12-17-2012

All Friends Are Equal â€“ Some Even More: An Investigation of Privacy Protection Among Facebook Users

Andre Deuker
Goethe University, andre.deuker@m-chair.net

Andreas Albers
Goethe University, andreas.albers@m-chair.net

Christoph Rosenkranz
Goethe University, rosenkranz@wiwi.uni-frankfurt.de

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

All Friends Are Equal â Some Even More: An Investigation of Privacy Protection Among Facebook Users

AndrÃ© Deuker
Goethe University, Germany

Andreas Albers
Goethe University, Germany

Christoph Rosenkranz
Goethe University, Germany

Abstract
Social networking sites (SNS) such as Facebook have created a new way for individuals to share personal data and interact with each other on the Internet. The disclosure of this personal data is directly tied to the existing relationships of individuals within an SNS. Individual privacy settings allow a selective disclosure of personal data to specific connected individuals. In this paper, we present first empirical insights of a grounded theory study, based on 37 qualitative interviews with Facebook users, which reveal factors that drive, or generally influence, the use of these individual privacy settings on SNS. By investigating this privacy protection behavior towards connected individuals, so-called â friendsâ in Facebookâ s terminology, we add new perspectives to existing theories of information privacy protection â individualsâ privacy protection behavior in nonanonymous online environments. We have developed a conceptual model showing that the motivation to use individual privacy settings depends on a complex interplay between different factors. As important drivers, motives for using SNS, existing relationships and context of personal data disclosure have been identified. Building on those insights further allows development or improvement of general privacy controls for individuals interacting with each other on the Internet.

Keywords: Social Networking Sites, Privacy Protection Behaviour, Privacy Settings, Grounded Theory

Permanent URL: http://sprouts.aisnet.org/12-17

Reference: Deuker, A., Albers, A., Rosenkranz, C. (2012). "All Friends Are Equal â Some Even More: An Investigation of Privacy Protection Among Facebook Users," Proceedings > Proceedings of JAIS Theory Development Workshop . *Sprouts: Working Papers on Information Systems*, 12(17). http://sprouts.aisnet.org/12-17

ALL FRIENDS ARE EQUAL – SOME EVEN MORE: AN INVESTIGATION OF PRIVACY PROTECTION AMONG FACEBOOK USERS

Abstract

Individual privacy settings enable members of social networking sites (SNS) to share specific personal data with selected parts of their contact network. This allows members sharing even more private data they would otherwise not want to share with all of their contacts. Although various privacy aspects have already been discussed in different disciplines, literature still lacks insights on how members protect their privacy towards different kinds of SNS contacts. Against this background we raise the research question why and how members set up individual privacy settings on SNS. We draw our results from a grounded theory study based on 37 semi-structured interviews and two focus group workshops with 41 participants. The results allow the extension of theories on members' privacy protection, particularly on privacy protection behavior in non-anonymous online environments. Furthermore, the results provide a basis for improving the design of existing privacy controls on SNS and further application areas.

INTRODUCTION

As people increasingly accomplish many facets of daily life online – both in work and in private (Boyd and Ellison, 2007; Davies 1997; Ellison et al., 2007) – it is becoming ever more important to understand the determinants of this behavior and its effects on information privacy (Belanger and Crossler, 2011; Viswanath et al., 2009). Even though the issue of privacy has been discussed and described in different disciplines for decades, research on information privacy in online settings is still an emerging field (Holvast 2009). Moreover, although the literature on information privacy behavior is rich, many theories and concepts in the body of knowledge are normative or purely descriptive (Smith et al., 2011; Xu et al., 2011).

Despite the fact that researchers have studied how individuals act with regard to privacy for decades and what users' concerns for information privacy are, the research results are fragmented and usually discipline-specific; with concepts and theories that are inconsistent and neither fully-developed nor empirically validated (Xu et. al., 2011). In particular, there have been very few studies that have considered privacy at the small group level as demonstrated by social networking sites (SNS, Beer, 2008) such as Facebook or Twitter, in which information boundaries are created in groups of various sizes and relationship levels; this entails questions such as whether and how limited-access groups differ from open access groups in their information norms and practices, or what differences exist in actual changes of privacy behavior (Smith et al., 2011).

Given the widespread adoption of SNS and the increasing public scrutiny surrounding privacy on the Internet, it is surprising that little empirical data has been collected on the privacy practices of SNS users (Lewis et al., 2008). The goal of the research reported here was to investigate the privacy preferences and the privacy behavior of members of online SNS. We analyzed the behavior of users of Facebook as one of the largest and most popular SNS regarding their privacy protection towards other connected members, so-called connected 'friends'. Specifically, we examined the preferences of users regarding their individual privacy settings – those privacy settings that enable SNS members to share specific personal data and activities with specific contacts. For example, members might share a private photo with some contacts

while they hide it from others. Against this background, we raise the following research question: *Why and how do members of SNS form individual privacy settings?*

As theory is fragmented, we have chosen an exploratory research approach, following the grounded theory methodology (GTM, Corbin and Strauss, 2008). Without the need for pre-defined hypotheses, the GTM approach allows us to consider aspects and relations that have not or only to some degree been considered in previous literature. In the next section, we provide the theoretical background and the related work of our study. Following this, we describe our research approach and design. Afterwards, we present our analysis and empirical findings. We discuss the implications of our results before we conclude the paper and give an outlook on further research.

THEORETICAL BACKGROUND AND RELATED WORK

Privacy and Information Privacy in Online Settings

Although different facets and elements of privacy can be distinguished as shown by Solove (2006) in a well-known taxonomy, privacy is and most likely will remain a diverse concept. Following Belanger et al., (2002), we understand privacy as *the ability to control and manage information about oneself*. The right of individuals for privacy is indispensable and undisputed in the development of modern societies that are based upon personal freedom and democracy (Westin 1967). The rise of the so-called 'information society' and increasing participation of individuals on the Internet has shifted the focus of research attention to *information privacy* in online settings (Davies, 1997).

The literature on information privacy is rich and covers various topics and levels of analysis (Belanger and Crossler, 2011; Smith et al., 2011). One stream of the literature specifically addresses the benefits of information privacy (Smith et al., 2011). It mainly takes on the consumers' perspective, those who are trading privacy in exchange for benefits such as financial rewards and personalization. Other researchers highlight the importance of taking a more interdisciplinary lens on information privacy, for example, incorporating a business and marketing perspective (Pavlou, 2011). The need for a consumer-centric view of information privacy is amplified by the rise of data-centric businesses such as Google and Facebook, whose revenue models rely on the availability of personal data.

Furthermore, information privacy research on an individual's level of analysis can be approached from two perspectives. In the first perspective, to which we refer to as *the individual-to-organization perspective*, the interactions between individuals as consumers and organizations as providers of services are investigated. For example, Son and Kim (2008) investigate individuals' reactions on privacy threats originating from online businesses in general. Malhotra et al., (2004) and Pavlou et al., (2007) focus particularly on the e-commerce domain. The second perspective, to which we refer to as *the individual-to-individual perspective*, comprises information privacy literature focusing on the interaction between individuals in online settings. This stream of literature comprises different kinds of computer-mediated social interactions. Here, examples can be found in the collaborative work and learning domain (Kreijns et al., 2003; Wasko and Faraj, 2005), and particularly in the growing amount of literature on SNS (Boyd and Ellison, 2007; Rosenblum, 2007, Strater and Lipford, 2008). With the rise of Web 2.0 technologies and social media, both perspectives on information privacy – the individual-to-organization and the individual-to-individual perspective – increasingly converge. For example,

Dwyer et al., (2007) describe individuals' information sharing and be-friending activities on SNS as a function of general privacy concerns, trust in the SNS (individual-to-organization perspective), and trust in other members of the SNS (individual-to-individual perspective).

