Improving Privacy Settings for Facebook by Using Interpersonal Distance as Criterion

Michaela Kauer
Technische Universität Darmstadt
– Institute of Ergonomics
Petersenstr. 30
64287 Darmstadt, Germany
kauer@iad.tu-darmstadt.de

Benjamin Franz
Technische Universität Darmstadt
– Institute of Ergonomics
Petersenstr. 30
64287 Darmstadt, Germany
b.franz@iad.tu-darmstadt.de

Thomas Pfeiffer
Center of Advanced Security
Research Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany
thomas.pfeiffer@cased.de

Martin Heine
Technische Universität Darmstadt
Petersenstr. 30
64287 Darmstadt, Germany
martin-heine@gmx.de

Delphine Christin
Center of Advanced Security
Research Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany
delphine.christin@seemoo.tu-
darmstadt.de

Abstract

The possibility to define custom privacy settings in Facebook has been improved over the last years. Still, numerous users do not know how to change those settings or do not use the settings because they are cumbersome to use. Within this paper a new method for defining the privacy settings in online social networks is presented that uses the social distance between users as setting criterion. This approach was tested as a paper prototype in a first user study with 10 participants. Results show that the number of errors was significantly decreased and that the subjective evaluation of the interface was promising.

Author Keywords

Social networks; privacy; user interface

ACM Classification Keywords

H.5.2. User Interfaces: Graphical user interfaces (GUI) and Interaction styles (e.g., commands, menus, forms, direct manipulation).

General Terms

Security

Introduction

Online social networks enable persons to stay in contact with friends, to exchange information with relevant others and to keep themselves informed about the life of others who live far away from them [7, 8]. Usage of social networks include viewing the information of others as well as presenting own information. This disclosure of information is a threat to one's privacy, if users are not able to fully and easily control the sharing of personal information [6]. According to [3, 4] people tend not to use privacy settings at all. This disuse is mainly due to two facts: 1) people often are not aware of the possibilities and 2) current interfaces are perceived to be too cumbersome to use. Even though the privacy settings in online social networks were improved, a high granularity of settings still goes along with high effort of the users. In Facebook, for example, all contacts are added as friends, which makes it hard "to indicate the role or value of the relationship" [1]. Privacy settings can be changed for each person but with respect to the high number of friends in online social networks [3] this is quite cumbersome. Additionally, privacy settings can be changed for lists, but lists are not easily manageable. According to Jones and O'Neill [4] people compose their sub-groups (lists) with regard to six criteria: social circles and cliques, tie strength, temporal episodes, geographical locations, functional roles and organizational boundaries. The sort of information and the amount of information shared varies between those groups. This is mainly due to the fact that the self-presentation is adapted to the group to which information is presented [2]. With the customization of privacy settings for each group it is possible to differentiate the amount of information displayed to single members of the networks. Still, one main

problem remains unsolved: The offline social network of people is dynamic. The dynamics of offline interpersonal relations can be a problem for online social networks, because people group "friends" into lists according to their current relationship. When those relationships change (e.g. a colleague becomes a friend or one loses the sight of a close friend) a status or group change in social networks is seldom the consequence [1]. Due to this static nature it is possible that people remain in a group, even if they are somehow different to the other members of that group (either having closer or looser ties to the user). This causes the problem of inadequate information behavior [8]. Either people receive information that they were not supposed to see (group is closer to user) or people do not receive a piece of information, even if the information would be suitable (person is closer to user). According to Skeels and Grudin [8] this leads to an adjustment of users' posts to suit all of their "friends", with the cost of lower satisfaction with the use of the social network.

Within this paper an approach will be presented which addresses these two major problems (non-usage of privacy settings and static representation of dynamic relationships) by shifting from voluntary usage of privacy settings to mandatory usage and by integrating interpersonal distance into the privacy setting interface. First, the general approach will be explained and the new interface will be presented. Afterwards the results of a user study of the concept will be presented. The paper closes with a discussion of the approach.

