "I am *often* concerned…" formulation. Including the word "*often*" helped us achieve much more realistic answers by avoiding a "talk is cheap" problem. This problem is inherent in privacy surveys, as it does not cost a respondent anything to express a desire for enhanced privacy protection (Harper and Singleton 2001).

Self-disclosure dynamics were captured on the basis of two dimensions of the Self-Disclosure Scale (Wheeless and Grotz 1976): Amount and Honesty. We also measured the "Conscious Control" construct—a dimension of self-disclosure which

emerged as important during the focus group discussions. Even when disclosing a lot in terms of "Amount", focus group participants claimed to consciously control *what exactly was disclosed*. The meaning of the "Conscious Control" construct lies between the reversed "Control of Depth" and "Intent" dimensions of the Self-Disclosure Scale developed by Wheeless and Grotz (1976). However, whereas "Control of Depth" largely reflects the perceived intimacy of the information revealed and "Intent" stands for the individual willingness to engage in the *"self-revealing disclosure"* (Wheeless and Grotz 1976, p. 339), our "Conscious Control" construct underscores consciousness of the self-restriction or information control act. We have chosen these dimensions as the most interesting in terms of the implied self-presentation and identity performance dynamics. All items reflecting self-disclosure had to be significantly changed or developed anew to address the specifics of OSN communication.

All constructs were modelled as reflective with questions anchored on a 7-point Likert scale (1: Strongly Disagree; 4: Neutral; 7: Strongly Agree).

Sampling

As the next step, an online questionnaire was launched in late Winter—Spring 2008. The respondents were recruited via university mailing lists and advertisements placed in various OSN groups. The targeted audience included users of two OSNs particularly popular in Germany: Facebook and StudiVZ. Survey participants had a chance to win numerous gift certificates as a reward for their participation. We obtained 210 usable observations in total. 49% of the respondents in our sample were male. 87.1% were students. 70.5% and 29.5% of the respondents indicated StudiVZ and Facebook as their main OSN platform, respectively.

Exploratory factor analysis

Exploratory Factor Analysis (EFA) is a widespread technique used to study interrelationships among variables in a sample. It is especially helpful when the number of variables is large, as it helps decrease complexity by mapping variables onto a reduced number of extracted factors (Churchill and Iacobucci 2002). The aim of the EFA in our study was to single out dimensions of the PCOSN construct. Hence, all 32 variables (see Tables 2 and 8) that measured various aspects of privacy concern were included in the analysis performed in SPSS 16.0.

At first, the applicability of our data for the EFA was checked by looking at several indicators. The Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0.908. Bartlett's Test of Sphericity was also significant at a 0.000 level. Examination of the anti-image correlation matrix did not force us to remove any items from the analysis. Taken as a whole, these criteria suggest that our data for the EFA was adequate.

We used a principal components analysis to examine if the category structure identified in the focus groups also existed in the extracted factor groups of the collected data. Direct Oblimin rotation was chosen as inter-correlation between extracted dimensions was expected[1]. In the initial solution, 7 factors (components) with Eigenvalues higher than 1 were extracted, with the first 2 factors accounting for

[1] Varimax rotation has rendered equivalent results.

Table 2 Summary of the extracted dimensions using explorative factor analysis (pattern matrix)

Item Number	Focus Group Category	Mean	SD	Components	
				Concerns about Organizational Threats	Concerns about Social Threats
Acc1**	General Accessibility	3.57	1.808	0.039	**0.669**
Acc_N2 (R)*		4.53	1.846	0.189	0.256
Acc3**		3.87	1.641	0.183	**0.585**
Acc4**		3.49	1.652	0.018	**0.648**
Acc5*		4.16	1.945	0.055	0.322
Acc_N6 (R)*		4.01	1.512	−0.025	0.360
SSC1	Uncontrollable Social Risks	3.39	1.598	−0.100	**0.840**
SSC2**		3.67	1.791	0.051	**0.599**
SSC3**		3.45	1.559	−0.124	**0.739**
SSB1	Bullying Social Risks	3.11	1.549	−0.086	**0.797**
SSB2		3.20	1.565	−0.049	**0.827**
SSB3		3.45	1.583	0.112	**0.763**
Col_N1 (R)**	Collection by OSN Provider	4.71	1.670	**0.698**	−0.031
Col_2		4.25	1.696	**0.572**	0.271
Col_3		4.06	1.650	**0.592**	0.321
SU_1	Secondary Use by OSN Provider	4.46	1.663	**0.550**	0.271
SU_N2 (R)**		4.21	1.651	**0.575**	−0.090
SU_N3 (R)**		5.47	1.569	**0.680**	−0.096
ColO_1	Collection by Third Parties	4.34	1.640	**0.646**	0.281
ColO_2		4.36	1.692	**0.709**	0.237
ColO_N3 (R)**		4.84	1.695	**0.770**	−0.005
SUO_1	Secondary Use by Third Parties	4.41	1.600	**0.625**	0.251
SUO_2		4.23	1.549	**0.648**	0.261
SUO_N3(R)**		4.87	1.713	**0.765**	−0.047
SUm_N1 (R)*	Marketing (Banners and Emails)	3.24	1.708	0.396	0.084
SUmb_N2 (R)**		4.60	1.584	**0.641**	−0.259
SUmb_3**		4.52	1.905	**0.697**	−0.152
SUme_4**		3.98	1.667	**0.485**	0.252
SUme_N5 (R)**		4.47	1.753	**0.527**	0.092
IdT_N1 (R)*	Identity Theft	3.82	1.626	0.265	0.267
IdT_N2 (R)*		3.51	1.628	0.214	0.234
IdT3*		3.76	1.478	0.202	0.373