Both perspectives on individuals' personal data show that privacy has an influence on the success of online business models relying on personal data and their interaction with individuals. Regarding this individual-to-organization perspective, issues of information privacy can reduce the adoption and usage of services. For example, an extension of Davis et al.,'s (1989) technology acceptance model shows that privacy and risk perceptions determine the use of IT and online services (Cazier et al., 2007). From the individual-to-individual perspective, issues of information privacy and privacy protection behavior affect the diffusion of information between individuals. This diffusion is essential, for example, in the context of viral marketing, where individuals are not purely considered to be consumers of advertisements, but also to act as distributors (Bampo et al., 2008; Porter and Golan, 2006). Consequently, understanding and supporting individuals' data sharing and protection behavior is a relevant aspect for organizations whose online business model is based on this personal data of individuals.

Privacy Protection Behavior on Social Networking Sites

As a result, privacy and personal data sharing behavior on SNS are analyzed from both business and privacy perspectives. Whereas for businesses, the main role of SNS as distributors of content and advertisements is investigated (Parameswaran and Whinston, 2007), several privacy protection aspects of personal data sharing and promoting behavior have been researched. For example, data diffusion on SNS is determined by the topology of its member networks as well as the individual characteristics of ties connecting members (Bakshy et al., 2012; Granovetter, 1973). Those ties between members can be described by different attributes such as the intimacy, intensity, and duration of occurring communication, or based on the social distance between their members (Gilbert and Karahalios, 2009).

In addition, literature on individuals' privacy protection behavior and literature on members' information consumption preferences expose a complex set of underlying reasons that determine the behavior of individuals on SNS. Such reasons vary among individuals and their corresponding motivation to use SNS (Joinson, 2008; Krasnova et al., 2008). For example, Acquisti and Grossklargs (2005) and Acquisti and Gross (2006) generally describe the complexity of privacy decision behavior on SNS, while Utz and Kramer (2009) highlight this aspect particularly with respect to the activities of members on SNS.

Furthermore, this stream of literature is also rich regarding contributions to information filtering and recommender systems (Adomavicius and Tuzhilin, 2005; Hanani et al., 2001). For example, knowledge of the interaction behavior of SNS members is often used to extract relevant posted contents from a members' network in order to aggregate it in the form of a personalized SNS newsfeed for an individual member; relevance in this context is mainly based on measuring the interaction of members with certain contents (e.g., regularly commented posts could indicate a higher relevance of their content for members). However, this ignores the fact that members could also be interested in content without someone having interacted with it beforehand (Backstrom et al., 2011; Bakshy et al., 2012; Taylor, 2011). Specifically, the role of privacy controls has been proposed as a major line of research for investigating tie strength of individuals connected with one another on SNS (Gilbert and Karahalios, 2009).

Individual Privacy Settings on Social Networking Sites

SNS such as Facebook have created a new way for individuals to share personal data. A large part of the activities of SNS members are driven by the characteristics of relationships between individuals on SNS – such as the network of friends on Facebook (Stutzman and Duffield, 2010). For example, several studies have shown that the majority of SNS members shares personal data to only specific groups of SNS contacts rather than disclosing it to everybody in their network (Taraszow et al., 2010; Utz and Kramer, 2009; Young and Quan-Haase, 2009).

Contact networks on SNS can include people that stand in different relations to an individual (Gilbert and Karahalios, 2009; Hangal et al., 2010). For decades, sociologists have investigated the different roles individuals can adopt in their life (e.g., the role of an individual in a work, social or family context). Individuals adapt a certain behavior, which they consider appropriate in a given context (Goffman, 1959; Wellman and Worteley, 1990). Individual privacy settings on SNS allow addressing this need of an individual to act in different roles in an online setting. For example, Facebook members can freely set up groups of contacts (e.g., close friends, school mates, colleagues, or acquaintances) in order to allow individuals to act differently for each group (e.g., to share only certain and different personal data in each group). Consequently, individual privacy settings of members influence the data diffusion on SNS on a micro- and tie-specific level (e.g., from an individual member perspective). However, the role and application of privacy settings has been investigated mainly on a general level, focusing on the differences between friends, friends-of-friends, and members that are in no relation to the individual (Boyd and Hargittai, 2010). A more differentiated understanding of individuals' privacy protection behavior on a micro-level is needed, considering the different social relationships universally referred to as 'friends' (Hangal et al., 2010; Houghton and Joinson, 2010).

The application of individual privacy settings determines the way data diffuses among SNS members and thus in the network as a whole. Providing these members with appropriate means to differentiate between different kinds of contacts is essential to keep their privacy protected and to allow them a high level of activity – i.e. active sharing of personal data (Van den Berg and Leenes, 2010). Thus, understanding why and how SNS members use individual privacy settings is an important aspect for SNS providers in order to establish and maintain a successful business model.

RESEARCH METHODOLOGY

The objective of this study is to provide a more differentiated understanding about individuals' actions and behavior as means of privacy protection in small group online settings. Thereby, we focus especially on (a) the individual-to-individual level and (b) on non-anonymous online environments such as SNS. We aim to uncover individuals' motivations, experiences, preferences, and actions in dealing with their most immediate audience on SNS: their network of contacts (network of 'friends' on Facebook). Thereby, we extend and connect theories on individuals' privacy protection behavior on SNS, sociological theories of behavior within groups and communities, and aspects of social network analysis.

We follow a qualitative research approach based on GTM (Corbin and Strauss, 2008). This allows us to consider facets that have not or only to some degree been considered in previous literature. Our investigation is focused on Facebook as the world's largest SNS. We decided in favor of Facebook for the following three reasons: (1) Facebook offers a large variety of personal data sharing functionalities and privacy protection mechanisms, especially in comparison to competing SNS (Bonneau and Preibusch, 2009; also documented at http:/blog.facebook.com/), (2) Facebook is one of the largest SNS in the number of users (HowManyAreThere.net, 2012), and (3) Facebook has become economically significant and has, compared to other SNS, a large socio-economic impact on society (Qualman, 2011).

Data Collection

We collected our data using several techniques. First, we conducted 37 semi-structured interviews with Facebook users that took place between March and June 2011. We used an interview guideline to maintain the interview flow in interviewee-directed interaction, asking for examples and trying to get to specific situations or events. The interview guideline was not shared with interviewees and was only used as a general outline, with lots of room for deviations and probing questions. The first part of the interview guideline consisted of questions helping us to *describe* each interviewee's usage and privacy protection behavior on Facebook. Besides demographic questions, questions of the first part of the guideline focused on:

- the frequency of usage in terms of log-ins;
- the interviewee's original motivation to join Facebook;
- whether and which data is shared;
- with whom data is shared (all Facebook members, friends-of-friends, friends, sub-groups of friends, or specific single friends);
- size and composition of the interviewee's contact network (e.g., how many distinct groups such as colleagues, school mates, close friends, and so forth can be identified in the interviewee's contact network);
- other SNS applications the interviewee is using besides Facebook and the purpose for using these SNS;

The second part of the interview guideline consisted of questions helping us to *understand* why interviewees show this particular behavior on Facebook. Exemplary questions are questions on:

- privacy awareness of the interviewee as regards Facebook (e.g., whether the interviewee experienced, heard, or read about problems and bad consequences resulting from using Facebook);
- general privacy awareness of the interviewee (e.g., whether the interviewee in general tries to avoid disclosing personal data online or whether personal data is disclosed if a sufficient benefit can be expected);
- perceived trust and attitude of the interviewee as regards the SNS provider Facebook and other, associated third party services (e.g., whether interviewees consider Facebook to be trustworthy);
- relationships towards different sub-groups in the interviewee's contact network (i.e., the interviewee's motivation to include a specific sub-group in their network of contacts; answers range from "just staying in touch" to specific kinds of interactions with other sub-groups);

- the interest in news and activities of sub-group members (e.g., which kind of information is interesting from contacts with whom interviewees intend to just stay in touch vs. activities and news of other sub-group members);

Our data collection strategy was open and based on random sampling, as we strived for analytical generalizability. We aimed to reach diversity of interviewees, particularly with regard to part one of the interview guideline (Facebook usage and data protection behavior). The sample comprises interviewees of different nationalities in the Western World, but with a focus on German interviewees (25 Germans, 4 British, 3 Americans, 2 Finns, 1 Canadian, 1 Italian, 1 Dutch). The interviewees range in age between 15 to 47 years, with 26 male and 11 female interviewees. The total experience with Facebook ranges between a few days and five years, whereas the interviewees' networks of contacts on Facebook vary between 11 to 1,581 contacts. In the second part of the study we organized two focus group workshops with 41 participants. Figure 1 depicts an overview about the whole set of study participants. It includes the participants of the semi-structured interviews as well as the participants of the focus group workshops.

