Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2012 Proceedings

European Conference on Information Systems (ECIS)

5-2-2012

# THE USAGE OF INDIVIDUAL PRIVACY SETTINGS ON SOCIAL NETWORKING SITES - DRAWING DESIRED DIGITAL IMAGES OF ONESELF

André Deuker
*Goethe University*

Christoph Rosenkranz
*Goethe University*

Andreas Albers
*Goethe University*

# THE USAGE OF INDIVIDUAL PRIVACY SETTINGS ON SOCIAL NETWORKING SITES – DRAWING DESIRED DIGITAL IMAGES OF ONESELF

Deuker, André, Goethe-University, Grüneburgplatz 1, RuW Building, 60323 Frankfurt, Germany, andre.deuker@m-chair.net

Rosenkranz, Christoph, Goethe-University, Grüneburgplatz 1, RuW Building, 60323 Frankfurt, Germany, rosenkranz@wiwi.uni-frankfurt.de

Albers, Andreas, Goethe-University, Grüneburgplatz 1, RuW Building, 60323 Frankfurt, Germany, andreas.albers@m-chair.net

## 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 behaviour towards connected individuals, so-called 'friends' in Facebook's terminology, we add new perspectives to existing theories of information privacy protection – individuals' privacy protection behaviour in non-anonymous 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, Facebook, Privacy Protection Behaviour, Privacy Protection Strategies, Individual Privacy Settings, Grounded Theory.*

# 1 Introduction

Individuals in the information society no longer merely use the Internet to search for information or to buy online, they also make intensive use of virtual communication and collaboration platforms (Vossen and Hagemann 2007). Online communities and *social networking sites* (SNS, Beer 2008) allow people with common interests to come together at little cost, help them to exchange ideas, and coordinate their activities (Rheingold 1993, Preece 2000, Preece 2001). SNS have now existed for more than 15 years and have continuously evolved (Boyd and Ellison 2007). As a result, SNS increasingly have an important impact on the social life of individuals and, consequently, on our society as a whole (Qualman 2011). Research on SNS is currently still an emerging field (Boyd and Ellison 2007). Existing studies mainly focus on measuring benefits or identifying factors that influence the acceptance of specific technologies. Given the impact of sharing personal data via SNS on an individual's social life and our society (Viswanath et al. 2009), SNS have increasingly moved into the focus of information privacy research (Belanger and Crossler 2011). Previous research on information privacy concerns has shed light on examining practices, actions of individuals and (mostly) consumers' concerns for information privacy. However, many theories and concepts in the body of knowledge are normative or purely descriptive and have not been addressed in empirical research on privacy - rigorous empirical studies are scarce (Smith et al. 2011). In particular, there have been very few studies that have considered privacy at the small group level such as demonstrated by SNS 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 processes, or what differences exist in actual changes of privacy behaviour (Smith et al. 2011).

In this paper, we investigate the privacy protection behaviour of SNS members with regard to their own network. This allows us to investigate individuals' privacy protection behaviour in a (partially) non-anonymous online environment. We do so by investigating and identifying factors that drive and influence the use of individual privacy settings within SNS. Whereas *general privacy settings* on SNS allow members to calibrate the disclosure of data towards the whole audience of an individual (e.g., other members, non-members and third-party services), *individual privacy settings* allow users to segregate the disclosure of such data to different parts of their network (e.g., sharing a certain picture only with individual friends or a pre-defined group such as 'close friends and family'). Despite this, only little systematic research has been conducted on SNS privacy controls in general (Bonneau and Preibusch 2009, Boyd and Hargittai 2010) or on the usage of individual privacy settings in particular. Distinct knowledge about individual privacy settings would help SNS providers, policy and decision-makers that need to address the increasing demand of individuals to be able to protect their privacy on SNS, but also to understand members' privacy protection behaviour in non-anonymous online environments in general. Consequently our research question is: *"Whether, why, and how do SNS members use individual privacy settings to protect their privacy?"*

In order to address this research question, we have adopted an exploratory research approach, following the Grounded Theory Methodology (GTM). Prior literature (e.g., Acquisti and Grossklags 2005, Acquisti and Gross 2006, Utz and Kramer 2009, Belanger and Crossler 2011) has shown that the motivations underlying the decision to disclose data or not, and to use privacy settings or not are manifold, varied and complex. Moreover, the overall stream of privacy research builds on normative arguments and theories (Smith et. al. 2011). Without the need for predefined hypotheses, the GTM approach allows us to consider facets that have previously not or only to some degree been considered. The focus of our study is on SNS, particularly on the world's largest SNS Facebook (HowManyAreThere.net 2011). The remainder of this paper is structured as follows: In Section 2, we discuss the related work and the theoretical background of our research. In Section 3, we describe and discuss our research design and present our findings in Section 4. Finally, in Section 5, we discuss our findings and conclude by providing an outlook on further research.

