Friend-to-Friend Privacy Protection on Social Networking Sites: A Grounded Theory Study

André Deuker
Goethe University Frankfurt, Frankfurt, Germany., andre.deuker@m-chair.net

Friend-to-Friend Privacy Protection on Social Networking Sites: A Grounded Theory Study

André Deuker
Goethe University Frankfurt am Main
andre.deuker@m-chair.net

ABSTRACT

Individual privacy settings allow members of Social Networking Sites (SNS) to share personal data with specifically selected contacts, such as close friends. This allows members to use SNS for sharing even more private data they would otherwise not want to share with all of their contacts. Although a considerable part of data sharing activities on SNS is limited to the direct contacts of its members, current research lacks insights on use and design of individual privacy settings. In this paper we investigate driving and inhibiting factors which explain the motivation of SNS members to use individual privacy settings. Thereby, we contribute a new facet to the general understanding of privacy protection behavior on SNS and also lay the ground for improving the design of individual privacy settings offered by SNS providers. We have drawn our results from a conducted grounded theory study based on 37 qualitative interviews with Facebook users.

Keywords

Social Networking Sites, Privacy Protection Behavior, Privacy Protection Strategies, Privacy Settings.

INTRODUCTION

Social Networking Sites (SNS; Beer, 2008) attract a large number of individuals, covering an ever-broadening spectrum of society. These online communities allow their members to meet, to articulate their social networks, to communicate, to share personal data and to refer to data from other Internet sources. After more than 15 years of growth and technical development (Boyd and Ellison, 2007), SNS have become an important part of many individuals' daily lives and thus of society as a whole (Qualman, 2011). Along with this increase in the overall importance of SNS, there is a growing interest in users' privacy protection behavior (Acquisti and Gross, 2006; Utz and Kramer, 2009), on the composition of members' networks of contacts (Gilbert and Karahalios 2009; Hangal, MacLean, Lam, and Heer, 2010), and the related adaption of individuals' offline behavior to SNS platforms (Boyd and Hargittai, 2010; Goffman, 1959; Wellman and Wortley, 1990). Here, an emerging field of research constitutes the friend-to-friend privacy protection field, e.g. research on the usage of individual privacy settings (Houghton and Joinson, 2010).

We define *individual privacy settings* as those privacy settings that enable SNS members to share specific personal data and activities with selected parts of their network of contacts. For example, a private photo can be shared with some contacts while it is hidden from others. On Facebook, access rights can be granted to individual friends, by setting up closed groups or by using self- or pre-defined lists of friends. Although individual privacy settings are constantly improved (Bonneau and Preibusch, 2009), research on the usage of privacy settings in general and individual privacy settings in particular is scarce (Pavlou, 2011). Distinct knowledge about the application of individual privacy settings would help SNS providers, policy- and decision-makers who need to understand and address the increasing demand for information privacy on SNS. Consequently our research question is: *What drives members to use individual privacy settings on SNS?*

In order to address this research question, we chose an exploratory research approach, following the Grounded Theory Methodology (GTM). Evidence from literature (Acquisti and Grossklargs, 2005; Acquisti and Gross, 2006; Utz and Kramer, 2009) and personal experience of the authors indicate that motives of individuals to disclose personal data are manifold and complex. Without the need for pre-defined hypotheses, the GTM approach allows us to consider aspects that have not or only to some degree been considered in previous literature. In this study, we focus on Facebook as the world's largest and most popular SNS.

The remainder of this paper is structured as follows. In the next section, we provide the theoretical background and the related work of our study. Following this, we describe our research methodology and we report and discuss our findings as well as their implications. Finally, we conclude this paper and give an outlook on further research.

THEORETICAL BACKGROUND AND RELATED WORK

Information privacy on SNS has become an increasingly important issue not just because of the growing number of users and the amount of personal data shared. Amplifying factors are “real names” initiatives of many SNS (Boyd, 2011), related questions on profile linkability (Zafarani and Liu, 2009), the integration of third-party services in SNS (Krishnamurthy and Wills, 2009) and social plugins for browsers and websites (Fletcher, 2010).