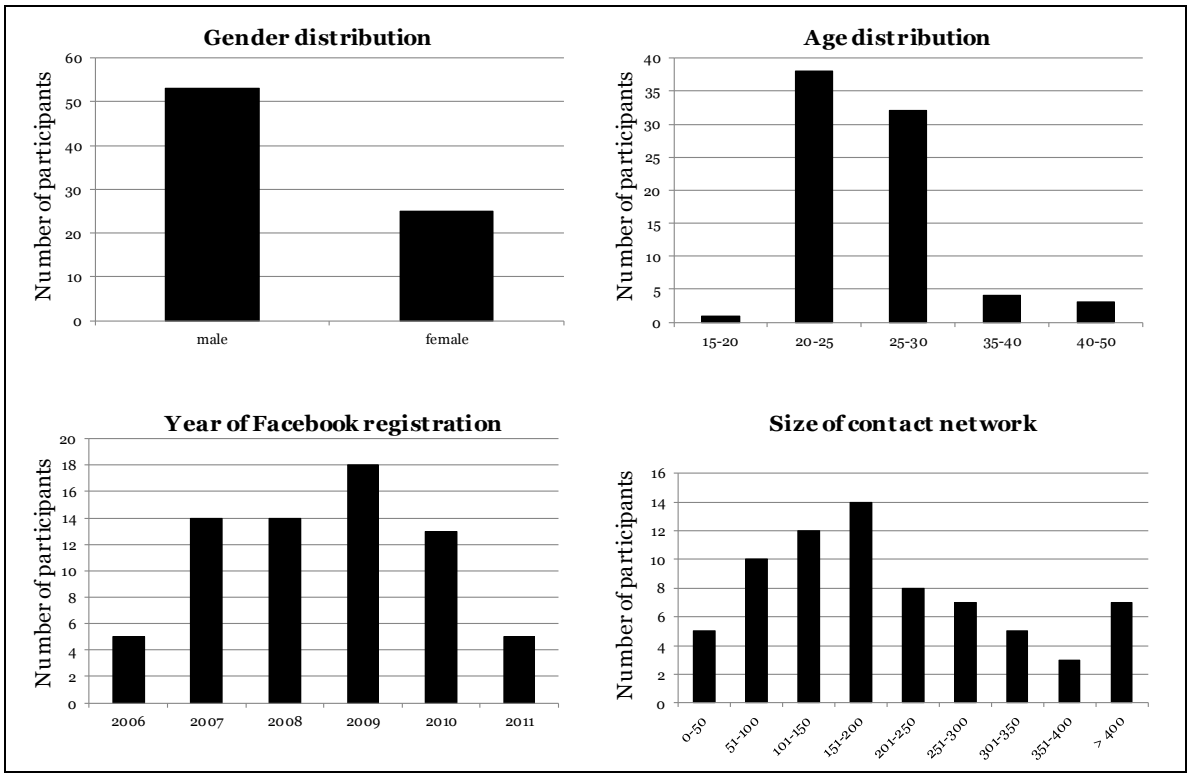

Figure 1. Participant structure

The interviews were conducted in three rounds. As literature indicates a potential bias in individuals' replies to privacy-related questions (Braunstein et al., 2011), we collected our first slice of data using Facebook channels on the Internet Relay Chat (IRC). IRC provides a tool for (anonymous) group communication, private messaging, and file exchange. It is divided into different networks that host thousands of chat rooms on a diversity of topics (Simpson, 2000).

We have chosen IRC as our first source of data collection in order to preserve anonymity of the interviewees and to create the first valid analytical benchmark for subsequent face-to-face interviews. We conducted 13 semi-structured interviews from March to April 2011 via private conversations on the IRC. The chat protocols extracted from the IRC sum up to 46 pages of text. Following this, we performed 24 face-to-face interviews with Facebook users in two rounds to collect the second and third slices of data. The interviews took place between April and June 2011. On average, each face-to-face interview lasted about 30 minutes. The interviews have been audio-recorded and transcribed, resulting in 220 transcript pages of text.

Two focus group workshops were organized based on the World Café workshop technique (Brown and Isaacs, 2005). The workshops took place in December 2011 and in April 2012. A World Café workshop aims to combine collected knowledge of all participants on a topic of mutual interest. The participants spread around a number of tables. A specific question or proposition is discussed at each table, moderated by one of the participants. Each participant is invited to share thoughts and opinions with the other participants and to note them down on a paper tablecloth. After 20 minutes, all participants except the moderators switch tables and go on with discussing another question on another table. This iterative process can achieve a deep understanding about the topic of interest. At the end, all moderators give a summary of results, which is discussed by all participants. Besides the summaries of the moderators and the discussions with the participants, we collected 23 square meters of paper tablecloth with brainstorming-like thoughts and comments on the according questions.

Data Analysis

Data collection and data analysis were conducted in parallel. That is, we analyzed and discussed the collected data already in between the three rounds of semi-structured interviews and the two rounds of World Café workshops. Thereby we compared new data with concepts and categories that emerged from previous rounds of data collection in order to spot potential contradictions and to extend the evolving theoretical concepts accordingly. Following this iterative cycle of constant comparison allowed us to keep the results of our analysis in line and consistent with the collected data (Corbin and Strauss, 2008). Furthermore, the data collected in the World Café workshops confirmed the results from the analysis of the semi-structured interviews, with no additional categories or concepts having occurred. Therefore, we jointly concluded that theoretical saturation had been reached (Guest et al., 2006).

GTM is a qualitative approach that uses a systematic set of procedures to develop an inductively derived theory about a phenomenon (Corbin and Strauss, 2008). Data analysis is conducted using three different coding procedures: open coding, axial coding, and selective coding (Corbin and Strauss, 2008). The process of data analysis was clustered into these three parts and was supported by the software program MaxQDA. First, in the process of open coding, we analyzed the collected data for recurring patterns, ideas, and concepts. In a next step of abstraction (selective coding), we identified important concepts serving as categories, other concepts representing properties of these categories, and further concepts representing dimensions of these properties. We used mind-mapping techniques that allowed us to arrange and connect the single concepts in a hierarchical and contextual order. In the third step of the analysis (axial coding), we specifically analyzed the data with a focus on passages defining and explaining relationships between the categories, their properties, and their dimensions.

In the next section, we present these categories and summarize them as well as their relationships in the form of a specific set of propositions. Together, the concepts and their

relationships form a conceptual model that is presented at the end of the next section. Following the procedures of GTM, our findings are grounded in the collected data. During selective coding, we identified constructs relationships between the higher-order categories that were identified during the open coding phase. By doing this, we selected our core categories and systematically related them to other categories, validating those relationships and filling in categories that need further refinement and development during axial coding (Corbin and Strauss, 2008). The results are presented in the following and are complemented with exemplary data (i.e., statements of the interviewees).

ANALYSIS AND RESULTS

Existing literature on SNS indicates that the reason for individuals to become members of an SNS and their resulting behavior on that SNS platform is individual for each member (Joinson, 2008; Krasnova et al., 2008). Our collected data also supports this fact. In the process of selective coding, five categories emerged that capture and describe these individual differences between members. Furthermore, they provide the foundation for explaining (1) why members apply individual privacy settings and (2) how members configure these individual privacy settings. For each identified category, the implications on the leading questions why and how members use individual privacy settings on SNS are summarized in the form of propositions.