(R) These items were reversed; * These items were removed after the EFA.** These items were removed after the CFA model fitting procedure (items with labels in bold were used in the final Structural Equation Model in Stage 3);

43.7% in the cumulative variance. Each subsequent factor explained less than 5.3% of the variance and was difficult to interpret. Taking into account that a substantial proportion of variance was captured by the first two factors, we limited the number of factors to be extracted to only 2, which was also suggested by the Scree Plot in the next step. The inter-factor correlation constituted 0.420[2]. Table 2 summarizes the identified dimensions and respective factor loadings. Factor loadings, indicating the effect of a respective factor on a given indicator when at the same time controlling for the other factors (Pedhazur and Schmelkin 1991), were considered meaningful when they exceeded the threshold of 0.4 (Hair et al. 1998).

The interpretation of the extracted factors—suggested dimensions of the PCOSN construct—is rather intuitive. It hints that individuals differentiate between two main sources of privacy concern: organizations and OSN users.

The first factor, which we called *Concerns about Organizational Threats*, combines all concerns users have that related to the organizational use of their information. Our study shows that, in the organizational context, users *neither* subjectively differentiate between *who* collects and uses the information they provide (OSN Provider vs. Third Parties) *nor* do they make a distinction between the *collection* and the *secondary use* of their information. In fact, secondary use is impossible without information collection, and therefore users might assume that a party collecting their information would also *use* it at some point.

The second factor, called *Concerns about Social Threats*, is mainly related to the risks stemming from the OSN user environment. We find that individuals don't make distinctions based on the nature of the threat (purposeful bullying vs. involuntary uncontrollable actions of others), instead concentrating on the threat source (social environment).

It is important to note that, despite the importance of the Accessibility Threats for the focus group participants, the items measuring this dimension did not form a separate factor. This might be because the accessibility of the information is the necessary pre-condition for all other threats. Therefore, when expressing their concern over accessibility, participants were in fact implying secondary-level threats (organizational, social, etc.). Additionally, *Identity Theft* neither emerged as a separate factor nor loaded highly on any of the identified dimensions.

In summary, the two main dimensions of the PCOSN construct have been identified as a result of the EFA: *Concerns about Organizational Threats* and Concerns about *Social Threats*. We will confirm the existence of this factor structure using Confirmatory Factor Analysis (CFA) in the next step.

Confirmatory factor analysis

At the next step, we assessed the reliability and validity of our PCOSN construct through a CFA with maximum likelihood estimation using AMOS 16.0.1. As derived in the EFA, we modelled the PCOSN construct as consisting of two separate first-order factors: *Concerns about Organizational Threats* and *Concerns about Social Threats*. In this analysis, all items from the EFA with loadings higher than 0.4

[2] Extraction of two factors using principal axis factoring method, as an alternative to principal components analysis, has rendered equivalent results.

Table 3 Final operationalization of "*user privacy concerns on OSNs*" construct

Dimension 1: Concerns about Organizational Threats	
Col_2	I am often concerned that OSN provider could store my information for the next couple of years
Col_3	Every now and then I feel anxious that OSN provider might know too much about me
SU_1	I am often concerned that OSN provider could share the information I provide with other parties (e.g. marketing, HR or government agencies)
ColO_1	I am often concerned other parties (e.g. marketing, HR, government agencies) could actually collect my publicly available information on OSN
ColO_2	I am often concerned that my current publicly available information could be stored at some other party (e.g. marketing, HR, government agencies) many years from now
SUO_1	I am often concerned that other parties (e.g. marketing, HR, government agencies) could share the information they have collected about me on OSN
SUO_2	It often worries me that other parties (e.g. marketing, HR, government agencies) could use the information they have collected about me from OSN for commercial purposes
Dimension 2: Concerns about Social Threats	
SSB1	I am often concerned that someone might purposefully embarrass me on OSN
SSB2	It often worries me that other users might purposefully write something undesired about me on OSN
SSB3	I am often concerned that other users might take advantage of the information they learned about me through OSN
SSC1	I am often concerned that I don't have control over the actions of other users

were included and restricted to load on the respective factors they were supposed to measure (*Organizational and Social Threats*). The factors themselves were allowed to correlate with each other.

In the process of model adjustment, several items were removed from the model (as summarized in Tables 2, 3 and 8). Accounting for the large number of newly developed scales, this practice is acceptable as long as Content Validity is ensured (Segars and Grover 1993). The resulting model is shown in Fig. 2. The model fulfilled all reliability and validity requirements (partly shown in Table 4) and had an excellent

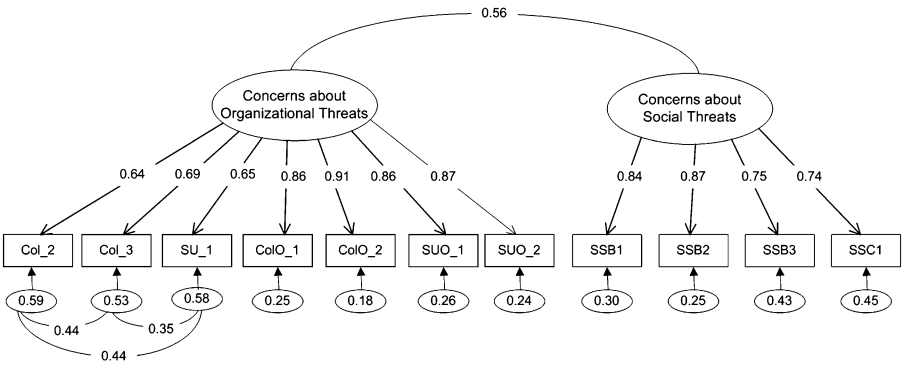

Fig. 2 "User privacy concerns on OSNs" construct—CFA results

Table 4 Quality criteria of the construct "*user privacy concerns on OSNs*"