# 2 Theoretical Background and Related Work

Numerous studies in many fields have improved our understanding of privacy and privacy behaviour in general (Smith et al. 2011). Poor information practices or poor privacy programs can result in a variety of privacy problems that are associated with individuals' concerns for information privacy (Solove 2008). However, 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). Similarly, a multitude of researchers have been addressing several SNS-related privacy aspects so far. On a general level, users' privacy decision-making displays a dichotomy between individuals' attitudes towards their privacy and their actual behaviour (Nordberg et al. 2007) as well as their willingness to trade privacy for convenience or other benefits (Acquisti and Grossklags 2005). This is also reflected in individuals' usage of SNS (Acquisti and Gross 2006). Active participation on SNS exposes members to privacy risks such as identity fraud, identity theft, being stalked or being under surveillance (Gross and Acquisti 2005). Beside a lack of awareness, motives of narcissism and impression management can be an incentive to take some of these risks (Utz and Kramer 2009).

A typical privacy protection strategy is to limit the visibility of disclosed data to a network of connected friends. For example, more than 50% of Utz and Kramer's (2009) sample, 64% of Young and Quan-Haase's (2009) sample and 76% of Taraszow's et al. (2010) sample of individuals limit disclosed data to the audience of their network of friends. As networks of friends can include individuals with very different social relationships to other members (Wellman and Wortley 1990, Gilbert and Karahalios 2009, Hangal et al. 2010), the protection of individuals' privacy towards other connected members has gained considerable importance (Stutzman and Duffield 2010). Overall, research on online privacy, privacy settings and privacy protection strategies is an emerging field. While the above existing studies mainly focus on measuring or describing such behaviour, it is our aim to identify factors that drive and influence privacy protection strategies in order to explain and predict this behaviour. Few theories or models exist that deal with individuals' online privacy protection behaviour in relation to their online social network. In this paper, we investigate the role of individual privacy settings as a means for privacy-enhancing behaviour on SNS. Thereby, we want to add a new facet to the general understanding of individuals' privacy protection behaviour outlined above, to the relation between members' SNS activity and privacy concerns (Rosenblum 2007, Livingstone 2008, Posey et al. 2010), to the use and awareness for privacy controls in general (Adu-Oppong et al. 2008, Boyd and Hargittai 2010), and to the question of how privacy settings constitute an indicator for social relationships (Gilbert and Karahalios 2009, Ledbetter et al. 2010).

# 3 Research Methodology

The objective of our study is to understand how SNS members protect their privacy and to learn about the particular role of and rationale for using individual privacy settings. We acknowledge the related work with regard to privacy protection of/by individuals (cf. Section 2). However, we aim for a deeper understanding in that matter: we want to uncover individuals' inner experiences and motives leading to the application of individual privacy settings. This allows extending theories on privacy protection by considering privacy protection in the non-anonymous environment of members' network of friends. To provide this novel and unique perspective on the usage of privacy settings on SNS our data collection, data analysis, and theory development are oriented upon the grounded theory methodology (GTM, Corbin and Strauss 2008). This allows us to consider facets that have not or only to some degree been considered in the existing literature.

## 3.1 Data Collection

The number of SNS is large and growing (Boyd and Ellison 2007, HowManyAreThere.net 2011). We have chosen Facebook and its users as the subject of our investigation because (a) Facebook offers a large variety of data sharing functionality and privacy control mechanisms (Bonneau and Preibusch