Why SNS Members Apply Individual Privacy Settings

Reason to Connect

In terms of members' reason to use an SNS, our collected data proves to be consistent with the corresponding SNS literature (Joinson, 2008; Krasnova et al., 2008). Members distinguish each other from one another regarding their reason to use an SNS and in the way they are connected with their network of contacts (see related work). In addition to that, we noted that members' reason to connect with other SNS members can either be the same for their whole contact network or may vary for specific groups in that contact network:

- Same reason for all contacts in the network: The members' reason to be connected is the same for each contact in their network. For example, Interviewee Oliver[1] reports: "My main intention to use Facebook is to keep in touch. I don't use the SNS for regular communication". The same holds for other members who use the network more actively, e.g. to create a certain image of themselves for all of their contacts. For example, interviewee Neal stated: "… the purpose of personal profiles is to create a picture of you for others. I did that for example by filling in my favorite books and movies… I saw other profiles including educational background, career histories and other things people seemed to be proud of."
- Different reasons for specific groups of contacts: Several interviewees mentioned having different reasons to be connected with specific groups of contacts in their network. An example of this is interviewee Adele, reporting: "On Facebook I share nearly everything with my best friends, like in real life. However, other Facebook friends like colleagues or

[1] All names of interviewees in this paper are pseudonyms.

people I met during my studies or on holidays I mainly want to stay in touch. I don't want to share everything with them."

From the reasons why members connect with contacts of their network, we can conclude that they either treat all of their contacts in the same manner or differentiate between specific groups of their network. Consequently, we propose:

Proposition 1: *Members in SNS primarily distinguish between different groups of contacts because of different reasons for being connected with those contacts.*

Level of Activity

The statements of interviewees Oliver, Neal, and Adele in the previous section already indicated what has been observed across the whole sample of collected data: SNS members show different levels of activity when using an SNS. This level of activity varies in intensity of SNS usage, ranging from 'rarely' (few times per year) to 'regularly' (several times per day). But even more important for this study is the members' level of activity regarding the disclosure of personal data. It varies between being either passive or active, based on the different reasons members have to connect:

- *Passive (low level of activity)*: All interviewees stated to use Facebook as a medium to be socially-informed and entertained: *"Reading the newsfeed is like reading a newspaper, it keeps me up-to-date and many things I forget immediately …"* (Interviewee Ralph). We consider a member's behavior on SNS as passive if personal data sharing activities are scarce. For instance, Interviewee Oliver's behavior for keeping connected results in a low level of activity. Also Adele's behavior towards her colleagues or holiday acquaintances implies a low level of activity (cf. above).
- *Active (high level of activity)*: While all members stated using the SNS for consuming content, their level of activity varies from 'almost never' to 'regularly'. Interviewees share personal data to inform others about themselves, about things they care about, or to give and to receive socially related feedback: *"Maybe I post status updates and other things to receive sympathy. I mean if I personally like a link I can enjoy it on my own. I post the link so that others say 'this link is cool'."* (Interviewee Steve).

Consequently, the varying reasons of SNS members to connect go hand in hand with different levels of activity. Whereas keeping in touch and informed is typically considered a passive way of using an SNS (low level of activity), motivations like presenting oneself to contacts or receiving socially-related feedback requires a more active contribution (higher level of activity). We conclude:

Proposition 2: *Different reasons of members to use SNS lead to different levels of activities.*

Regarding the use of individual privacy settings, we noted that SNS members with an overall low level of activity have little reason to distinguish between their contacts. An example is interviewee Oliver who, as mentioned above, mainly uses an SNS to keep connected with other members. We suggest:

Proposition 3: *An overall low level of activity makes it obsolete to distinguish between different groups of contacts by means of individual privacy settings.*

Inhibitors

Several times we noted that SNS members referred to different reasons hindering them to use the SNS in a more active way. These inhibitors, as we refer to them, usually relate to aspects of members' privacy. Either members are afraid of being able to protect their privacy appropriately or that it would require simply too much effort for them. We identified the following types of inhibitors that in general prevent members showing a higher level of activity on SNS:

- *Mistrust of provider (Facebook)*: Many interviewees report having a general low level of activity because they do not trust the platform provider Facebook: *"I don't trust Facebook, it sells information. It goes into your contact lists and asks for everything. It wants to know where you work and where you graduated from, how much money you make. All information is collected in one spot."* (Interviewee Hope).
- *Reliability of privacy protection mechanisms:* Interviewees stated having reduced their level of activity (i.e. active contribution) because they do not trust the reliability of privacy protection mechanisms that are provided by Facebook: *"I don't use these privacy settings because they change these settings so often. I limit what I put on Facebook."* (Interviewee Ian). Another reason reported by several interviewees denotes the complexity of privacy protection mechanisms and the related issue whether members are capable of using these privacy controls in an appropriate manner to achieve the desired outcome: *"Recently I was tagged on a photo and friends of mine made fun out of it. I found this strange as I thought I had disabled tagging. Sometimes you cannot control what happens."* (Interviewee Taylor).
- *Effort to protect privacy:* It is well-known by the interviewees that protecting privacy on a contact-to-contact level by means of individual privacy settings is a complex endeavor. For example, interviewee Wendy reported: *"It took me quite some time to understand how to configure the access rights for different parts of my friends network […] I had to read and browse through many of these privacy setting menus"*. Not everybody is willing to take this much effort; many interviewees reportedly react to this by reducing their level of activity. An example of this behavior is interviewee Garry, who limits his level of activity by carefully selecting his network of friends: *"I like this function but I'm not using it, I'm just too lazy. I don't add people I don't like."*

In summary, many interviewees would like to be more active, but mistrust Facebook as a platform provider, do not perceive its privacy protection mechanisms as reliable, or consider the effort to protect their privacy as too high. All these factors ultimately inhibit their level of activity, which leads us to conclude:

> ***Proposition 4:*** *Individual privacy considerations (mistrust of the provider, reliability of privacy protection mechanisms, and effort to use individual privacy settings) reduce members' level of activity.*

Consequences of Privacy Threats from Contact Networks

Individual privacy settings allow SNS members to control the disclosure of personal data towards different contacts or groups of contacts in their network and thereby allow members to treat the latter differently or individually (see propositions 1 and 2). We asked the interviewees for their reasons or need to actually treat specific groups of contacts differently. We identified two different types of consequences, which members are afraid of if they are not using individual privacy settings, to distinguish between the recipients of their contributions: (a) *misinterpretation*

or unintended interpretation and (b) *misuse or unintended use* of personal data shared on an SNS platform:

- *Misinterpretation or unintended interpretation:* The first possible consequence and, at the same time, the key motivation of SNS members to distinguish between contacts is to avoid misinterpretation or unintended interpretation of shared personal data. Most interviewees consider this the most important inadvertent consequence, which can occur in their own network of contacts: *"What other people think about me is important to me. I read the newsfeed regularly and this determines how I think about others – especially of those I have not seen for a longer time. When I met them again I noticed several times, that my impression of them was completely wrong. Maybe this is because Facebook displays only some information. I don't like to get a wrong impression of others but it would be worse if others got a wrong impression of me."* (Interviewee Quentin). On a general level, we identified two reasons responsible for this worry. First, misinterpretations or unintended interpretations may be caused by incomplete information about a member, since shared personal data or activity might only reflect an extract of that member's life: *"The party photos I posted there represent just a small part of my life. However, as most of my photos on Facebook are party photos one could assume partying is a major part of my life."* (Interviewee Steve). The second reason for misinterpretation or unintended interpretation is potentially misleading personal data, such as irony, sarcasm or insider jokes: *"I've got a special kind of humor. Sometimes I post absolute nonsense just for fun. Outsiders who don't know me and just read this might think I'm an idiot."* (Interviewee Taylor).
- *Misuse or unintended use:* This second privacy threat was mentioned only in four cases. These interviewees reported that their shared personal data had been *misused or used in an unintended way.* One of these cases was described by interviewee Dorotha, who stated: *"I restricted access for some of my friends because when I met my new boyfriend one girl was trying to make things hard for me"*. The prevalent opinion among interviewees regarding threats of misuse is expressed by interviewee Hans, who states: *"I think people I've added or accepted as friends are trustworthy. They won't misuse my data."*

In summary, our data shows that individuals mainly distinguish between different groups of contacts within their contact network to avoid wrong or unintended interpretations of their data. Avoiding misuse or unintended use of personal data is an additional motivation to apply individual privacy settings. Nevertheless, SNS members seek to minimize this kind of consequence mainly by limiting access towards their contact network. We propose:

> ***Proposition 5:*** *Individual privacy settings allow members to share different personal data and show different levels of activity towards different parts of their contact network. The key motivation for this is to avoid threats of misinterpretation or unintended interpretation.*

Figure 2 documents the actual application of privacy settings of participants, including the interviewees as well as the participants of the World Café workshop participants. It shows that nearly 90 percent of our participants restrict access to at least some of their disclosed data to their contact network. In addition, 45 percent of our participants at least occasionally apply individual privacy settings to specific personal data.