A multitude of researchers have been addressing several SNS-related privacy aspects so far (Pavlou, 2011). For example, Nordberg, Horne and Horne (2007) describe a dichotomy between individuals’ attitudes towards privacy and their actual behavior. Acquisti and Grossklargs (2005) point to the willingness of many individuals to trade privacy for convenience, which also applies to SNS (Acquisti and Gross, 2006). Risks related to the participation on SNS have been elaborated, among them threats of identity fraud, identity theft, being stalked or being under surveillance (Gross and Acquisti, 2005). Besides a lack of awareness, motives of narcissism and impression management can trigger members’ acceptance of these risks (Utz and Kramer, 2009).

In this study, we focus on a special aspect of privacy, the privacy protection towards connected contacts (‘friends’ in the terminology of Facebook). This is motivated by the fact that a considerable amount of SNS interaction takes place exclusively within the boundaries of members’ personal network of contacts. 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 show that users restrict access to their personal data and activities solely to their network of friends.

Based on this related work, the paper in hand aims to contribute to the current lack of knowledge on how members of SNS protect their privacy towards a non-anonymous audience on SNS.

RESEARCH METHODOLOGY

In this paper, we investigate the role of individual privacy settings as a means for privacy-enhancing behavior on SNS. Thereby we add a new facet to the general understanding of members’ privacy protection behavior and to the use of privacy controls in general (Boyd and Hargittai, 2010; Houghtona and Joinsona, 2010). While we acknowledge the existing work, we aim for a deeper understanding of that matter. We want to uncover individuals’ inner experiences and motivations leading to the usage of individual privacy settings on SNS. To do so, our data collection and data analysis is based upon the GTM (Corbin and Strauss, 2008).

Data Collection

Facebook and its members have been chosen as the subject of our study because of (i) its large number of users (Fletcher, 2010), (ii) its economic importance in comparison to other SNS (eMarketer.com, 2011), (iii) its socio-economic impact on society (Qualman, 2011) and particularly (iv) its large variety of data sharing functionality and privacy control mechanisms (Bonneau and Preibusch, 2009; also documented on http://blog.facebook.com/). We conducted 37 semi-structured interviews with Facebook members in three rounds between March and June 2011. As we strive for analytical generalizability, our sample selection strategy was open and based on random sampling. 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 Facebook experience between a few days and five years and networks of friends on Facebook ranging from 11 to 1,581 contacts.

In order to avoid a bias in replies to privacy related questions (Braunstein, Granka and Staddon, 2011), our first slice of data was collected using anonymous Facebook channels on the Internet Relay Chat (http://www.irc.org/). This first slice of data comprised 13 personal chat protocols, summing up 46 pages of text. We used this data as a valid analytical benchmark for subsequent face-to-face interviews. The second and third data slices comprised eight and 16 semi-structured face-to-face interviews with Facebook users. On average, each of the face-to-face interviews lasted about 30 minutes. Each interview 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, Bunce and Johnson, 2006).

Data Analysis

Data collection and analysis were conducted in parallel. Intermediary results were analyzed and discussed already in between the three rounds of interviews. The collected insights were compared to already existing insights to spot and explain potential contradictions and to extend the interview guide accordingly. Following this cycle of constant comparison (Corbin and

Strauss, 2008) allowed us to obtain a consistent understanding about factors driving or inhibiting the usage of individual privacy settings on SNS. The process of data analysis is clustered in two parts. First, in the process of open coding, we identified concepts that explain or generally influence the usage of individual privacy settings. This included a process of abstraction where we identified a few concepts as core categories and other concepts as properties of categories. In the second step (axial coding), we clustered the categories in categories with a positive influence on the usage of individual privacy settings (drivers), categories with a negative influence on the usage of individual privacy settings (inhibitors), and contextual factors.

STUDY FINDINGS: DRIVERS AND INHIBITORS FOR USING INDIVIDUAL PRIVACY SETTINGS

In this section, we present driving and inhibiting motives of SNS members for the usage of the individual privacy settings. Those categories explaining motives for using individual privacy settings (drivers) are marked with (+), whereas categories describing motives for not using individual privacy settings (inhibitors) are marked with (-).