2009; also documented at http://blog.facebook.com/), (b) Facebook's large number of users (Owyang 2008, 2009, 2010), (c) Facebook's economic importance in comparison to other SNS (eMarketer.com 2011) and (d) its socio-economic impact on society (Qualman 2011). We conducted 37 semi-structured interviews with Facebook members in three rounds between March and June 2011. The sample selection strategy is open and based on random sampling as we strive for analytical generalisability. The sample comprises interviewees of different nationalities in the Western World, but with a focus on German informants (25 Germans, 4 British, 3 Americans, 2 Finns, 1 Canadian, 1 Italian, 1 Dutch). Interviewees range in age from 15 to 47 years, with 26 male and 11 female interviewees, total experience with the Facebook system between a few days and five years, and networks of friends on Facebook ranging from 11 to 1,581 contacts. As the literature has indicated, there is a potential bias in individuals' replies to privacy-related questions (Braunstein et al. 2011), so we collected our first slice of data using Facebook channels on the Internet Relay Chat (http://www.irc.org/). This preserved the interviewees' anonymity and promised to deliver a valid analytical benchmark for the subsequent face-to-face interviews. The first slice of data comprises 13 personal chat protocols summing up to 46 pages of text. The second and third data slices comprise eight and 16 semi-structured face-to-face interviews with Facebook users. On average, each face-to-face interview lasted about 30 minutes. Each of the interviews has been audio-recorded and transcribed, resulting in up to 220 transcript pages of text. After the second round of interviews and the analysis of the third slice of data, we jointly concluded that theoretical saturation was reached (Guest et al. 2006).

### 3.2 Data Analysis

Data collection and data analysis were conducted in parallel. Intermediary results were analysed and already discussed by the research team in between the three rounds of interviews. Insights collected from each slice of data were compared with the already existing insights to identify and to explain potential contradictions, but also to adapt the interview guideline accordingly. This inductive-deductive cycle of constant comparison (Corbin and Strauss 2008, p. 65) allowed us to develop a consistent model of individuals' privacy protection behaviour and their rationale to use individual privacy settings. The process of data analysis is clustered into two parts. First, in the process of open coding, we analysed the data material for recurring patterns, ideas, and concepts (Corbin and Strauss 2008, p. 65). This included a process of abstraction where we identified a few concepts as (core) categories or properties of these categories, whereas other concepts were identified as specific dimensions of the categories' properties (cf. Section 4.1). In the second step of analysis, we analysed the data with particular focus on the categories' relationship to one another by using axial coding (Corbin and Strauss 2008, p. 195). This process resulted in a conceptual model (cf. Section 4.2).

## 4 Study Findings

### 4.1 Digital Footprint, Perceived Privacy Threats and Privacy Protection Strategies

In order to get an initial impression about how individuals use Facebook, we collected the interviewees' motivation to join the platform, and their focus of activities on Facebook at the beginning of each interview. First, we noticed at a very early stage in our analysis that different ways of using Facebook create different digital traces, further referred to as the category *digital footprint* of each user. The property *focus of activities* of this category describes different ways of how individuals can use Facebook.

*Passive consumption* leads to a weak digital footprint. It comprises activities that focus, for example, on using 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).

In contrast, *active contribution* results in a more detailed digital footprint. Members who actively participate in Facebook post data to inform others about things they care about, or to give and 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).

Another motivation for active contribution is to create and shape a public profile. Each of the interviewees showed elements of passive consumption, while the degree of active contribution varied from 'rarely' (few times a year) to 'regularly' (several times a day) among the interviewees:

*"[...] the purpose of personal profiles is to create a picture of you for others. I did that for example by filling in my favourite books and movies… I saw other profiles including educational background, career histories and other things people seemed to be proud of."* (Interviewee Neal).

In order to learn how individuals protect their digital footprint from prying eyes, we subsequently asked questions about their immediate *audience of activities* – their network of friends on Facebook. More interestingly the size of an individual's network of friends (varying between 11 and 1,581) were the answers to questions on whether and how they categorise their network of friends. This resulted in a number of sub-networks. We noted that the interviewees' networks of friends are composed of sub-networks that can be described by two different types of relationships: *social distance* and *topical relation*. Sub-networks that were mentioned and characterised based on social distance were, for example, 'close friends', 'friends', 'acquaintances', 'barely known' or 'nearly strangers'. Stated sub-networks based on a topical relation were more diverse and reflect different parts of an interviewees' life. An example is 'using the same application'. Most often, people assigned both a blend of social distance and a topical relation to the individual members of their network of friends; for example, 'family members', 'school mates', 'student fellows', 'colleagues', 'former colleagues', 'club mates' or 'neighbours'.

Subsequently, we asked the interviewees about the privacy threats originating from their usage of Facebook. Thereby, we noticed that potential privacy threats go back to different *origins*. At first, it is the Facebook platform itself or, more general, the *SNS provider*. Interviewees fear losing control of data once they have disclosed it on the platform. They fear that their data is misused or used in a way not intended by them, for example, that the provider sells their personal data to third parties:

*"I think Facebook handles my data not that trustworthily like I wish they'd do. Instead they're doing many things… they sell my data and so on."* (Interviewee Adele).