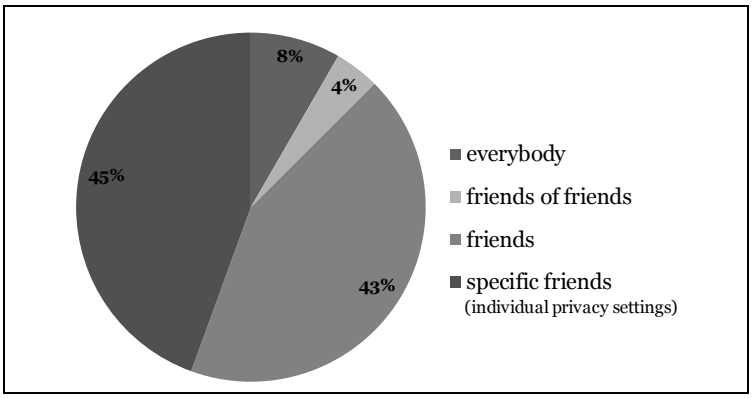

Figure 2. Most restrictive privacy settings of the participants

How SNS Members Apply Individual Privacy Settings

Composition of Contact Networks: Our interviewees' networks of contacts can be differentiated based on two factors: size and composition. The smallest size of a network which an interviewee reported consisted of 11 contacts, whereas the largest network was comprised of 1,581 contacts. The composition of members' contact network turns out to have an important impact on their privacy protection behavior. This raises the question of how many groups and which kinds of them an SNS member needs to distinguish to feel his or her privacy protected. We identified two main types of groups. These groups can be distinguished from one another in the way their members are interconnected with each other (i.e. their structure):

- *Small world network groups*: Following existing literature on social network analysis (Granovetter, 1973, Watts, 2003), we consider groups of contacts in which members are tightly interconnected with each other as "small world network groups". For example, member A is connected with the members B, C, and D whereas B, C and D are also connected with each other. Thereby, several of such groups, which occur in our empirical data, can be considered as those "small world network groups" (e.g. *'family members', 'sport club members', 'school mates', 'colleagues',* or *'former colleagues').*
- *Unconnected groups*: "Unconnected groups" are considered to be groups of contacts within a member's network that are not interconnected with one another. For example, member A is connected with member B, C and D, but B, C and D are not connected with one another. Unconnected groups describe a type of group that has been mentioned by the interviewees and does not show the characteristics of a small world network group (e.g. *'acquaintances'*, *'barely known'* or *'nearly strangers')*.

Most often, small world network groups pointed to a specific context of a members' life (e.g., colleagues at work) while unconnected groups rather display a personal relationship (e.g., acquaintances). In addition, contacts of a member can also be part of more than one group. For instance, a contact can be in the sport club as well as in the school mates group of a certain member. Furthermore, a sport club contact can also be an acquaintance of that member. We therefore suggest:

Proposition 6: *Groups of contacts within networks of contacts differentiate from one another in their structure – in particular whether the contacts in these groups are interconnected or not.*

We make this distinction between groups intentionally explicit as our collected data has shown that these group types directly determine the way members apply individual privacy settings. While the interviewees do not hesitate to differentiate between unconnected contacts, some interviewees reported to have difficulties applying individual privacy settings to differentiate between contacts that are part of a small world network group. Ellison et al., (2006) describe that individuals participate in SNS to build up social capital, which refers to network ties that are characterized by goodwill, mutual support, social trust, and mutual obligation (Huysman and Wulf, 2004). Potential loss of such social capital seems to be at least one of the reasons why members avoid distinguishing in-between a small world network group of contacts. For example, interviewee Neal reported: *"This has the potential to destroy friendships. At least it could cause severe discussions in the sense 'why did you hide this from me while A can see it?' For me this would be worse than for example the case where my personal data is sold to a marketing agency."* We conclude:

Proposition 7: *Members tend to avoid applying individual privacy settings to different contacts within small world network groups of contacts to avoid loss of social capital.*

Interpersonal Ties – Characteristics of SNS Relationships

Based upon the different groups of contacts reported by the interviewees, we investigated the characteristics of ties between the interviewees and their contacts on a tie-specific level. We asked questions such as *"Imagine you would have to write down a description of each of your contacts, including everything you know about this contact. How would these descriptions differ from one another for different contacts?"* or the other way around: "Imagine each of your contacts would have to write a description of you, including everything you think the contact knows about you. How would these descriptions look like and how would they differ from one another?" We particularly linked the answers to those questions to the different groups of contacts that the interviewees had mentioned before. For example, we asked them how the potential descriptions of such members would differ for a close friend and an acquaintance – or from sport club members and colleagues.

The answers to these and further questions allowed us to consider several dimensions of *interpersonal ties* as described by Gilbert and Karahalios (2009, see brackets). For example, the reports of the interviewees showed that the provided contact descriptions typically differ from one another in length (dimensions 'intensity' and 'duration'), amount of personal or confidential information (dimensions 'intimacy' and 'emotional support') and in topic (dimensions 'structural' and 'services'). Scrutinizing the answers along these dimensions, two facets of interpersonal ties turned out to be particularly important to determine how members distinguish between groups of contacts within their network and how they define individual privacy settings: *contextual relation* and *personal relation*.

First, *contextual relation* refers to different kinds of commonalities that a member shares with a given contact. Following Dey et al., (2001), we consider *context* as any information that describes an SNS members' situation in their life. All interviewees could place each of their contacts in specific parts of their personal life, which again can be represented by different context dimensions:

- *Leisure context*, for example, *'application members'*, *'sport club members'*, *'party acquaintances'* or *'holiday acquaintances'*.

- *Location context*, for example, *'neighbors', 'people from the place where I live', 'people from the place where I grew up'*.
- *Educational context*, for example, *'university', 'bachelor studies', 'master studies', 'school', 'primary school', 'secondary school', 'semester abroad friends'*.
- *Professional context*, for example, *'colleagues', 'former colleagues', 'colleagues at the same hierarchy', 'superiors'*.
- *Social context*, for example, *'family', 'common friends', 'partner's friends'*.

The examples of the different context dimensions above represent the groups of contacts the interviewees have mentioned and to which they have a particular reason to be connected. Most of these groups show the characteristics of small world network groups – 'holiday acquaintances' and 'party acquaintances' might be an exception here, though. However, we identified no small world network group whose focus and origin was not associated to one of these context dimensions. We propose:

> ***Proposition 8:*** *Small world network groups of contacts usually originate from and refer to a specific context of members' lives.*

Our collected data indicates the existence of a contextual relation between a contact and the personal data a member shares with this contact. Members disclose personal data in a context-specific way to their contacts. An example of this is interviewee Taylor who reports that "*being tagged on a photo is not a problem, I mean if my friends can see it. Many of them have been at the party as well … they know how it was."* A contextual relation implies that the contact has sufficient background information about the shared personal data (e.g., because the contact was together with Taylor at that party). Consequently, he or she will not interpret the data in a wrong or unintended way. We suggest:

> ***Proposition 9:*** *Members share personal data in a context-specific way. This means, they share personal data with those contacts that are affected by or involved in it.*

A second facet of interpersonal ties is the *personal relation* between the members and their individual contacts. However, determining the personal level of interpersonal ties is a complex endeavor. For example, Gilbert and Karahalios (2009) count the number of intimacy and positive words on the members' SNS walls and in their inboxes to address this. Apart from context-specific sharing of personal data, the interviewees often explained their privacy protection behavior by comparing 'close friends' or 'friends' with 'acquaintances' or 'barely known'. Many interviewees reported to share all of their personal data with close friends or regular friends, whereas they rather share only selected personal data or no personal data to contacts in a more distanced relation.