Latent Variable	Item	Mean	Standard Deviation	Standardized Factor Loading	AVE	Composite Reliability	Cronbach's Alpha
Concerns about Organizational Threats	Col_2	4.25	1.696	0.643	0.63	0.92	0.926
	Col_3	4.06	1.650	0.687			
	SU_1	4.46	1.663	0.648			
	ColO_1	4.34	1.640	0.864			
	ColO_2	4.36	1.692	0.907			
	SUO_1	4.41	1.600	0.859			
	SUO_2	4.23	1.549	0.874			
Concerns about Social Threats	SSB1	3.11	1.549	0.838	0.64	0.88	0.879
	SSB2	3.20	1.565	0.869			
	SSB3	3.45	1.583	0.755			
	SSC1	3.39	1.598	0.742			

fit (χ^2/df=1.985; GFI=0.937; AGFI=0.896; RMSEA=0.069; CFI=0.976)[3]. Taken together, these results provide evidence that the PCOSN construct is measured well.

In summary, the two main dimensions of the PCOSN construct were identified and validated as a result of EFA and CFA: *Concerns about Organizational* and *Concerns about Social Threats*. Typically, scales derived on the basis of one sample should not be directly reused with the same sample. However, taking into account the explorative nature of our study, we applied these scales within the collected data to better understand self-presentation dynamics on OSN platforms. In the next sections, we will empirically investigate the impact of the identified concerns on various self-disclosure strategies in a Structural Equation Model (SEM).

STAGE 3: Identity construction and privacy concerns

Our focus groups have shown that privacy concerns are changing the way individuals disclose information about themselves. In this light, exploring the impact of the identified privacy concerns regarding *Organizational and Social Threats* on individual self-disclosure is an important step towards understanding of the underlying self-communication dynamics on OSN platforms. Wheeless and Grotz (1976) single out as amount, honesty, intent of self-disclosure, control of depth, and its positive-negative nature as dimensions of the individual self-disclosure. In the context of OSNs, *(i)* amount reduction and *(ii)* falsification vs. honesty of the disclosed information, as well as *(iii)* conscious control of the information to be released may encompass the most salient aspects of the information disclosure strategies with respect to privacy risks. We therefore concentrated exclusively on these three strategies.

[3] Discussion on the required thresholds to ensure validity and reliability of the measured construct can be found in the "Measurement Model Evaluation – Confirmatory Factor Analysis" part of this paper. The required cut-off criteria for model fit can be found in Table 7 below.

Focus group participants emphasized reducing the *amount* of information disclosed as an important strategy for dealing with rising privacy concerns. From the *organizational* perspective, any information disclosed—independent of its sensitivity—gives marketers additional insights into an individual's personality, and hence into the tastes and preferences of a potential customer. Similarly, for an HR-manager, every additional piece of information reveals more about the potential candidate and may therefore serve as the basis for an employment decision. For example, Kluemper and Rosen (2008) have shown that Facebook profiles contain enough information to judge on one's job performance. Furthermore, the information that individuals reveal can be used to implement more refined phishing attacks (Hogben 2007). We therefore hypothesize that:

- H1: User *Concerns* regarding privacy-related *Organizational Threats* are negatively related to the *Amount of the Information disclosed* on the platform.

In addition, the *amount* of information revealed can also be negatively affected by the degree of *social* risks perceived. Detailed and updated profiles can be more attractive for bullies, who might eventually use this information to harass a victim. Similarly, one's own friends and acquaintances can spread information they obtain through an OSN and interpret it in the wrong context. The media presents abundant examples of such incidents taking place (Hogben 2007).

Goffman (1959) asserts that, in the process of impression management, an individual speaks to an anticipated audience. Implicitly accounting for the potential risks of speaking to this expected "audience", individuals may repress the disclosure of personal information (Schau and Gilly 2003). We therefore hypothesize that:

- H2: User *Concerns* regarding *Social Threats* are negatively related to the *Amount of the Information disclosed* on the platform.

In order to protect themselves from daunting risks, users may be tempted to partially falsify some of the information they provide. For example, by giving the wrong name or contact information, users can avoid direct recognition and identification and thereby protect themselves from the prying eyes of organizations. Accounting for social risks, participants might engage in over-enhancement or misrepresentation to make them look better in the eyes of the others and thereby diminish the risk of being laughed at or humiliated. Schau and Gilly (2003, p.387) argue that self-presentation strategies often go hand in hand with modification or fabrication of the information a person reveals about him-or herself, so that the image one projects is more in line with a person's view on oneself: "*a desired self*". We therefore hypothesize that:

- H3: User *Concerns* regarding privacy-related *Organizational Threats* are negatively related to the *Honesty of the Information disclosed* on the platform.
- H4: User *Concerns* regarding *Social Threats* are negatively related to the H*onesty of the Information disclosed* on the platform.