General Approach

For the approach presented herein, it is important to distinguish between static information and dynamic

Interface Concepts without groups:
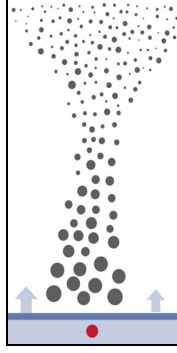
Red dot on left side represents user. Closer friends are displayed closer to the user and have bigger portraits. By now, there are no friends selected, as can be seen by the light blue area that includes only the user.
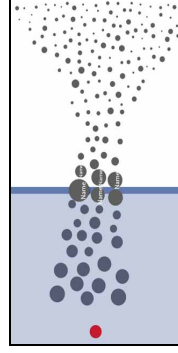
During selection process the blue bar is moved to the right. Friends that are crossed by the bar are enlarged and additional information is displayed (name). The light blue area represents the selection. Friends that are farer away can be moved manually into the selection area.

information in social networks. We define seldom changed information belonging to the profile information (date of birth, gender, name etc.) as static, whereas dynamic information is all kinds of information which users share on a social network (pictures, messages, postings etc.). It is assumed that sharing dynamic information is often a time-critical task, which means that privacy settings are often disregarded. Therefore, fast and easy settings would increase the probability of adequate privacy settings. This can be reached by integrating interpersonal distance into a mandatory user interface for privacy settings. By means of this user interface the user can decide with whom he is going to share after he decided what he is going to share. The interface concept will be presented in the next section.

Interface Concept

The new interface for sharing dynamic content uses the criterion of interpersonal distance to help users define their relevant target group by offering a sorted series of all present friends. From there on a selection of the friends the users intends to share certain content with should be possible with very few clicks.

To evaluate interpersonal distance, two sources are considered: Manual user input and automated algorithms. The arrangement of new ties during the confirmation process of a new "friend", made by the user, gives an initial idea of the tie strength of new connections. If needed, manual input can also be used to express developments of existing ties, although these processes are rather meant to be handled by an automated algorithm. The algorithm is meant to support the user in keeping his/her tie strength up to date by integrating information like number of

messages shared, postings and amount of shared content [e.g. 9]. Up to now, those algorithms were not used to assist users with regard to privacy. We suggest combining an algorithm with our interface to maximize the benefit of both. The combination of manual input and algorithm ensures the suitability of the interfaces for the use in existing online social networks where users already have a number of unsorted social ties.

On the interface the user's profile picture is placed on the far left side, from there on his present ties are arranged on the horizontal axis in order of increasing interpersonal distance. To show the gradation of tie strength the size of the profile pictures decreases and the distance to the user increases the weaker the ties become. Friends can be selected by sliding a bar from left to right. When the bar is moved over a picture, it is magnified and additional information (e.g. name, hometown) is provided. Pictures crossed by the bar become part of the target group and are selected. Sharing content with all ties is simply made by sliding the bar the entire way to the right side. See the side bar for a visualization of the interface.

Additionally, it is possible to select friends independent of their tie strength "out of the crowd". This can be done by manually clicking on single pictures. By moving the cursor over the profile pictures additional information is presented. Simultaneously, surrounding ties are moved slightly away, to create room without hiding people to enable searching and adding people out of the area of weak ties. Besides, it is possible to search for contacts by name.

A finer differentiation is possible by extending the interface with groups/lists (see figure 1). This extension

Criteria for friend selection (40 in total):

- very good friends (8)
- current partner (1)
- friends of the partner that are also friends of the user or contacts the user had not talked to within a year (5)
- Colleagues or fellow students to whom the user has a good relationship (5)
- Colleagues or fellow students to whom the user has almost no contact (5)
- Contacts to whom the user really want to appear serious even if it does not have any disadvantages if not (4)
- Family members (5)
- Remote friends to whom the user has regular contact without private relationship (5)
- former partner (1)
- authority person with relation of dependence (1)

offers two possibilities to share content: 1) Using the overall interpersonal distance by sliding a big bar from side to side, users can select friends independent from the original grouping (e.g. vacation pictures meant to be shared with close friends independent from any groups). 2) Select a predefined group, while taking benefit of interpersonal distance as well (e.g. pictures of the company Christmas party meant to be shared with close friends from work only). Additionally, it is possible to share with a complete group.
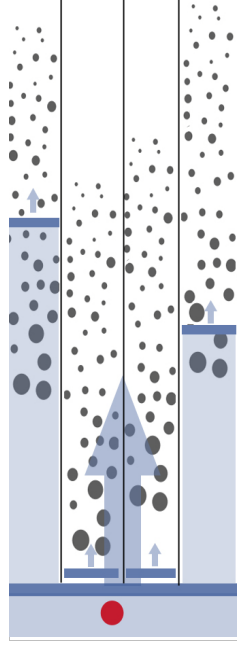

Figure 1. Privacy interface with groups. Bars can be slid to select contacts (dots). Blue area represents selection. Social distance is presented on the abscissa. The ordinate is used to avoid overlaps between contacts.