Another potential threat is that the SNS provider changes settings or functionalities without informing the members properly or asking for confirmation:

*"[...] there are many changes in the system I haven't noticed immediately. I can just trust in the power of media or to be duly informed by my own network of friends*" (Interviewee Steve).

*Unconnected individuals* (unconnected members, but also non-members) that can access this personal data constitute a second origin of potential threats:

*"[...] the first thing I did was to turn off the visibility of my profile in Google search results"* (Interviewee Virginia).

Potential threats originating at unconnected individuals are less predictable, as in this case members of Facebook simply do not know or are not aware of who accesses their profile:

*"Personal information I've disclosed in my profile is not really critical, but it is related to my name… one can use this information to gather even more information about me. My address for example."* (Interviewee Zara).

The members' network of friends constitutes the third origin of potential privacy threats:

*"[...] okay it's called network of friends, but few of them are actually friends… some of them I see less*

*than once a year."* (Interviewee Xavier).

While we were analysing the threats related to the interviewees' network of friends, we noticed that a different type of threat has emerged, which is different to the type of threats that were mentioned in relation to the SNS provider or to people outside the interviewees' network of friends. Most threats originating from an SNS provider or from unconnected individuals can be described as threats of *misuse or unintended use*, whereas most threats originating from the individuals' social network can be described as threats of *wrong or unintended interpretation* of disclosed data:

*"What other people think about me is important to me. I read the news feed 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).

This latter type of threat is very important because it was mentioned across a wide number of interviews. Therefore, we suggest that it is essential to distinguish between threats of misuse or unintended use and threats of wrong or unintended interpretation.

Understanding how individuals protect their privacy on SNS is also closely related to the question of how they become aware of potential privacy threats. We explicitly considered this aspect: every time a potential privacy threat was mentioned by the interviewees, we asked how they became aware of it. *Media* is the *source of awareness* that is intuitively the most obvious one. When we asked the interviewees how they become or became aware of potential privacy threats in general, most interviewees very promptly referred to television, radio reports, newspaper articles, internet sources or media in general (e.g., *"I changed the privacy settings just because of press releases and media reports"*, Interviewee Paul). *Personal experience and learning* are a second source of awareness, but less obvious if compared to media. Although we noted already at the beginning of the data collection in one of our theoretical notes *"The interviewees have a rich set of personal experiences that determines their data protection behaviour on Facebook",* the related statements did not pour out of the interviewees like in the case of media.

Here, we benefited from the qualitative approach of using semi-structured interviews because we could ask questions that were more specific. This allowed us, for example, to distinguish between different personal experiences leading to an awareness of potential privacy threats:

- Individuals collect personal experiences about potential privacy threats by learning from similar systems – *"Before I joined Facebook I was using another SNS already. When I registered on Facebook I had a certain sensibility for the privacy topic"* (Interviewee Neal).
- Individuals learn through conversations, discussions and stories spreading across their own social network - *"A friend told me about a girl who joined the Facebook group 'fuck for world peace'. In a job interview she was asked by the interviewer what she would do to save world peace"* (Interviewee Ralph).
- Individuals become aware of potential privacy threats by experiencing them on their own or by observing them in their own social network – *"Personally I had no bad experiences but a photo of a friend of mine was manipulated and circulated in the network. Therefore I'm very careful what I disclose and to whom."* (Interviewee Uli).
- Individuals become aware of potential privacy threats by observing the data sharing and privacy protection behaviour of others - *"Many people disclose personal information that should stay private. It's damaging their reputation."* (Interviewee Ralph).

In the process of axial coding, it turned out that media and individuals' personal experiences are both sources of privacy awareness, but affected different types of potential privacy threats. Media especially creates awareness of threats of misuse or unintended use, that is, the unintended usage of personal data by Facebook, or individuals that are not part of a member's network of friends. Personal

experiences create awareness of threats of misuse or unintended use (e.g., a manipulated, embarrassing picture of an individual) as well as threats of wrong or unintended interpretation (e.g., misinterpreted data that can harm one's reputation).

An individual's motivation to pursue privacy protection measures is to avoid the set of potential threats that they are aware of – the perceived privacy threats. So how do Facebook members respond to privacy threats they are aware of? Three *privacy protection strategies* on Facebook emerged from our collected data. *Limited disclosure* is the most secure strategy and based on the insight: *"Information I don't disclose cannot be misused"* (Interviewee Eliot) or interpreted in the wrong way.