(+) Follow real life communication patterns: In the offline world, terms like “friend” and “networks of friends” describe social roles and define relationships between people (Wellman and Wortley, 1990). In Facebook, the term “friend” implies that there is a mutually confirmed connection between two individuals. In relation to that, our analyzed data confirms what had already been indicated by literature (Gilbert and Karahalios, 2009; Hangal et al., 2010) – most networks of friends in Facebook are composed of contacts in different relation to the individual: *“Not all of my Facebook friends are friends in reality. There are also colleagues, family members or people that I have met no more than once in my life”* (Interviewee Paul[1]). In the offline world many individuals would treat each contact in a differentiated manner (Wellman and Wortley, 1990). We identified three strategies describing how network members transfer this behavior to the Facebook platform:

- By limiting what personal data to disclose: *“I’m limiting what I put in there. It’s too complicated to define who can see what.”* (Interviewee Bernard).
- By limiting whom to accept in their network: *“In fact my network of friends only consists of friends. For colleagues and so on I’m using a different network.”* (Interviewee Fabian).
- By limiting distribution of personal data: “*In Facebook I share nearly everything with my best friends, like in real life. However, other Facebook friends like colleagues or 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.”* (Interviewee Adele).

Individual privacy settings allow members to combine contacts with whom they have different social relations in their network of friends without the need to reduce their level of activity. Individual privacy settings are used by members who intend to follow communication patterns of the real world, that is, to take and act accordingly to different roles members have in their everyday life (Goffmann, 1959).

(+) Protect against misuse: A key motivation of privacy protection is to avoid misuse or unintended use of disclosed information. Most interviewees mentioned that they consider the SNS provider Facebook and people who are not part of their network of friends as main origins for threats of misuse or unintended use: *“I think people I’ve added or accepted as friends are trustworthy. They won’t misuse my data. I’m afraid that people I’m not connected to could misuse my data.”* (Interviewee Hans). However, some interviewees also reported that they have experienced negative situations caused by friends who misused the data they had disclosed: *“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.”* (Interviewee Dorotha). Compared to typical threats of misuse originating from the SNS provider (e. g. personal data is sold) or to unknown people outside the network of friends (e. g. human resources agent who uses this data in a job interview), consequences of misuse or unintended use by friends are closer and more immediate.

***(+) Prevent misinterpretation*: ** Whereas only some of our interviewees stated being afraid that their shared personal data could be misused by some of their friends, more than two-thirds of the asked respondents stated that they were afraid their data could wrongly be interpreted and thus creating a false image of themselves. *“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). We identified two components, which the interviewees consider to be responsible for potentially wrong interpretations of their shared personal data:

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

- Incomplete data, representing snapshots of members' lives: *"The party photos I posted there represent just a small part of my life. However, as most of my photos in Facebook are party photos one could assume partying is a major part of my life."* (Interviewee Steve).
- Misleading data (e. g., 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).

Compared to the motive for protection against misuse, preventing misinterpretation seems to be a more important reason why members use individual privacy settings. The motive has been mentioned also by interviewees who share personal data only on an occasional basis.

(+) Keep others interested: A few interviewees reported using individual privacy settings to prevent spamming friends, who might not be interested in their postings: *"Nobody is interested in everything. I try to post messages only to those friends who I think are interested or affected by it."* (Interviewee Eleni). Although the level of active contribution varies across our interviewees, every interviewee uses the social network, especially the Facebook Newsfeed, as means to stay informed or to be up-to-date: *"Reading the newsfeed is like reading a newspaper, it keeps me up-to-date and many things I forget immediately..."* (Interviewee Ralph). In addition, each interviewee stated he or she could identify content he or she is more interested in than in others. We noted that members distinguish between two types of content:

- Informational Content (links, pictures, videos, music): Members distinguish content based on whether they are interested in the topic of the posted content, independent from whom of their friends posted the content: *"I am interested in soccer. If someone has posted an interesting link or a video then I'll have a look at it"*. (Interviewee Zara).
- Social Content (status updates, profile updates, comments, private photos): Content is considered to be more interesting if members can identify a connection to their personal life or if unusual, non-daily things are reported*: "A friend of mine posted that he went to the cinema at the weekend. When I talked to him a few days later we talked about the movie. Most people in my Facebook network I meet only a few times a year, in their case I would only be interested if they experienced something extraordinary at the weekend."*(Interviewee Neal).

Our collected empirical data indicates that the schema outlined above may represent only the tip of an even more complex decision-making schema on how people judge the attractiveness of SNS content.