Conscious Control, a measure reflecting the extent of conscious adjustment of the information being disclosed, reflects the dynamics observed in the focus group discussions, where participants claimed to carefully self-select information they were about to publish. This conscious filtering of disclosed information appears to be an important mechanism of identity control and is an integral part of the identity

protection process. Thus, w*hat* participants reveal is often a result of what they feel is harmless to them with respect to both organizational and social threats. In fact, concerns regarding these threats can motivate user to carefully consider the information she is about to publish. We therefore hypothesize that:

- H5: User *Concerns* regarding privacy-related *Organizational Threats* are positively related to the *Conscious Control* behind information disclosure on the platform.
- H6: User *Concerns* regarding *Social Threats* are positively related to the *Conscious Control* behind information disclosure on the platform.

The summary of the model hypotheses is presented in Fig. 3.

Research methodology

The model depicted in Fig. 3 is a SEM. In line with methodological guidelines (Anderson and Gerbing 1988), we evaluate the Measurement Model (MM) first and the Structural Model (SM) second. The assessment of the MM focuses on the relationship between latent constructs and their respective indicators (Byrne 2001). SM evaluation involves finding links between dependent (endogenous variables: dimensions of self-disclosure) and independent (exogenous variables: privacy concerns) variables.

Measurement model evaluation — confirmatory factor analysis

CFA using maximum likelihood estimation was employed to evaluate the reliability and validity of our MM using AMOS 16.0.1. Initial model evaluation led us to eliminate several items measuring self-disclosure dimensions (see

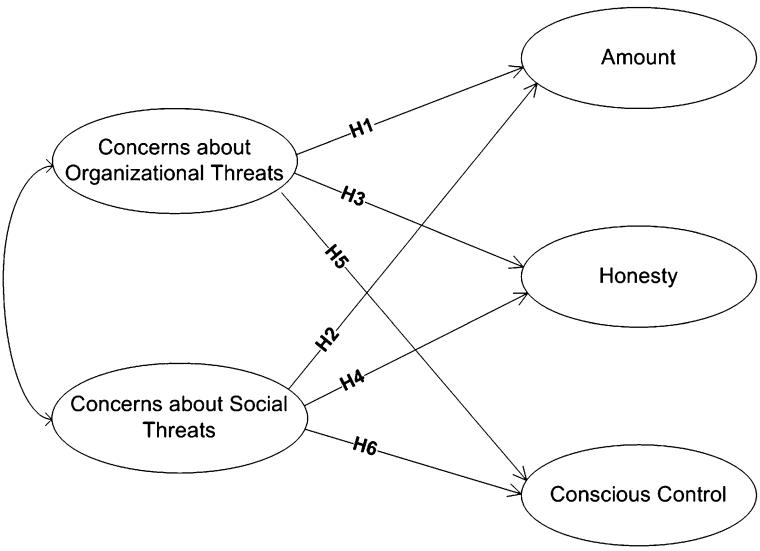

Fig. 3 Research model: impact of privacy concerns on self-disclosure

Table 5 Quality criteria of the constructs

Latent Variable	Item	Mean	Standard Deviation	Standardized Factor Loading	AVE	Composite Reliability	Cronbach's Alpha
Concerns about Organizational Threats	Col_2	4.25	1.696	0.645	0.63	0.92	0.926
	Col_3	4.06	1.650	0.689			
	SU_1	4.46	1.663	0.648			
	ColO_1	4.34	1.640	0.864			
	ColO_2	4.36	1.692	0.907			
	SUO_1	4.41	1.600	0.859			
	SUO_2	4.23	1.549	0.873			
Concerns about Social Threats	SSB1	3.11	1.549	0.838	0.64	0.79	0.879
	SSB2	3.20	1.565	0.869			
	SSB3	3.45	1.583	0.753			
	SSC1	3.39	1.598	0.744			
Amount	SD_A_1	3.47	1.714	0.589	0.49	0.79	0.787
	SD_A_2	3.40	1.678	0.720			
	SD_A_3	3.23	1.752	0.827			
	SD_A_4	3.13	1.569	0.647			
Honesty	SD_H_2	5.07	1.685	0.912	0.72	0.84	0.830
	SD_H_3	5.00	1.700	0.779			
Conscious Control	SD_C_1	5.20	1.571	0.873	0.63	0.83	0.830
	SD_C_2	5.25	1.600	0.730			
	SD_C_3	5.48	1.458	0.765			

Tables 5 and 8). The remaining indicators have been used to evaluate the final adjusted model.

In the first step, we assessed the Internal Consistency, Convergent validity, and Discriminant validity of the measured constructs as shown in Tables 5 and 6.

Convergent validity reflects the extent to which several attempts to measure the same construct are in consent (Bagozzi and Philips 1982). Convergent Validity was verified by evaluating:

- Indicator Reliability, which is ensured when indicator loadings are significant and exceed the cut-off level of 0.7 (Bagozzi and Yi 1988). In our study, all

Table 6 Square root of AVE (diagonal elements) and inter-construct correlation (off-diagonal elements)

	OT	ST	Am	Ho	CC
Organizational Threats (OT)	*0.791*				
Social Threats (ST)	0.557	*0.803*			
Amount (Am)	−0.163	−0.026	*0.701*		
Honesty (Ho)	−0.108	−0.002	0.172	*0.848*	
Conscious Control (CC)	0.189	0.244	−0.092	0.350	*0.792*

Table 7 Goodness-of-fit measures for measurement and structural models

Fit Measures	Recommended Value (Source)	CFA	SM
χ^2/df	< 2.00 (Carmines and McIver 1981)	1.445	1.588
GFI	> 0.90 (Jöreskog and Sörborm 1989)	0.91	0.90
AGFI	> 0.80 (Jöreskog and Sörborm 1989)	0.88	0.87
RMSEA	< 0.08 (Jöreskog and Sörborm 1993)	0.046	0.053
CFI	> 0.95 (Hu and Bentler 1999)	0.97	0.96
IFI	> 0.95 (Hu and Bentler 1999)	0.97	0.96
TLI	> 0.95 (Hu and Bentler 1999)	0.96	0.95

indicators were significant, with five out of twenty slightly lower than the required cut-off level;

- Composite Reliability—values for all constructs in our study exceeded the threshold of 0.6 (Bagozzi and Yi 1988);
- Average Variance Extracted (AVE)—values for all measured constructs surpassed or closely approached the required threshold level of 0.5 (Fornell and Larcker 1981).