*Identity blurring* is a strategy making it harder to relate disclosed data to an individual's real identity in order to protect their privacy:

*"I've chosen a profile picture where it's hard to identify me… instead of my real name I've chosen a pseudonym that sounds slightly different from my real name. I did that because I don't want everybody to find me"* (Interviewee Adele).

*Limited distribution* refers to the specification of access rights for data once it has been disclosed on an SNS. In the course of this investigation, we focused on (a) general privacy settings, used to distinguish between non-members, unconnected members, indirectly connected members (friends of friends) and directly connected members, then (b) on individual privacy settings to distinguish among directly connected members in one's own network of friends. Further ways to limit distribution on Facebook are the disclosure of content in closed topical groups and the disclosure of data by means of personal messages. Apart from these Facebook-specific ways, limiting distribution by using different SNS for the distribution of different data (e.g., private data via Facebook, professional data via LinkedIn) is another way to control the audience of disclosed data.

We noticed that members have a trade-off between the limited disclosure and the limited distribution strategy to address threats originating from their own network of friends because of at least two factors: First, some members prefer to choose the limited disclosure strategy since it requires less effort and time:

*"I don't want to think about this [about who should have access to a posted content] every time I post something. Instead I already decided at the beginning to post only such information that can be seen by everybody in my friend network."* (Interviewee Virginia).

Second, some members decide in favour of the limited disclosure strategy because fine-grained specification of access rights bears some privacy pitfalls in itself. At least to a certain degree, privacy settings are considered to be a statement on the status of a friendship or relationship:

*"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."* (Interviewee Neal).

In conclusion, we notice that the rationales behind peoples' decision for privacy strategies are manifold and complex. Any explanation and measurement of members' usage of privacy settings on SNS requires careful consideration of the interrelationships between the different privacy protection strategies.

## 4.2 Conceptual Model

Figure 1 summarises our findings as a complex interplay between digital footprint, potential threats, sources of awareness and resulting privacy protection strategies. The axis between the main categories *privacy protection strategies* and *perceived privacy threats* is based upon the relationship of *potential threats* and *privacy protection strategies* that members use to address them. *Limited disclosure* turned out to be the most powerful and universal strategy. It can be used to avoid both types of threats and threats of each origin. *Identity blurring* in turn focuses especially on threats originating from the unconnected individuals. *Limited distribution* refers especially to unconnected individuals (general

privacy settings) and threats originating from the members' own network of friends (individual privacy settings). For threats originating from the network of friends, *limited disclosure* and *limited distribution* are the strategies of choice that members use to protect their privacy.