(-) Avoid effort: The configuration of individual privacy settings requires time and effort. We identified three dimensions of effort, which SNS members have to take into account in order to apply individual privacy settings properly:

- Effort to get an initial understanding of how (individual) privacy settings work: *"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."* (Interviewee Wendy).
- Effort to configure individual privacy settings: *"I like this function but I'm not using it, I'm just too lazy. I don't add people I don't like."* (Interviewee Garry).
- Effort to pay attention and react on potential changes in privacy setting functionality: *"[...] 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).

Most interviewees use individual privacy settings at least occasionally, if they want to hide a specific content from certain friends or if they want to grant access to a specific content (e. g. a photo) to only a few friends. Less than half of the respondents use self-defined lists of friends to assign individual access rights. When asked about why they have not created lists of friends, "required effort" has been one of the first mentioned reasons.

(-) Save social capital: Individual privacy settings allow following real life communication patterns by treating different friends differently. One facet of this is to separate groups of friends from each other that have no connection in real life as well: *"Apart from some intersections, most of the groups I've formed don't know one another. For each group I appear differently… in the sports club I behave differently than at work. I don't want these two appearances to merge."* (Interviewee Quentin). In social network theory, these different groups are termed as small world networks (Watts, 2003). For example, probably most of the members of the sports club are connected to one another (small world network 1) or probably most of the work colleagues are connected to one another (small world network 2). But sport club members and colleagues are only connected to one another via one "weak tie" (Granovetter, 1973) – Interviewee Quentin. Against this background, we noticed that people use individual privacy settings to distinguish small world networks in their network of friends, but they hesitate to use individual privacy settings to distinguish between friends, who are part of the same small world network: *"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). Here, a notable difference between privacy protection in real world scenarios and online privacy protection occurs: *"In the real life this is a tacit decision, on Facebook I have to pigeonhole my friends and I don't want them to see this."* (Interviewee Neal). Especially within small world networks, the usage of individual privacy settings thus bears the risk of destroying accumulated social capital.

(-) Issues of missing trust in SNS provider: Facebook provides a technical platform for social interaction. Each activity on this platform and associated services could be traced, stored and analyzed by Facebook. Although most users seem to accept this fact, some interviewees have reported to react on this by reducing their level of activity. Their dominant privacy protection strategy is to limit disclosure towards Facebook: *"I've many friends who don't trust Facebook. They don't use individual privacy settings not because they don't consider them useful, but because they don't disclose anything they would have to protect."* (Interviewee Oliver). We noticed this position in different notions. One interviewee reported disclosing only the minimal amount of information required to get registered in order to be able to only consume information passively. Others reported limiting their level of active contribution because they do not trust Facebook, although in principle they would like to use it more intensely. This category demonstrates that a minimum level of activity by members is necessary before the use of (individual) privacy settings becomes meaningful.

(-) Issues of privacy setting reliability: Another motive for not using individual privacy settings is because respondents distrust the reliability of privacy setting functionalities. We identified two dimensions of reliability:

- Reliability that privacy settings are not changed unexpectedly: *"I don't use these privacy settings because they change these settings so often. I limit what I put on Facebook."* (Interviewee Ian).
- Reliability that privacy settings work in the way members expect them to work: "*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).

Members entrust content and personal data to the platform under the assumption that this is protected by the provided privacy protection mechanisms. Doubts in the reliability of privacy protection functionalities and users' self-doubt to apply them correctly will limit the amount of personal data people share on the platform.

(+/-) Individual context of SNS usage: On an individual level, we noticed that members who actively contribute to the SNS consider drivers and inhibitors to be more important than members with a focus on passive consumption. In addition, members with larger networks of contacts composed of several small world networks tend to consider drivers and inhibitors to be more important than members with small contact networks composed of few small world networks.

DISCUSSION AND IMPLICATIONS

Drivers, inhibitors and individuals' context of SNS usage shape a preliminary causal model of factors determining or generally influencing the usage of individual privacy settings. Figure 1 summarizes these findings and provides a first tentative conceptual model.