Our results suggest that we can assume Convergent Validity. Internal Consistency, a measure reflecting reliability of different items used to measure the same construct, was also ensured: Cronbach's Alpha for all constructs was higher than the required value of 0.7 (Nunnally 1978).

In the next step, we assessed Discriminant Validity, a measure indicating sufficient divergence between operationalizations of different constructs. Discriminant validity is fulfilled when the square root of AVE of any latent variable exceeds

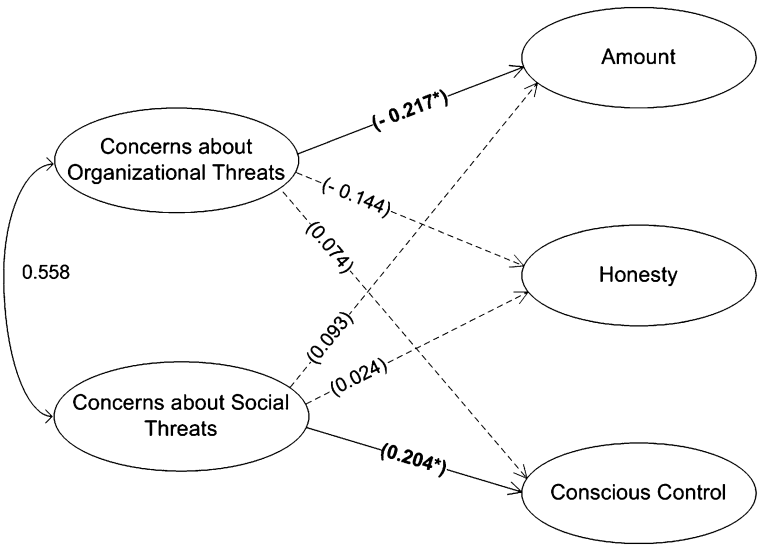

Fig. 4 Results of structural model

the correlation between this and any other latent variables (Fornell and Larcker 1981). As seen in Table 6, this requirement is met for all constructs in our model.

Next, we assessed the quality of our MM by looking at the overall measures of goodness of fit. For a good model fit, it is suggested that χ^2/df should not exceed 2 (Carmines and McIver 1981). As Table 7 (column "CFA") shows, our model meets this requirement. All other required criteria for GFI, AGFI, RMSEA, CFI, IFI, TLI fit indices were also met by the MM. Overall, these results suggest that our MM is well specified.

Structural model evaluation

We next assessed the SM. As shown in Table 7 (column "SM"), our SM has a good overall fit. All recommended cut-off criteria are met. An important part of the evaluation of the SM is assessment of the path coefficients and their significance (see Fig. 4). As a result of model evaluation, hypotheses H1 and H6 were supported; hypotheses H2, H3, H4 and H5 were rejected. Furthermore, 3.3%, 1.7% and 6.4% of the variance (R^2) in the endogenous variables Amount, Honesty, and Conscious Control respectively were explained by our model. The implications of the model results are discussed below.

Discussion and managerial implications

Using the developed taxonomy of privacy concerns of users in OSNs as a basis for the SEM, we find that Concerns about *Organizational and Social Threats* impact different information disclosure strategies in distinct ways.

We find that concerns regarding *Organizational Threat*s have a negative influence on the *amount* of information individuals disclose: users tend to reduce self-presentation on the platform when they fear that their information will be collected, stored, and used by the OSN provider and various Third Parties. Hogben (2007) warns of the risks of digital dossier aggregation and the subsequent use of this information for marketing, HR, insurance, state security, and other purposes. Advanced customer data analysis and granular personalization become possible due to existence of information-intensive OSN profiles pool. The low cost of information storage makes it possible to store user data for an indefinite amount time and process it on demand. In response to their concerns over these practices, users decrease the amount of the information they provide.

Interestingly, concerns over *Social Threats* do not have a significant impact on the *amount* of information individuals disclose. This is in line with Tufekci (2008), who finds little to no relationship between concerns regarding profile accessibility to the unwanted audience and the amount of information disclosed on the network, explaining this result by user reliance on privacy settings and the usage of nicknames. In fact, privacy settings can be more powerful when dealing with social rather than organizational threats. In fact, whereas users may rely on available functionality to limit access to their information and control actions of other OSN members, these control measures are largely ineffective when dealing with privacy concerns originating from the actions of an OSN provider. Overall, the use of privacy controls may moderate a relationship between concerns regarding social threats and behaviour—a relevant

hypothesis which is, however, beyond the scope of our study and should be addressed in the future research endeavours.