Method

To test this new approach a user study with a paper prototype was conducted. In the pre-test phase 10 participants (4 female/6 male; aged between 21 and 28 years; number of contacts between 124 and 338; mean number of contacts = 241; all daily users) were asked to select 40 friends according to a number of criteria out of their Facebook friends (see side bar). Afterwards, participants were asked to send the experimenter a PowerPoint file in which all friends were located on a scale to determine their personal distance to the participant (see figure 3 for an example). The experimenter prepared the paper prototype by cutting

out photos of the friends and sticking them on polystyrene. Friends that were closer to the participants had bigger polystyrene blocks than those friends that were not that close to the participant. On the backside of the blocks additional information (e.g. name) was placed. This information became visible (by turning the block), when the friends passed the selection mark.
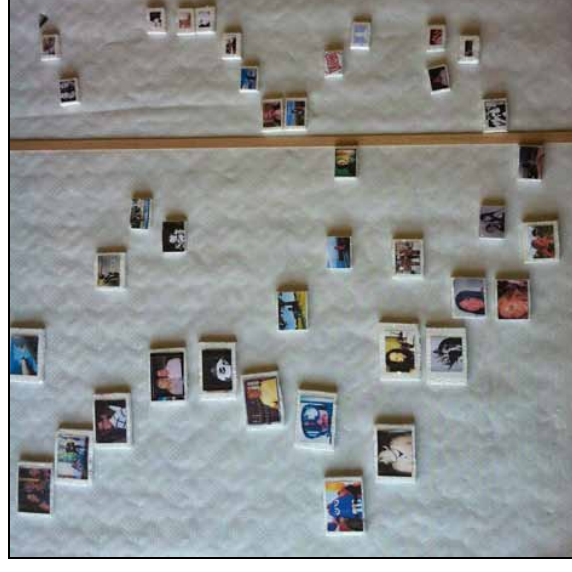

Figure 2. Paper prototype of interface concept.

In the experiment participants were confronted with six tasks they had to solve (e.g. share an embarrassing photo with some close friends or invite to a birthday surprise party). In a first round, participants were asked to solve the tasks by using the regular Facebook privacy settings. After each task the experimenter noted on a list with whom the participant shared the

Tasks

- Invite contacts for the surprise birthday party of your best friend.

- You intentionally missed the Christmas party at your workplace and decided to hang out with friends instead. Post your position on the wall to invite other contacts.

- Share this picture (2x):

- You moved. Share your new address.

- You are on a short trip to London. Post your location.
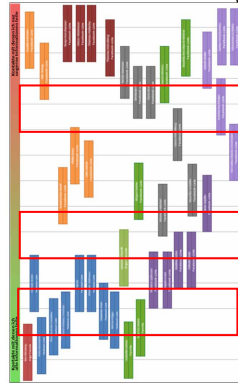
Overlaps in interpersonal distance.

information. Then, the participant was confronted with a list with all contacts on it to decide who should be allowed to see that information and who should not. By comparison of actual shares and intended shares the number of incorrect shares (either unintended sharing or unintended exclusion) for each task was computed. This procedure was repeated for the new interface concept without groups (round 2) and with groups (round 3). In round 2 only two tasks were performed. After the three rounds a semi-structured interview was conducted to collect the participants' subjective evaluation of the interface.
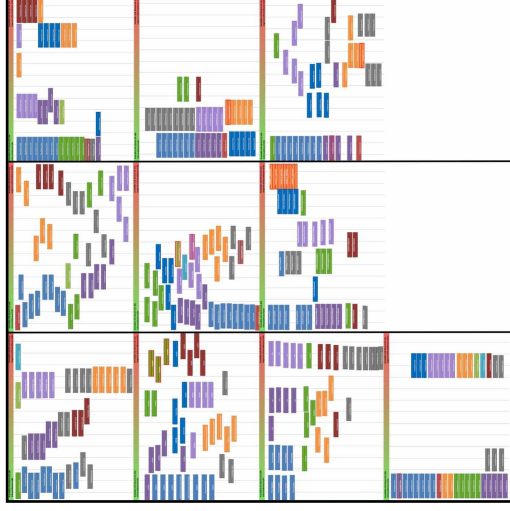

Figure 3. Alignment of the 40 Facebook friends according to interpersonal distance for each participant.

Results

Results from Preparation Phase
A result prior to the user test was the fact that only two out of ten participants stated to use groups/lists to

differentiate between their friends. This is remarkable because the interpersonal distance scales shows big differences in their relationships to the friends (compare figure 3). Additionally, it often seems impossible to form non-overlapping groups/lists based on social distance because there are often friends that would belong to multiple groups which makes the privacy settings even more cumbersome.

Objective results
The main results of this preliminary study is the change in the number of errors between round 1 (using the standard Facebook interface) and round 2 (using the new user interface). First, it is important to note that none of the participants made zero mistakes during all six tasks, neither with the common Facebook interface (between 2 and 86 errors) nor with the new user interface (between 1 and 21 errors). Additionally, the number of intended shares remains almost stable between the two rounds (1348 vs. 1328). Overall, the number of errors decreased with the new interface from 239 to 92. That is a decrease of over 60%. Five participants reduced their errors for involuntary information disclosure (IID; reduction = 52 errors) and involuntary information exclusion (IIE; reduction = 76), two participants reduced either IID/IIE (reduction = 41 errors) and increased the other (increase = 5), one participant increased IID (increase = 1 error) and remained stable for IIE, and 2 participants increased IID (increase = 3 errors) and IIE (increase = 6 errors).

Subjective results
After finishing the entire tasks users were interviewed about the new interface. Users called the interface clearly structured, self-explanatory, and intuitive. Furthermore, some users stated that sharing with the

new interface felt "faster", even if no interaction times were measured. Overall, participants liked the new interface. Still, some participants said that the algorithm for the pre-selection will be critical for the interface's success.

Discussion and Outlook

Within a first user study the new privacy interface was tested with 10 regular Facebook users. It turned out that the interface was rated very high in terms of acceptance and that almost all participants experienced a reduction in errors during the sharing process. Still, those results are preliminary, because the study was conducted with help of a paper prototype and the test rounds between Facebook interface and new interface were not permutated. Therefore, results might be biased. Additionally, interpersonal distance is only one possible criterion that might be used to decide with whom one is going to share information. In real networks family members are also part of the network. Even if it can be assumed that they are personally close to the user, it might be that some sort of information (e.g. party pictures) should not be shared with them. To check this and if the interface is feasible for high numbers of contacts (e.g. what happens if an important contact is "lost in the crowd"?) the new interface will be tested as software prototype with more users in their real social network. Furthermore it is planned to test the interface for different user groups to see if it is equally helpful for regular and occasional users. Those tests will show if privacy settings are important enough for users to spend time on them. By now, it can be said that the interface is a promising approach and that the actual sharing behavior of Google+ users at least partially supports the idea of tie strength as sharing criterion [5].

References

[1] boyd, D. Reflections on Friendster, Trust and Intimacy. Intimate (Ubiquitous) Computing Workshop - Ubicomp, Seattle, Washington, USA, (2003).

[2] DiMicco, J.M. and Millen, D.R. Identity management: multiple presentations of self in facebook. In Proc. of the 2007 international ACM conference on Supporting group work, ACM (2007), 383–386.

[3] Gross, R. and Acquisti, A. Information revelation and privacy in online social networks. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, (2005), 71–80.

[4] Jones, S. and O'Neill, E. Feasibility of structural network clustering for group-based privacy control in social networks. Proc. of the Sixth Symposium on Usable Privacy and Security, ACM (2010), 9:1-9:13.

[5] Kairam, S., Brzozowksi, M., Huffaker, S., & Chi, E. (2012). Talking in Circles: Selective Sharing in Google+. Proc. CHI '12, (pp. 1065-1074). Austin, Texas.

[6] Krishnamurthy, B. and Wills, C.E. Characterizing privacy in online social networks. In Proc. of the first workshop on Online social networks, (2008), 37–42.

[7] Mehdizadeh, S. Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook. Cyberpsychology, Behavior, and Social Networking, 13, 4, 2010.

[8] Skeels, M. M., and Grudin, Jo. When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and LinkedIn. In Proc. ACM GROUP Conference (2009).

[9] Xiang, R., Neville, J. and Rogati, M. Modeling Relationship Strength in Online Social Networks. In Proc. ACM WWW Conference (2010).