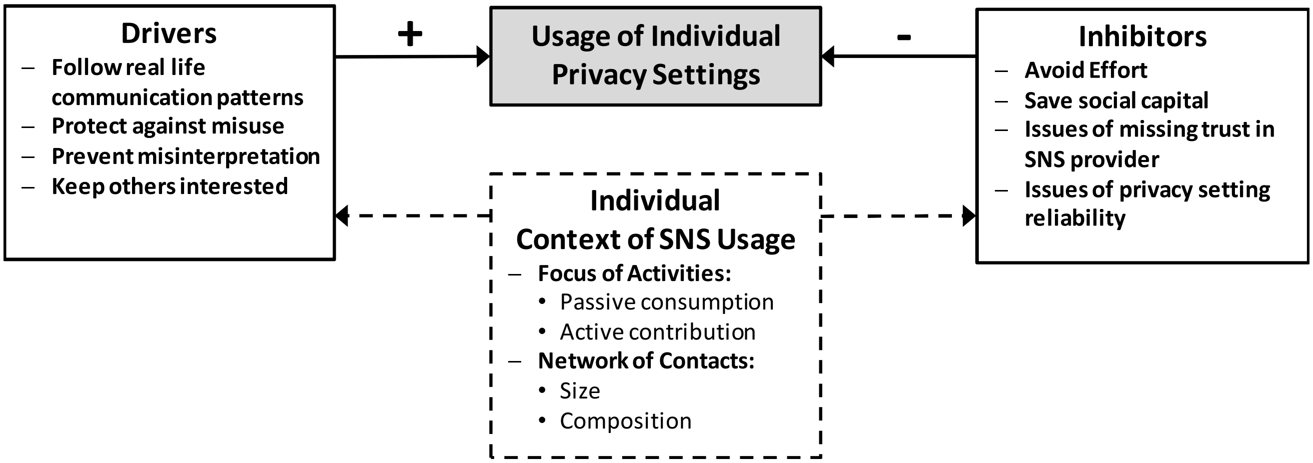
Drivers
– Follow real life communication patterns
– Protect against misuse
– Prevent misinterpretation
– Keep others interested
+
Usage of Individual Privacy Settings
-
Inhibitors
– Avoid Effort
– Save social capital
– Issues of missing trust in SNS provider
– Issues of privacy setting reliability
Individual Context of SNS Usage
– Focus of Activities:
• Passive consumption
• Active contribution
– Network of Contacts:
• Size
• Composition

Figure 1. Preliminary Causal Model of the Usage of Individual Privacy Settings

A few interviewees do not use individual privacy settings because of their intent to share their personal data (general image, ideas, views or opinions) with the greatest possible audience. However, most of the interviewees stated that, at a certain level of activity and disclosure, the possibility of following and establishing real-life communication patterns via SNS is indispensable. Many of those who do not use individual privacy settings reported that they would like to use Facebook more intensively only if their concerns about the usage of individual privacy settings are resolved or alleviated.

Overcoming the inhibiting factors requires the SNS to provide the same means that people apply to their privacy protection behavior in the offline world. Aside from the mentioned issues on the trustworthiness of the platform provider, many of the elaborated inhibitors point to design issues of privacy controls for privacy protection in a non-anonymous online space like Facebook. For example, the inhibitor "Save social capital" can be addressed by blurring whether a part of the profile is actually hidden or whether a friend has not filled in this part of the profile. The identified drivers for the usage of individual privacy settings provide indications on how to support users in configuring their privacy settings, for example, to reduce their configuration effort.

Although we claim that our main results can be generalized, the actual importance of different drivers or inhibitors might vary depending on the sample selection. Our informants are mainly from Western countries and as indicated, most of them who use individual privacy settings do so in order to prevent misinterpretation, whereas only some of them use it as a means to protect against misuse and unintended use. This situation might be different in countries that do not have the guarantee of freedom of speech. Other factors such as users' characteristics and goals, skills, power or culture may also play key roles in causal explanations. In the first instance, the results apply to Facebook. However, at the given level of abstraction we claim that the general results are also applicable to other SNS as well. This claim can be supported by the statements of many interviewees who reported to behave similarly on other SNS they use.

The findings provide an empirical and theoretical baseline for improving existing privacy controls. Moreover, the provided insights may help researchers, policy- and decision-makers to better understand how individuals extend their presentation of themselves in their everyday life in a non-anonymous online space. Social plugins for e-mail browsers, social recommendation systems or even more privacy sensitive online services such as electronic healthcare platforms (e. g. http://www.patientslikeme.com) and electronic patient records (e. g. http://healthvault.com) are further areas to which the provided insights might be applicable.