Our collected data shows that the contacts in a close or distanced personal relation with an SNS member differentiate from one another in the amount of knowledge this member has about them: "*I know much more about my good friends. Maybe I know the 100 most important things about the life of a good friend but only the ten most important things about an acquaintance.*" (Interviewee Oliver). We acknowledge that the amount of knowledge cannot alone predict social relationships on SNS. However, having only little personal data available about a contact (and vice versa: expecting the contact knows only a few things about oneself) raises the probability that shared personal data will get interpreted in a wrong or unintended way.

Many interviewees reported to share only a minimum of personal data with these contacts. Therefore, they apply very restrictive individual privacy settings for those contacts. In opposite, contacts in a close personal relationship to the SNS member have enough background knowledge about the latter to be able to interpret his or her personal data appropriately — even if there is no contextual relation. We therefore conclude:

Proposition 10: *SNS members share any kind of personal data with contacts to which they have a close personal relation. Members share little or selected personal data with contacts with which they only have a distanced personal relation.*

Conceptual Model

Figure 3 depicts a conceptual model, which links all developed concepts using the propositions as outlined above. It provides an overview of the different concepts that came out to determine members' reasons to apply and setup individual privacy settings in a certain way.

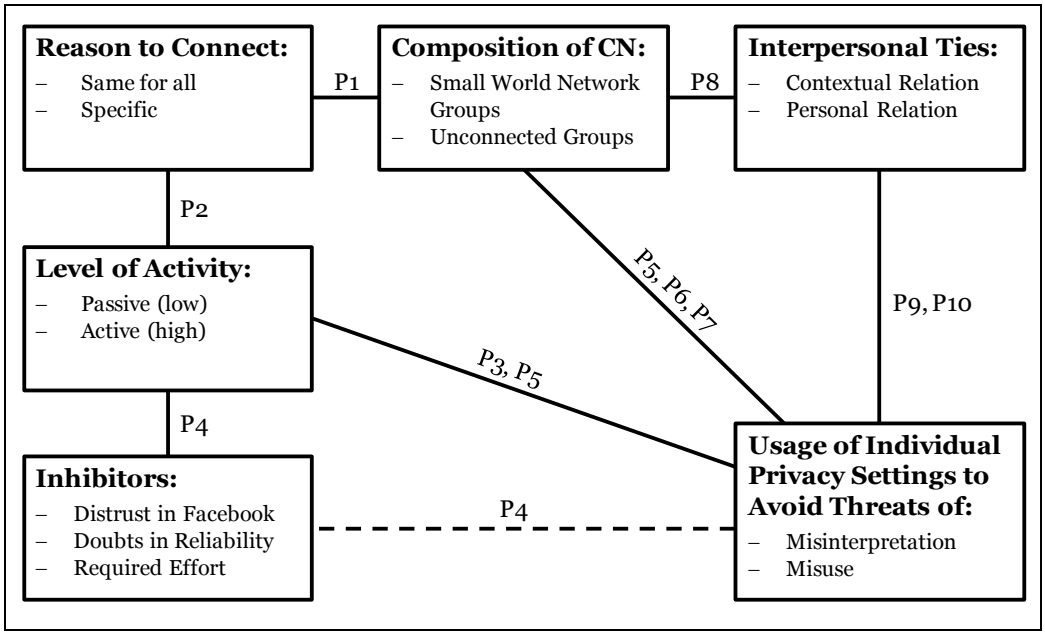

Figure 3. Conceptual Model

Many interviewees reported to have specific reasons to connect with specific contacts in their network. Thereby, members distinguish between different groups of contacts based on the reasons that they want to connect and interact with these contacts (P1). Different kinds of reasons to connect and to interact are associated with different levels of activity. For example, 'keeping connected' as the main motivation to be connected with a contact will probably result in only sporadic interactions and a low level of activity (i.e. a member merely consuming shared personal data by their contacts), whereas 'keeping others informed' will result in a more active behavior (e.g. actively sharing personal data) (P2). An overall low level of activity makes it obsolete to apply individual privacy settings, as this goes along with a low probability of privacy threats (P3). Choosing an overall low level of activity can be grounded in the fact that SNS members doubt in the ability to protect their privacy appropriately or with an adequate effort.

This also indirectly inhibits the usage of individual privacy settings, as no data has to be protected that could be subject of misuse or misinterpretation (P4).

In general, individual privacy settings allow showing different levels of activity to certain groups within the network of contacts, thereby avoiding wrong or unintended interpretation of data (P5). Groups of contacts within a member's network typically differ in their structure. Small world network groups are those groups of contacts that are tightly interconnected with one another. Unconnected groups are those groups of contacts that members can identify, but whose contacts are not interconnected with one another (P6). Individual privacy settings are configured based on both of these types of groups. However, these groups affect the way members assign individual privacy settings. In particular, members tend to avoid differentiating between members that are part of a small world network group. A reason for this is the potential loss of social capital (P7).

Whether or not specific personal data or a category of personal data is shared with a group of contacts depends on the risk that these contacts could misinterpret this personal data or interpret it in an unintended way. Members share personal data specifically with those contacts that have a contextual relation to the personal data being shared (P9) or in a closer personal relation to be able to interpret the shared personal data appropriately (P10).

DISCUSSION

The first part of our analysis provided propositions 1 to 5 as an explanation of *why* SNS members use individual privacy settings when being active on an SNS. The second part of our analysis expanded with propositions 6 to 10 as an explanation on *how* SNS members use and set up their individual privacy settings. Both parts of the results are closely related to each other. The findings have been summarized in a conceptual model (cf. Figure 3).

On a very general level, we conclude that SNS members apply individual privacy settings to (re-)establish communication patterns with their contacts, comparable to the communication patterns they have already been pursuing in the offline world (Goffman, 1959; Wellman and Worteley, 1990). In this regard, we identified and described *small world network groups* that SNS members attempt to transfer from the offline world to SNS. While such groups are genuinely separated from each other in the offline world (e.g., sport club members, colleagues at work, etc.), it requires individual privacy settings to virtually distinguish between these groups in an SNS. Furthermore, SNS members distinguish between different kinds of personal relationships within their network of contacts. Here, most often SNS members restrict access to their personal data to contacts for whom they only want to share their contact details or for whom they do not want to reject their connect request. This especially applies to contacts that are only in weak contextual and personal relation to an SNS member (e.g., 'acquaintances', 'barley known').

In the line of future research, Gilbert and Karahalios (2009) have proposed to investigate the role of privacy controls in order to predict the tie strength between SNS members. Based on our analysis, we are able to distinguish between *four types of contacts*, which are determined by the individual privacy settings of an SNS member (cf. Figure 4): A contact

- has access to everything an SNS member shares (type 1 contact),
- has access to everything but specific context-related personal data (type 2 contact),
- has no access but to specific context-related personal data (type 3 contact) or

- has no or generally limited access to personal data (type 4 contact).

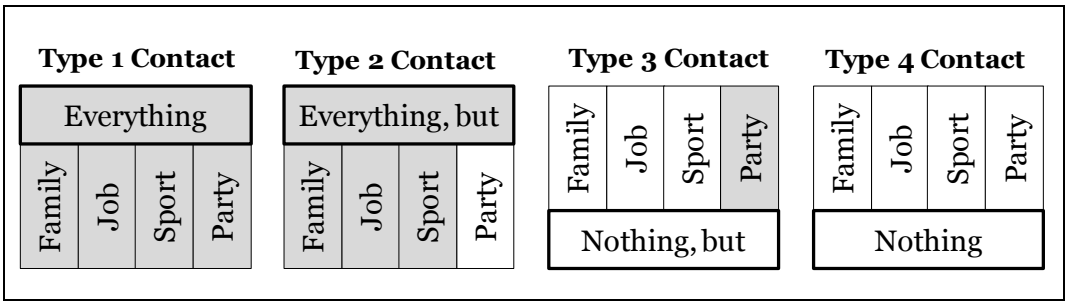

Figure 4. . Types of contacts, based on assigned individual privacy settings

Our findings on how members apply individual privacy settings indicate that these settings can be used to show (on a discrete scale) the differences in tie strength between a member and different types of his or her contacts. Most likely, type 1 contacts will be in a strong tie relationship to the member, type 4 contacts will be in a weak tie relationship, whereas type 2 and type 3 contacts of an SNS member might be in-between those two extremes.