We find a significant link between concerns about *Social Threats* and the *Conscious Control* dimension, which demonstrates that individuals consciously weigh and select the information they disclose, adapting it with regard to the expectations concerning their "imagined audience" (Boyd 2007). Indeed, users have certain positive and negative expectations with regard to their social environment, and hence adjust their self-communication with respect to it. Importance of conscious control in managing concerns regarding social threats underscores importance of impression management in the individual self-communication. Thus, users carefully self-select information they present about themselves in their attempt to avoid public embarrassment or secret revelation.

In our study, we find no link between the *Honesty* of individuals when they disclose information and privacy concerns. This outcome suggests that, when in doubt, participants choose not to disclose certain information rather than falsifying the relevant details. An analysis of the means shows that, on average, participants slightly agreed with the statements about always being honest and trustful with the information they provided on OSNs (see Table 5). The truthfulness of revealed information is partly related to the presence of real-life friends on the network, who implicit verify one's statements (Donath and Boyd 2004). Moreover, falsified information connected to the user can also be a source of risk.

As a whole, our findings suggest that individuals engage in selective privacy-conscious self-communication on OSN platforms. We show that user privacy concerns do impact identity performance in a negative way, undermining the self-sustainability of these platforms in the long-run. Our results call for OSN providers and policy-makers to take immediate measures to address these concerns.

Concerns regarding *Organizational Threats, which* include the collection and secondary use of member information, can be pro-actively addressed by developing fair privacy policies, which may, in turn, help to develop more trust in OSN providers. Culnan and Armstrong (1999) find that if fair information practices are observed, customers will more willingly continue the relationship with the firm that collects information about them. These insights are tightly connected with the notion of the procedural fairness which reflects the extent a provider empowers user with procedures to control their privacy as well as informs users about these procedures (Son and Kim 2007). Furthermore, giving users more control over their information through various privacy settings may help them to protect themselves against data collection by third parties. Hence, transparency and usability of available controls should be the top priority as well. From the technical side, access controls should be enhanced to prevent unauthorized access to member profiles or systematic information crawling by third parties.

Concerns regarding *Social Threats* can be alleviated by offering users clear mechanisms to deal with the improper behaviour of others; user options might include explicitly confirming photo tags before associated photos are published, enhanced settings to facilitate the management of different friends groups or clear conflict escalation procedures. These measures will help to protect users by giving them greater control over their identity and context.

In line with principles of procedural fairness, it is important to teach users how to protect their information. Users should be explicitly advised not to reveal sensitive information, e.g. their contact, location, and financial details, on the network. Once they have been informed about potential risks and protection methods, users will be able to consciously decide how much information to disclose in an atmosphere of trust and transparency. This, in turn, would lead users to view the OSN as a safe environment for self-presentation and identity construction.

Taking into account the popularity of OSN platforms, policy-makers should contribute by developing and publicizing clear guidelines for how to deal with user information, who owns it, and how users should proceed in the case of information misuse.

All of these measures would help ensure more responsible self-disclosure on the platform without endangering its self-sustainability. Furthermore, they would encourage users to create social capital without having to sacrifice their privacy.

Concluding remarks

Until now, little was understood about the privacy concerns of OSN users and the impact of those concerns on self-presentation strategies.

Recognizing that this research gap maybe caused by the lack of measurement instruments adequately capturing the unique OSN context, we initially concentrated our efforts on developing and validating measures for the "*User Privacy Concerns on OSNs*" construct. On the basis of qualitative focus group results, we developed a tentative framework capturing various aspects of privacy-related concerns of users on OSNs. Our framework was then empirically validated on the basis of survey responses from 210 subjects. We found that concerns about Organizational and Social Threats constitute two underlying dimensions of the PCOSN construct.

At the next step, we examined the impact of the identified concerns on three self-disclosure dimensions: amount, honesty, and conscious control. We found that users tend to reduce how much information they disclose as a response to perceived Organizational Threats. Additionally, users tend to consciously screen the information they publish in light of concerns stemming from the OSN user environment. On the basis of our findings, we provide insights for the OSN provider and policy-makers, who can then develop specific mechanisms to alleviate identified user concerns and thereby ensure network sustainability as well as public value.

Both focus group participants as well as survey respondents in our study were mainly students. Even though students represent an important part of OSN users (Facebook 2009), other population groups are gaining in importance as well (Insidefacebook 2009). Hence, validation of the PCOSN construct dimensions with other population group represents a promising venue for further research. Furthermore, taking a closer look at the relationship between identified dimensions of privacy concerns and actual, as opposed to self-reported, self-disclosure behaviour may reveal additional dynamics in how privacy concerns impact the process of identity construction—another relevant opportunity for future studies.

Appendix 1

Table 8 Construct operationalization

GENERAL ACCESSIBILITY	
Acc1	I am often concerned that someone I don't expect (e.g. a stranger, my "ex", my parents, teacher, boss) could view my profile on OSN
Acc_N2	It is not important for me that someone I do not want (e.g. my boss, my teacher) could view my profile on OSN *(reversed)*
Acc3	I am often concerned that I cannot limit access to some information I publish on OSN for some people
Acc4	I feel uncomfortable that many people might follow changes in my profile
Acc5	If I was in a job application process I would make many changes to my profile
Acc_N6	I don't care what opinion others build about me based on what I write on OSN *(reversed)*
SOCIAL THREATS	
Uncontrollable Social Risks	
SSC1*	**I am often concerned that I don't have control over the actions of other users**
SSC2	It bothers me when other users tag me in pictures
SSC3	It bothers me when other users post something about me on the Wall
Bullying	
SSB1	**I am often concerned that someone might purposefully embarrass me on OSN**
SSB2	**It often worries me that other users might purposefully write something undesired about me on OSN**
SSB3	**I am often concerned that other users might take advantage of the information they learned about me through OSN**
ORGANIZATIONAL THREATS	
Collection by OSN Provider	
Col_N1	It never actually worries me that OSN provider could collect information about me over the years *(reversed)*
Col_2	**I am often concerned that OSN provider could store my information for the next couple of years**
Col_3	**Every now and then I feel anxious that OSN provider might know too much about me**
Secondary Use by OSN Provider	
SU_1	**I am often concerned that OSN provider could share the information I provide with other parties (e.g. marketing, HR or government agencies)**
SU_N2	It rarely worries me that OSN provider could use the information I provide for commercial purposes *(reversed)*
SU_N3	Even if OSN provider would start to share some of my information, I do not see a real threat to my privacy *(reversed)*
Collection by Third Parties	
ColO_1	**I am often concerned other parties (e.g. marketing, HR, government agencies) could actually collect my publicly available information on OSN**
ColO_2	**I am often concerned that my current publicly available information could be stored at some other party (e.g. marketing, HR, government agencies) many years from now**
ColO_N3	Even if third parties would collect my public information on OSN, I do not see a real threat to my privacy *(reversed)*
Secondary Use by Third Parties	
SUO_1	**I am often concerned that other parties (e.g. marketing, HR, government agencies) could share the information they have collected about me on OSN**

SUO_2	**It often worries me that other parties (e.g. marketing, HR, government agencies) could use the information they have collected about me from OSN for commercial purposes**
SUO_N3	Even if other parties would start to use my information for commercial purposes, I do not see a real threat to my privacy *(reversed)*
Marketing: Banners	
SUm_N1	I would find personalized advertising (e.g. banners) better than paying for OSN *(reversed)*
SUmb_N2	Overall, I would find it good if displayed banners would be tailored to my interests *(reversed)*
SUmb_3	It would bother me that the information in my profile would be used to display personalized banners to me
Marketing: Emails	
SUme_4	I am often concerned that based on the information I provide on OSN I could receive more advertising emails
SUme_N5	It never actually worries me that due to my presence on OSN I could receive more emails from advertisers *(reversed)*
IDENTITY THEFT	
IdT_N1	I actually do not worry that based on my OSN profile someone could sign up to another website *(reversed)*
IdT_N2	I do not think that based on my OSN profile someone could so easily buy something in the Internet *(reversed)*
IdT3	I think that OSN profiles are abused by the criminals, who based on this information start acting under a false name in the Internet
INFORMATION DISCLOSURE	
Amount	
SD_A_1	**I have a comprehensive profile on OSN**
SD_A _2	**I find time to keep my profile up-to-date**
SD_A_ 3	**I keep my friends updated about what is going on in my life through OSN**
SD_A_ 4	**When I have something to say, I like to share it on OSN**
Honesty	
SD_H_1N	I am not always completely sincere when I write about myself on OSN *(reversed)*
SD_H_2	**I am always honest in the information I provide on OSN**
SD_H_3	**I am always truthful when I write about myself on OSN**
Conscious Control	
SD_C_1	**When I post something on OSN , I am always careful about what exactly I am saying about myself**
SD_C_2	**When I express myself on OSN , I always consider who can see the information I publish**
SD_C_3	**I think carefully how much I reveal about myself on OSN**
SD_C_4	I consciously hold back certain information from OSN
SD_C_5	When networking on OSN I don't care what kind of information I reveal about myself *(reversed)*

*items selected in bold were used in the final SEM as described in "STAGE 3: Identity Construction and Privacy Concerns"

References

Acquisti A, Gross R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: 6th Workshop on Privacy Enhancing Technologies. UK: Springer-Verlag; 2006. p. 36–58.

Anderson JC, Gerbing DW. Structural equation modeling in practice: a review and recommended two-step approach. Psychological Bulletin. 1988;103(3):411–23.

Bagozzi RP, Phillips LW. Representing and Testing Organizational Theories: A Holistic Construal. Administrative Science Quarterly. 1982;27(3):459–89.
Bagozzi RP, Yi Y. On the evaluation of structural equation models. Journal of the Academy of Marketing Science. 1988;16(1):74–94.
Boyd D, Ellison N. Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication 2007;13(1):11.
Boyd D. Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. In: Buckingham D, editor. Youth, Identity, and Digital Media. Cambridge, USA: MIT Press; 2007. p. 119–42.
Boyd D. Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. Convergence. 2008;14(1):13–20.
Boyd D, Heer J. Profiles as Conversation: Networked Identity Performance on Friendster. Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39). IEEE Computer Society. USA. 2006.
Brym RJ, Lenton RL. Love Online: A Report on Digital Dating in Canada. 2001. http://www.nelson.com/nelson/harcourt/sociology/newsociety3e/loveonline.pdf. Accessed 12 November 2008.
Byrne BM. Structural Equation Modeling with AMOS: Basic Concepts, Applications and Programming. USA: Lawrence Erlbaum Associates; 2001.
Carmines EG, McIver JP. Analyzing models with unobserved variables: Analysis of covariance structures. In: Bohrnstedt GW, Borgatta EF, editors. Social measurement: Current issues. Newbury Park: Sage; 1981. p. 65–115.
Churchill GA, Iacobucci D. Marketing Research: Methodological Foundations. 8th ed. Australia: South-Western College Pub; 2002.
Culnan MJ, Armstrong P. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science. 1999;10(1):104–15.
Donath J, Boyd D. Public Displays of Connection. BT Technology Journal. 2004;22(4):71–82.
Dwyer C, Hiltz SR, Passerini K. Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace. Thirteenth American Conference on Information Systems. USA. 2007.
Ellison N, Heino R, Gibbs J. Managing impressions online: Self-presentation processes in the online dating environment. Journal of Computer-Mediated Communication 2006;11:2, article 2.
Ellison N, Steinfield C, Lampe C. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication 2007;12:4, article 1.
Facebook. Statistics. Press Center. http://www.facebook.com/press/info.php?statistics. Accessed 20 June 2009.
Fornell C, Larcker DF. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research. 1981;18(3):39–50.
Gibbs JL, Ellison NB, Heino RD. Self-Presentation in Online Personals. Communication Research 2006;33(2):152–177.
Goffman E. The presentation of self in everyday life. New York, USA: Anchor; 1959.
Gumbrecht M. Blogs as "Protected Space", Workshop on the Weblogging Ecosystem: Aggregation, Analysis, and Dynamics. New York: ACM Press; 2004.
Gurses S, Rizk R, Günther O. Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback. ICIS 2008.
Harper J, Singleton S. With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us. Competitive Enterprise Institute 2001; doi:10.2139/ssrn.299930
Hair JF, Tatham RL, Anderson RE, Black W. Multivariate Data Analysis, 5th ed. Prentice Hall; 1998.
Hewitt, A. and Forte, A., Crossing boundaries: Identity management and student/faculty relationships on the Facebook. Poster/Extended Abstract. CSCW 2006.
Higgins ET. Self-discrepancy: A theory relating self and affect Psychological Review1987;94(3):319–340.
Hogben G. Security Issues and Recommendations for Online Social Networks. In: ENISA Position Paper 1, 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf. Accessed 20 Jun 2009.
Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling. 1999;6(1):1–55.
Insidefacebook. Fastest Growing Demographic on Facebook: Women Over 55, February 2nd, 2009. http://www.insidefacebook.com/2009/02/02/fastest-growing-demographic-on-facebook-women-over-55. Accessed 20 Jun 2009.
Internet Safety Technical Task Force. Enhancing Child Safety and Online Technologies. In: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking

of State Attorneys General of the United States 2008. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf Accessed 20 Jun 2009.
Jöreskog KG, Sörborm D. LISREL-7 user's reference guide Mooresville: Scientific Software; 1989.
Jöreskog KG, Sörborm D. LISREL 8: Structural Equation Modeling with the SIMPLIS™ Command Language Chicago: Scientific Software International; 1993.
Kluemper, D, Rosen, P. A new method of employment selection: The use of social networking websites in hiring. 68th Annual Meeting of the Academy of Management. 2008.
Krasnova H, Hildebrand T, Günther O, Kovrigin S, Nowobilska A. Why Participate In An Online Social Networks: An Empirical Analysis. ECIS 2008. http://is2.lse.ac.uk/asp/aspecis/20080183.pdf Accessed 20 Jun 2009.
Krasnova H, Kolesnikova E, Günther O. It Won't Happen To Me!: Self-Disclosure in Online Social Networks. 15th Americas Conference on Information Systems 2009.
Lampe C, Ellison N, Steinfield C. A Familiar Face(book): Profile Elements as Signals in an Online Social Network. SIGCHI conference on Human factors in computing systems, USA 2007: 435–444.
Lampe C, Ellison NB, Steinfield C. Changes in use and perception of Facebook. Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work: 721–730.
Landis JR, Koch GG. The measurement of observer agreement for categorical data. Biometrics. 1977;33:159–74.
Lusoli W, Miltgen C. (2009). Young People and Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks. In: JRC Scientific and Technical Reports 2009. http://ftp.jrc.es/EURdoc/JRC50089.pdf. Accessed 20 Jun 2009.
Malhotra NK, Kim SS, Agarwal J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research. 2004;15(4):336–55.
Nunnally JC. Psychometric Theory. 2nd ed. New York: McGraw-Hill; 1978.
Pedhazur, EJ, Schmelkin LP. Measurement, design, and analysis: An integrated approach. Hillsdale, N.J.: Lawrence Erlbaum Associates; 1991.
Ryan GW, Bernard HR. Data management and analysis methods. In: Denzin N, Lincoln Y, editors. Handbook of qualitative research. 2nd ed. Thousand Oaks, CA: Sage; 2000. p. 769–802.
Schau HJ, Gilly MC. We are what we post? Self-presentation in personal web space. Journal of Consumer Research. 2003;30(3):385–404.
Segars AH, Grover V. Re-examining perceived ease of use and usefulness: a confirmatory factor analysis. MIS Quarterly. 1993;17:517–25.
Smith HJ, Milberg SJ, Burke SJ. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly. 1996;20(2):167–96.
Son J-Y, Kim SS. Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly. 2008;32(3):503–29.
Stutzman F. An Evaluation of Identity-Sharing Behavior in Social Network Communities. International Digital and Media Arts Journal. 2006;3(1):10–3.
Tufekci Z. Can you see me now? Audience and disclosure regulation in Online Social Network Sites. Bulletin of Science, Technology & Society 2008;28(1):20–36.
Walther JB. Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. Communication Research. 1996;23:3–44.
Wheeless LR, Grotz J. Conceptualization and measurement of reported self-disclosure. Human Communication Research. 1976;2(4):338–46.
Wieschowski S. Studenten demonstrieren gegen das SchnüffelVZ. In: Spiegel Online 2007. http://www.spiegel.de/netzwelt/web/0,1518,523906,00.html Accessed 20 Jun 2009.