CONCLUSION AND OUTLOOK

The motivations of members to use (or not use) individual privacy settings are complex and manifold. They comprise questions of general attitudes towards privacy, towards the platform provider but also towards members' own network of contacts. These questions are all worth answering since an increasing amount of personal data on SNS is mainly shared exclusively within the boundaries of members' network of contacts. Overcoming the inhibiting factors would allow for a more personal use, which promises to increase the overall network activity. While acknowledging the limitations of our approach, we would not have been able to produce this substantial, innovative insight without applying grounded theory techniques. Our model aims to provide a first theoretical baseline for 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 constructs, propositions, testable hypotheses or design guidelines. Consequently, we encourage further qualitative and quantitative work in this domain, to challenge and to comment on our insights.

REFERENCES

1. Acquisti, A. and Grossklags, J. (2005) Privacy and Rationality in Individual Decision Making, *IEEE Security and Privacy*, 3, 1, 26-33.
2. Acquisti, A. and Gross, R. (2006) Imagined communities: awareness, information sharing and privacy protection on the Facebook, *Privacy Enhancing Technologies*, 4258, 36-58.
3. 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, 516-529.
4. Bonneau, J. and Preibusch, S. (2009) The Privacy Jungle: On the Market for Data Protection in Social Networks, *Proceedings of The Eighth Workshop on the Economics of Information Security*, London, 121-167.
5. Boyd, D. and Ellison, N. (2007) Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication*, 13, 1, 210-230.
6. Boyd, D. and Hargittai, E. (2010) Facebook privacy settings: Who cares? *First Monday*, 15, 8.

7. Boyd, D. (2011) "Real Names" Policies Are an Abuse of Power, Blog post, available at http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html, accessed on 2012-02-23.
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)*, Pittsburgh, PA, USA.
9. Corbin, J. and Strauss, A. (2008) Basics of Qualitative Research 3e - Techniques and Procedures for Developing Grounded Theory, Sage Publications, London.
10. 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.
11. Fletcher, D. (2010) Friends Without Borders. Time Magazine. Issue on "Facebook… and how it's redefining privacy, May 31, 2010.
12. Gilbert, E. and Karahalios, K. (2009) Predicting tie strength with social media, *Proceedings of the 27th international conference on Human factors in computing systems*, 211-220.
13. Goffman, E. (1959) The presentation of self in everyday life, Doubleday, New York.
14. Granovetter, M.N. (1973) The strength of weak ties, *The American Journal of Sociology*, 78, 6, 1360-1380.
15. Gross, R. and Acquisti, A. (2005) Information revelation and privacy in online social networks, *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71-80.
16. Guest, G., Bunce, A. and Johnson, L. (2006) How Many Interviews Are Enough? *Field Methods*, 18, 1, 59-82.
17. 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*, Washington D.C., USA.
18. Houghton, D. and Joinson, A. (2010) Privacy, Social Network Sites, and Social Relations, *Journal of Technology in Human Services*, 28, 1-2, 74-94.
19. Krishnamurthy, B. and Wills, E. (2009) Privacy Diffusion on the Web: A Longitudinal Perspective, *Proceedings of the 18th international conference on World Wide Web*, Madrid, Spain.
20. 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*, 41, 1, 100-126.
21. Pavlou, P. (2011) State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, 35, 4, 977-988.
22. Qualman, E. (2011) Socialnomics - How social media transforms the way we live and do business, revised and updated. John Wiley & Sons, New Jersey.
23. 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, 81-102.
24. 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.
25. Watts, D. J. (2003) Six Degrees: The Science of a Connected Age, W. W. Norton & Co, New York.
26. Wellman, B. and Wortley, S. (1990) Different Strokes from Different Folks: Community Ties and Social Support, *American Journal of Sociology*, 96, 3, 558-588.
27. Young, A. and Quan-Haase, A. (2009) Information revelation and internet privacy concerns on social network sites: a case study of Facebook, *Proceedings of the fourth international conference on communities and technologies*, 265-274.
28. Zafarani R. and Liu, H. (2009) Connecting corresponding identities across communities, *Proceedings of the 3rd International Conference on Weblogs and Social Media*, ICWSM.