Besides these theoretical implications, understanding why and how members use individual privacy settings on SNS also provides a number of practical implications. Our analysis has shown that SNS members use individual privacy settings to show different levels of activities towards different groups of contacts in their network. Our analysis also demonstrated that mistrust of the reliability of individual privacy settings and their related complexity keeps SNS members from engaging in a higher level of activity on SNS. In this regard, two out of three identified inhibiting factors (i.e. the reliability and the configuration effort) indicate design problems of individual privacy settings, which could and need to be addressed by the platform provider Facebook. Consequently, our insights on why and how members use individual privacy settings can be used to guide SNS members in setting up their individual privacy settings, as well as to help SNS providers in improving existing individual privacy settings design.

In addition to their original purpose of protecting privacy towards connected SNS members, individual privacy settings might be applicable and useable to other aspects of members' SNS activities. An example is filtering information that the members receive from their contact network, in the case of Facebook via a centralized newsfeed (Chen et al., 2010, Chen et al., 2011). Literature indicates that this amount of information is large and diverse in topics, almost resulting in an information overload for SNS members (Borgs et al., 2007; Koroleva et al., 2010). We noted several times that individual privacy settings are defined on a contextual basis: family-related, personal data is shared with family; job-related, personal data is shared with colleagues. This holds especially true for our type 3 contacts (no access but to specific context-related personal data). This information could be seen as an indication that a member is particularly interested in receiving contextually related data from those groups. Thereby, current information filtering systems as Facebook's edge rank system, which is mainly based on quantitative research observing SNS members' activities, could be improved by incorporating this group information (Backstrom et al., 2010; Bakshy et al., 2012; Taylor, 2011).

Although we claim that our main results can be generalized across any SNS, we have to disclose and discuss some limitations of our study. The actual importance of the single concepts

that we have identified might vary depending on the data sample composition. As our informants are mainly from Western countries, different responses regarding the potential threats originating from members' network of contacts are possible for other parts of the world. This might also affect the importance and relation of the associated categories. For example, we could imagine that interviewees from countries that do not have a guaranteed freedom of speech would consider threats of misuse originating in their own contact network or from the provider to be more important and severe, and even threatening to their lives. Consequently, we do not claim that our concepts are the only valid or useful ones to examine and explain privacy protection behavior in non-anonymous online environments such as SNS.

CONCLUSION

From a societal perspective, individuals become increasingly aware of general privacy threats on SNS and increasingly demand from their providers to protect them from the latter. Whereas there is no protection towards the SNS service provider, our analysis has shown that the members will protect their privacy towards their contacts by reducing their level of activity or abstain from using these services at all. "Real name" initiatives of many SNS (Boyd, 2011), aspects of profile likability between different online services (Zafarani and Liu, 2009), and the integration of third party services having access to members' contact network (Krishnamurty and Wills, 2009) give rise to the assumption that individual-to-individual privacy protection in non-anonymous online environments will become an even more important research topic. Our analysis on why and how members use individual privacy settings contributes to this issue. It turned out that understanding why and how members use individual privacy settings on SNS might be one of the most complex questions on individuals' privacy protection behavior to-date. It raises several complicated and interrelated questions with regard to members' general attitude towards privacy, awareness and perception of privacy threats, the motivation to use SNS, and finally to connect with other SNS members. All these questions are worth answering because an increasing amount of personal data is shared exclusively within members' network of contacts.

Our findings provide an empirical and theoretical baseline for improving existing privacy controls on SNS, for example, by reducing members' effort to configure such controls. Moreover, the insights may also help researchers or policy- and decision-makers to better understand how individuals extend the presentation of themselves in everyday live to non-anonymous online environments. In the first instance, the presented results originate from Facebook members. However, at the given level of abstraction on the level of categories and propositions summarized in Figure 1, we claim that our results hold for other SNS as well. This is supported by the statements of many interviewees and World Café workshop participants who reported to behave similarly on other SNS they use. Our results can also be transferrable to social plug-ins for e-mail applications (Fisher et al., 2006; Neustaedter et al., 2005, Yoo et al., 2009), social recommendation systems (Siersdorfer and Sizov, 2009), or even more privacy-sensitive online services such as healthcare platforms (e.g., http://www.patientslikeme.com) and electronic patient records (e.g., http://healthvault.com).

While acknowledging and describing the limitations of our approach in the previous section, we would not have been able to produce this substantial, innovative insight without applying grounded theory techniques. Our model aims to provide a theoretical baseline for subsequent quantitative studies on members' motivation to use individual privacy settings. However, the elaborated motives for using individual privacy settings require further

specification to be transferable into testable hypotheses or design guidelines. Consequently, we encourage further qualitative and quantitative research in this domain to challenge and to comment on our insights.

REFERENCES

Acquisti, A., and Grossklags, J. (2005) "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy* (3:1), pp. 26-33.

Acquisti, A., and Gross, R. (2006) "Imagined communities: awareness, information sharing and privacy protection on the Facebook," *Privacy Enhancing Technologies* (4258), pp. 36-58.

Adomavicius, G., and Tuzhilin, A. (2005) "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions," *IEEE Transactions on Knowledge and Data Engineering* (17: 6), pp. 734-749.

Backstrom, L., Bakshy, E., Kleinberg, J., Lento, T., and Rosenn, I. (2011) "Center of Attention: How Facebook Users Allocate Attention across Friends," in *Proceedings of the Fifth International Conference on Weblogs and Social Media*, Barcelona, Catalonia, Spain.

Bakshy, E., Rosenn, I., Marlow, C., and Adamic, L. (2012) "The Role of Social Networks in Information Diffusion," in *Proceedings of ACM WWW 2012*. Lyon, France, pp. 519-528.

Bampo, M., Ewing, M., Mather, D., Stewart, D., and Wallace, M. (2008) "The Effects of the Social Structure of Digital Networks on Viral Marketing Performance," *Information Systems Research* (19:3), pp. 273-290.

Beer, D. (2008) "Social network(ing) sites… revisiting the story so far: A response to danah boyd & Nicole Ellison," *Journal of Computer-Mediated Communication* (13), pp. 516-529.

Belanger, F., and Crossler, R. (2011) "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35: 4), pp.1017-1041.

Belanger, F., Hiller, J., and Smith, W. J. (2002) "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3/4), pp. 245-270.

Bonneau, J., and Preibusch, S. (2009) „The Privacy Jungle: On the Market for Data Protection in Social Networks," in *Proceedings of The Eighth Workshop on the Economics of Information Security*, pp. 121-167.

Borgs, C., Chayes, J., Karrer, B., Meeder, B., Ravi, R., Reagans, R., and Sayedi, A. (2010) "Gametheoretic Models of Information Overload in Social Networks. Social Networks," (12:1), pp. 146-161.

Boyd, D. (2011) ""Real Names" Policies Are an Abuse of Power," available at http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html, accessed on 2012-02-23.

Boyd, D., and Ellison, N. (2007) "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication* (13:1), article 11.

Boyd, D., and Hargittai, E. (2010) "Facebook privacy settings: Who cares?" *First Monday* (15:8).

Braunstein, A., Granka, L., and Staddon, J. 2011. „Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It," in *Proceedings of the Syposium on Usable Privacy and Security*, Pittsburgh, PA, USA.

Brown, J., and Isaacs, D. (2005) "The World Café – Shaping Our Futures Through Conversations That Matter," San Francisco: Berrett-Koehler.

Cazier J., Wison E., and Medlin B. (2007) "The Role of Privacy Risk in IT Acceptance – An Empirical Study," *International Journal of Information Security and Privacy* (1:2), pp. 61-73.

Chen, J, Nairn, R., Nelson, L., Bernstein, M., and Chi, E. (2010) „Short and tweet: experiments on recommending content from information streams," in *Proceedings of the 28th international conference on Human factors in computing systems*, pp. 1185-1194.

Chen, J., Nairn, R., and Chi, E. (2011) „Speak Little and Well: Recommending Conversations in Online Social Streams," in *Proceedings of the 2011 annual conference on Human factors in computing systems*, New York, pp. 217-226.