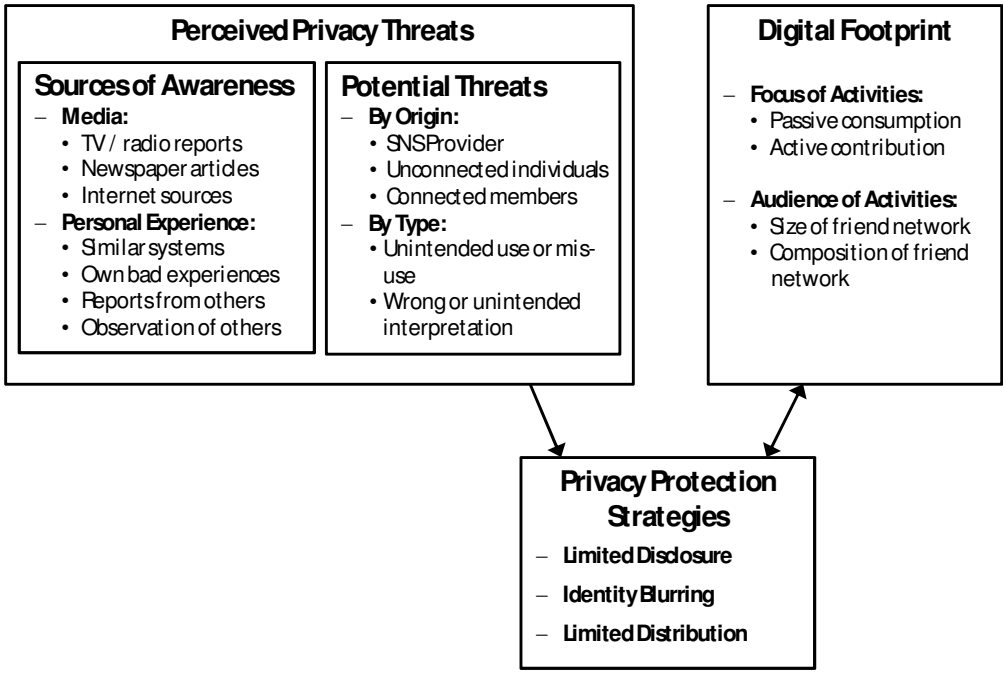


*Figure 1. Conceptual relationships between the core categories.*

The axis between the main category *privacy protection strategies* and *digital footprint* reflects the fact that the selection of *privacy protection strategies* has a significant influence on the *focus of activities* and vice versa. Individuals, who use Facebook mainly for passive consumption of contents, have less reason to pursue privacy protection strategies than members who are willing to actively contribute and participate. Individuals who limit the distribution of data in order to protect their privacy naturally at the same time reduce their level of active contribution and participation:

*"There is a trade-off between protecting my private sphere and disclosing personal information about me. As my close friends and other friends know about this information anyway, I decided to disclose only a few personal pieces of information."* (Interviewee Neal).

In addition, threats originating in a member's network of friends can be described by the relation between *audience of activities* and *privacy protection strategies*. Thereby, a small and homogenous network of friends seems to be less prone to threats of unintended or wrong interpretation than a large and inhomogeneous network comprising many different sub-groups.

## 4.3 Consequences for the use of Individual Privacy Settings

The theoretical model described in Figure 1 provides the opportunity to discuss whether, why and how members of Facebook use individual privacy settings to protect their privacy. First, members use individual privacy settings to limit the distribution of data within their network of friends. Wrong or unintended interpretation of disclosed data emerged as the main type of threat people are afraid of with regard to their own network of friends. However, individuals who decide to disclose less data about themselves to protect their privacy have no or little need to use individual privacy settings:

*"If I decided to use Facebook more intensively I would have to use privacy settings. For example satirical posts should be visible only to my close friends who know that they don't have to take them seriously"* (Interviewee Uli).

Individual privacy settings can be assigned on an individual basis, for example, a photo is visible to person A and person C, person G and person K, but also based on predefined lists of people. This photo is visible to list 1 (comprising A and C) and list 2 (comprising G and K). To answer how the interviewees decide on the distribution of these individual access rights, we asked about the predefined lists some of the interviewees have formed in order to assign individual access rights. It turned out that these lists follow the same pattern described above (cf. Section 4.1) on the composition of the interviewees' network of friends.

The access right for a given content that a member aims to disclose depends on the social distance between the member and the potential audience, and whether or not there is a topical relationship between the potential audience and the content to be disclosed. Many interviewees identified photos as the kind of media that has the highest potential to be misinterpreted. However, other contents are affected as well. Interviewees seek to minimise the probability of wrong or misinterpretation by assigning access rights rather to close friends than to acquaintances. This is because close friends typically have a profound knowledge about the member who discloses the data and can interpret the content based on this knowledge:

*"Photos on Facebook show some specific parts of my life. People who know me know how to take them but others could get a wrong impression about me."* (Interviewee Steve).

*"I've got a special kind of humour. 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).

*Topical relation* refers to the question of whether the audience has knowledge about the specific piece of data, for example a photo. Assuming the photo is a party photo, other party guests have a topical relationship to the photo when they have been to this party as well. They will interpret the photo in the context of the data they have about the situation, resulting in a lower probability for wrong or unintended interpretation.

*"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. But someone who was not there and who let's say should have a more serious picture of me does not necessarily need to see this photo. For example my boss."* (Interviewee Taylor).

In Section 4.1, we identified that threats originating from the individuals' social network mainly are related to threats of *wrong or unintended interpretation* of disclosed data. For a given content, the potential to be wrongly or unintendedly interpreted is affected by social distance and topical relation of individuals. Figure 2 summarises the potential for misinterpretations of a specific disclosed content based on the social distance and topical relation of individuals – which may overlap freely to some degree. A few interviewees also used individual privacy settings primarily because they were afraid of threats of misuse or unintended use originating from their network of friends. Here, the social distance seems to have the strongest influence on the decision of who will be granted access to a given content.

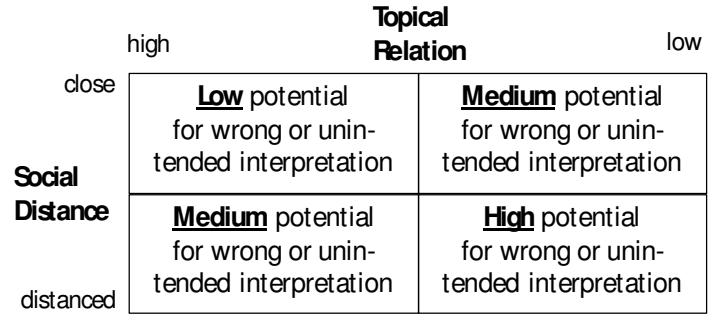


*Figure 2. Potential for misinterpretation with regard to social distance and topical relation.*

# 5 Discussion and Conclusion

In many cases, members of SNS restrict the visibility of their profile and their interaction on the SNS to their network of friends, and exclude unknown or unconnected members (cf. Section 2). Our study has shown that threats regarding the protection of members' privacy also do exist within this network of friends. In this regard, a dominant threat for individuals is the fear of wrong or unintended interpretation of disclosed data, which may result in the creation of an undesired image of oneself. To avoid this perceived threat, members limit either their disclosed data or the visibility of this data. Limiting disclosure implies relinquishing the opportunity to receive socially-related feedback or to create and shape a public profile. In contrast, being actively involved and established in an online social network and simultaneously protecting one's privacy often requires considerable effort by individuals to manage their individual privacy settings. This effort is frequently avoided.

The consequences of using individual privacy settings on SNS, which we draw from our conceptual model, are grounded in the analysis of our collected empirical data. Although we claim that our main results can be generalised, the actual importance of the single concepts we identified and put into relation to one another may vary depending on the sample composition. For example, our informants are mainly from Western countries and we could well imagine very different responses of individuals from countries that do not have the guarantee of freedom of speech. In this case, individual privacy settings might be predominantly used to avoid misuse of critically posted data, in the sense that it is forwarded to a public body, and less to avoid wrong or unintended interpretation. The same holds true for the sources of awareness – although we claim to have covered the main sources of awareness for potential threats, the importance of the single components and the relation to the connected potential threats we discovered might be especially true for Western countries. Consequently, we do not claim that our concepts are the only valid ones to use to examine privacy protection strategies. Other factors such as users' skills, characteristics and goals, power, or culture may also play key roles in causal explanations.

From a societal perspective, individuals have increasingly become privacy-aware and demand to be able to protect this privacy on SNS (cf. Section 2). In the near future, understanding this demand of users may become a crucial requirement for SNS and other online applications in developing a successful business value proposition. The findings at hand provide a first building block of knowledge for researchers, policy and decision-makers, and SNS providers to understand how members can use SNS while considering their privacy needs. The results might also apply to application systems that are similar to SNS, for example, social plug-ins for e-mail browsers, or even more for privacy-sensitive online applications such as electronic healthcare platforms (e.g., http://www.patientslikeme.com/) or electronic patient records (e.g., http://www.healthvault.com/).

Understanding whether, why and how people use individual privacy settings might be one of the most complex questions on individuals' privacy protection behaviour to date. It covers questions on individuals' general attitudes towards privacy, their awareness of potential threats, their motivation to use the SNS, the composition and relation to different parts of their personal network of friends as well as the specific context in which given data shall be disclosed. These questions are all worth answering since an increasing amount of data on SNS is shared exclusively in individuals' network of friends. For SNS, an indicator of the growing importance of individual privacy settings is the permanent evolution of privacy protection controls at the world's largest SNS 'Facebook'. Consequently, this study investigated SNS members' rationales to use individual privacy settings as a means to control the distribution of data within their personal network of friends. Some of the components of the conceptual model have already been discussed individually and in a more general context in related work. However, the interrelation of categories, their properties and dimensions as well as the particular focus on individual privacy settings, constitute our novel theoretical contribution to research in this domain. While acknowledging the limitations of our approach, we would not have been able to produce this innovative, substantial insight without applying grounded theory techniques. Our model is intended to allow researchers to develop propositions for investigating privacy protection strategies.

We encourage others to comment on and challenge our insights. Consequently, we encourage further qualitative and quantitative work in this domain.

## References


Acquisti, A. and Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. IEEE Security and Privacy, Vol. 3, No. 1. pp. 26-33.

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

Adu-Oppong, F., Gardiner, C., Kapadia, A. and Tsang, P. (2008) Social Circles: Tackling Privacy in Social Networks. Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, USA.

Beer, D. (2008). Social network(ing) sites… revisiting the story so far: A response to danah boyd & Nicole Ellison. In 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.

Bonneau, J., 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 (WEIS 2009) (June 2009), pp. 121-167.

Boyd, D. and Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. In Journal of Computer-Mediated Communication, Vol. 13, No. 1., pp. 210-230.

Boyd, D. and Hargittai, E. (2010) Facebook privacy settings: Who cares? In First Monday, Vol. 15, No. 8.

Braunstein, A., Granka, L. and Staddon, J. (2011). Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It. Syposium on Usable Privacy and Security (SOUPS) 2011, Pittsburgh, PA USA.

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

eMarketer.com (2011). Social Network Ad Revenues to Reach $10 Billion Worldwide in 2013. http://www.emarketer.com/PressRelease.aspx?R=1008629, accessed on 2011-11-27.

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, pp. 211-220.

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80.

Guest, G., Bunce, A. and Johnson, L. (2006). How Many Interviews Are Enough? Field Methods, Vol. 18, No. 1., pp. 59-82.

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

Hawn, C. (2009). Take Two Aspirin And Tweet Me In The Morning: How Twitter, Facebook, And Other Social Media Are Reshaping Health Care. Health Affairs, 28 (2), pp. 361-368.

HowManyAreThere.net (2011). How Many Social Networking Websites Are There? http://howmanyarethere.net/how-many-social-networking-websites-are-there/, accessed on 2011-11-27.

Ledbetter, A., Mazer, J., DeGroot, J., Meyer, K., Mao, Y. and Swafford, B. (2011). Attitudes Toward Online Social Connection and Self-Disclosure as Predictors of Facebook Communication and Relational Closeness. Communication Research 38 (I), pp. 27-53.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10 (3), pp. 393-411.

Nordberg, P., Horne, D. R. and Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure and Intentions versus Behaviors. The Journal of Consumer Affairs, Vol. 41, No. 1, pp. 100-126.

Owyang, J. (2008). Social Networks Site Usage: Visitors, Members, Page Views, and Engagement by the Numbers in 2008. http://www.web-strategist.com/blog/2008/11/19/social-networks-site-usage-visitors-members-page-views-and-engagement-by-the-numbers-in-2008/, accessed on 2011-11-27.

Owyang, J. (2009). A Collection of Social Network Stats for 2009. http://www.web-strategist.com/blog/2009/01/11/a-collection-of-soical-network-stats-for-2009/, accessed on 2011-11-27.

Owyang, J. (2010). A Collection of Social Network Stats for 2010. http://www.web-strategist.com/blog/2010/01/19/a-collection-of-social-network-stats-for-2010/, accessed on 2011-11-27.

Posey, C., Lowry, P., Roberts, T. and Ellis, T. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. EJIS.

Preece, J. (2000). Online Communities. Designing Usability, Supporting Sociability. John Wiley & Sons, Chichester et al., UK.

Preece, J. (2001). Sociability and usability in online communities: determining and measuring success. Behaviour & Information Technology, 20 (5), pp. 347-356.

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

Rheingold, H. (1993). The Virtual Community: Finding Connection in a Computerized World. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA.

Rosenblum, D. (2007). What Anyone Can Know: The Privacy Risks of Social Networking Sites. IEEE Security and Privacy, Vol. 5, No. 3. (2007), pp. 40-49.

Schielein, T., Schmid, R., Dobmeier, M. and Spiessl, H. (2008). Self-help from the cyberspace?--An analysis of self-help forums for patients with bipolar affective disorders. Psychiatrische Praxis, 35 (1), pp. 28.

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

Solove, D.J. (2008). Understanding Privacy. Cambridge, MA: Harvard University Press.

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 (April 2010), 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 (MCP), Volume 6, Number 1, pp. 81-102.

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.

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.

Vossen, G. and Hagemann, S. (2007). Unleashing Web 2.0: From Concepts to Creativity. Morgan Kaufmann Burlington, MA, USA.

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

Xu, Heng; Dinev, Tamara; Smith, Jeff; and Hart, Paul (2011) "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," Journal of the Association for Information Systems: Vol. 12: Iss. 12, Article 1.

Young, A. and Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of Facebook. In C&T '09: Proceedings of the fourth international conference on communities and technologies (June 2009), pp. 265-274.