Corbin, J., and Strauss, A. (2008) "Basics of Qualitative Research 3e - Techniques and Procedures for Developing Grounded Theory," London: Sage Publications.

Davies, S. G. (1997) "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape*, P. E. Agre and M. Rotenberg (eds.), Cambridge, MA: MIT Press, pp. 143-165.

Davis, F. D. (1989) "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly (13:3), pp. 319–340.

Dey, A., Kortüm, G., Morse, D., and Schmidt, A. (2001) „Understanding and using Context," *Personal and Ubiquitous Computing*, (5:1), pp. 4-7.

Dwyer C., Hiltz S., and Passerini K. (2007) "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado, USA.

Ellison, N. B., Steinfield, C., and Lampe, C. (2007) "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication*, *12*(4), article 1.

Eppler, M., and Mengis, J. (2004) "The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines" *The Information Society* (20:5), pp. 325-344.

Fisher, D., Brush, A. J., and Smith, M. 2006. "Social Information Matters!," in *Proceedings of the 2nd Invitational Workshop on Personal Information Management* at SIGIR 2006, pp. 53-55.

Gilbert, E., and Karahalios, K. 2009. „Predicting tie strength with social media," in *Proceedings of the 27th international conference on Human factors in computing systems*, Boston, MA, USA, pp. 211-220.

Goffman, E. (1959) "The presentation of self in everyday life," New York: Doubleday.

Granovetter, M.N. (1973) "The strength of weak ties," *The American Journal of Sociology* (78:6), pp. 1360-1380.

Guest, G., Bunce, A., and Johnson, L. (2006) "How Many Interviews Are Enough?" *Field Methods* (18:1), pp. 59-82.

Hanani, U., Shapira, B., and Shoval, P. (2001) "Information Filtering: Overview of Issues, Research and Systems," *User Modeling and User-Adapted Interaction* (11:3), pp. 203-259.

Hangal, S., MacLean, D., Lam, M., and Heer, J. (2010) "All Friends are Not Equal: Using Weights in Social Graphs to Improve Search," *Proceedings of the 4th SNA-KDD Workshop*, Washington D.C., USA.

Holvast, J. (2009) "History of Privacy," in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda (eds.), Boston: Springer, pp. 13-42.

Houghton, D., and Joinson, A. (2010) "Privacy, Social Network Sites, and Social Relations," *Journal of Technology in Human Services* (28:1-2), pp. 74-94.

HowManyAreThere.net (2012) "How Many Social Networking Websites Are There," http://howmanyarethere.net/how-many-social-networking-websites-are-there/ accessed on 2012-03-14.

Huysman, M., and Wulf, V. (eds.) (2004) ”Social capital and information technology,” Cambridge, MA: MIT Press.

Joinson, A. (2008) “Looking at, looking up or keeping up with people? Motives on the use of Facebook,” in *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pp. 1027-1036.

Koroleva, K., Krasnova, H., and Guenther, O. (2010) ““Stop Spamming Me!” - Exploring Information Overload on Facebook,” in *Proceedings of the 15th Americas Conference on Information Systems*, Peru.

Krasnova, H., Hildebrand, T., Guenther, O., Kovrigin, A., and Nowobilska, A. (2008) “Why Participate in an Online Social Network? An Empirical Analysis,” in *Proceedings of the European Conference on Information Systems*, paper 33.

Kreijns, K., Kirschner, P., and Jochems, W. (2003) „Identifying the pitfalls for social interaction in computer-supported collaborative learning environments: a review of the research,” *Computers in Human Behavior* (19), pp. 335-353.

Krishnamurthy, B., and Wills, E. (2009) “Privacy Diffusion on the Web: A Longitudinal Perspective,” in *Proceedings of the 18th international conference on World Wide Web*, Madrid, Spain, pp. 541-550.

Lewis, K., Kaufman, J., and 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), pp. 79-100.

Malhotra, N., Kim, S., and Agarwal, J. (2004) “Internet Users’Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” Information Systems Research (15:4), pp. 336-355.

Neustaedter C., Brush A., Smith M., and Fisher D. (2005) “The social network and relationship finder: Social sorting for email triage.” in *Proceedings of the Second Conference on Email and Anti-Spam*, Stanford, California, USA.

Parameswaran, M., and Whinston, A. (2007) “Social Computing: An Overview,” *Communications of the Association for Information Systems* (19), pp. 762-780.

Pavlou P., Liang H., and Xue Y. (2007) “Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective” *MIS Quarterly* (31:1), pp. 105–136.

Pavlou, Paul A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly*, (35: 4) pp. 977-988.

Porter, L., and Golan, G. (2006) “From Subservient Chickens to Brawny Men: A Comparison of Viral Advertising to Television Advertising,” *Journal of Interactive Advertising* (6:2), pp. 26-33.

Qualman, E. (2011) “Socialnomics - How social media transforms the way we live and do business, revised and updated,” New Jersey: John Wiley & Sons.

Rosenblum, D. (2007) “What Anyone Can Know: The Privacy Risks of Social Networking Sites” *IEEE Security & Privacy (May/June)*, pp. 40-49.

Siersdorfer, S., and Sizov, S. (2009) “Social Recommender Systems for Web 2.0 Folksonomiesm,” in: *Proceedings of the 20th ACM Conference on Hypertext and Hypermedia*, Torino, Italy, pp. 261-270.

Simpson, Carol. (2000) “Internet Relay Chat” *Educational Media and Technology Yearboo*k (25), pp. 62-65.

Smith, H. J., Dinev, T., and Xu, H. (2011) “Information Privacy Research: An Interdisciplinary Review,” *MIS Quarterly* (35:4), pp. 989-1015.

Solove, D. J. (2006) "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (Vol. 154:3), pp. 477-560.

Son, J.Y., Kim, S.S. (2008) "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.

Strater, K., and Lipford, H. (2008) "Strategies and struggles with privacy in an online social networking community," in

Stutzman, F., Duffield, J. (2010) Friends only: examining a privacy-enhancing behaviour in facebook. In CHI '10: Proceedings of the 28th international conference on Human factors in computing systems, pp. 1553-1562.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., and Arsoy, A. (2010) "Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example," *International Journal of Media and Cultural Politics* (6:1), pp. 81-102.

Taylor, D. (2011) "Everything you need to know about Facebook's EdgeRank," http://thenextweb.com socialmedia/2011/05/09/everything-you-need-to-know-about-facebooks-edgerank/, accessed on 2012-03-16.

Utz, S., and Kramer, N. (2009) "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms," *Cyberpsychology: Journal of Psychosocial Research on Cyperspace* (3:2), article 1.

Van den Berg, B., and Leenes, R. (2010) „Audience segregation in social network sites," in *Proceedings of the Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust*, Washington D.C., pp. 1111-1117.

Viswanath, B., Misolve, A., Cha, M., and Gummadi, K. (2009) "On the evolution of user interaction in Facebook," in *Proceedings of the 2nd ACM workshop on Online social networks*, pp. 37-42.

Wasko M.M., and Faraj S. (2005) "Why should I share? Examining social capital and knowledge contribution in electronic networks of practice," *MIS Quarterly* (29:1), pp. 35–57.

Watts, D. J. (2003) "Six Degrees: The Science of a Connected Age," New York:W W Norton & Co.

Wellman, B., and Wortley, S. (1990) "Different Strokes from Different Folks: Community Ties and Social Support," *American Journal of Sociology* (96:3), pp. 558-588.

Westin, A. (1967) Privacy and Freedom, New York: Atheneum.

Xu, H., Dinev, T, Smith, J., and Hart, P. (2011) "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12: 12), article 1.

Yoo S., Yang Y., Lin F., and Moon I. (2009) "Mining social networks for personalized email prioritization," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, Paris, France, pp. 967-976.

Young, A., and Quan-Haase, A. (2009) "Information revelation and internet privacy concerns on social network sites: a case study of Facebook," in *Proceedings of the fourth international conference on communities and technologies* , pp. 265-274.

Zafarani R., and Liu, H. (2009) "Connecting corresponding identities across communities," *Proceedings of the 3rd International Conference on Weblogs and Social Media*.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts