Privacy Settings in Online Social Networks - Preferences, Perception, and Reality

Michel Netter, Moritz Riesner, Michael Weber, Günther Pernul
University of Regensburg
{firstname.lastname}@wiwi.uni-regensburg.de

Abstract

To approach privacy threats stemming from interacting with other users on Online Social Networks (OSN), effective Social Identity Management (SIdM) is a key requirement. SIdM refers to the deliberate and targeted disclosure of personal information to a subset of one's contacts on OSN. Yet, unlike the physical world, SIdM on OSN is compromised by unavailable or insufficient settings as well as by properties of mediated communication (e.g. persistence). In this paper, we employ a novel approach based on the participants' Facebook profiles content to study privacy settings in OSN. Our results indicate a mismatch between perceived, preferred, and actual settings that can be reduced to lack of awareness and control by the user.

1. Introduction

Over the last decade, the evolution of the WWW led to a significant growth of Online Social Networks (OSN). While Social Networks have always been an important part of daily life, the advent of easy-to-use services and their ability to bridge spatial and temporal boundaries increasingly shifts social life to their online counterparts. Yet, the rise of OSN has also been accompanied by privacy concerns. While privacy concerns can be directed at a number of stakeholders, such as the site operator, advertisers and third-party applications, this work focuses on privacy threats stemming from other *contacts* on OSN, a threat that has been pointed out by a number of publications [12, 17]. As OSN evolve to multipurpose platforms, where contacts from different social contexts are present [8], the problem of conflicting social spheres emerges [3], i.e. it becomes increasingly difficult to simultaneously meet the expectations of multiple audiences [17].

Similar to the real life, in which people act according to the current context and depending on the people that are present, they require *Social Identity Management* (SIdM) on OSN, referring to the deliberate and targeted disclosure of subsets of their personal attributes to selected online contacts [20], i.e. to be able to present different identity facets to different people and keep those facets consistent [9]. Although the majority of connections between OSN users is based on preexisting relationships of the real world [18, 5], applying the metaphor of a real-life conversation to information disclosure on OSN often leads to misconceptions, for instance, because information is not transient and its audience is greater than intended. As a result, for instance a shared personal photograph can be seen by contacts who were not intended to have access (such as employers or colleagues), indicating a discrepancy between the actual disclosure setting on the OSN and perceived and intended settings.

In this work, we operationalize privacy concerns stemming from interacting with other users on OSN by investigating discrepancies between the user's intended, perceived and actual privacy settings on OSN in a novel way by using a customized questionnaire that is based on a Facebook-Application installed temporarily in the user's profile. This provides the opportunity to inquire the participants' perceived and expected disclosure settings for actual items found in their profile. Further, we gather the items' actual disclosure settings through the application to identify the user's misconceptions and quantify potential mismatches.

2. Related Work

An often-cited definition of OSN and description of their history until 2007 is given in [6]. Several authors have voiced privacy concerns addressing personal information that is disclosed on OSN [10, 2], leading to suggestions for improving privacy settings and their presentation. Various surveys have been conducted on existing privacy controls on OSN in general [4] and for SIdM in particular [22].

The contribution of this paper consists of identifying the perceived, desired and actual disclosure settings of OSN users and the discrepancies between them. The study is based on the assumption that survey respondents' answers regarding perceived and desired settings are more correct when the questions are referring to actual profile-items. Thus, these data points were queried for particular profile items in the participants' OSN

accounts. To the best of our knowledge, no other work has examined all three aspects - perceived, desired and actual settings - on this level of granularity.

There is a large body of work surveying the usage of OSN and their privacy settings in general, such as [5] and [11]. [7] investigates differences between privacy awareness and users' behavior. Also, [13] and [23] analyze factors that predict more restrictive privacy settings by the users. Further, in [1], a possible connection between the users' attitude towards privacy and their actual disclosure settings was investigated by comparing their answers to a questionnaire on the visibility of their profile to the public on Facebook. Unlike our work, their questionnaire did not present actual profile items. Similarly, in [16] the participants' intended disclosure settings for a number of information categories were queried. Then, using a Facebook-application, items of these categories were gathered to assess whether the actual disclosure settings corresponded to the users' intentions. Both [1] and [16] only feature broad disclosure settings and do not consider the disclosure to only a subset of the participants' contacts.

Expected and actual disclosure settings for particular pictures of Facebook-users were surveyed in [15]. Regarding disclosure granularity, when investigating discrepancies between intended and actual settings, their analysis only considers the general setting *some friends*. In contrast, we analyze this discrepancy on the granularity of disclosure to a particular contact. Further, we also consider the type of relationship with the contact.

3. Conceptual Model and Research Questions

Assuming that real-world SIdM strategies are applied to OSN [21], this work investigates possible disparities when doing so by analyzing disclosure settings of items posted to OSN. Note that in the remainder we use the terms *disclosure setting* and *visibility setting* interchangeably. Figure 1 illustrates the conceptual model of our research problem, by displaying three perspectives on the disclosure setting of a particular item of one study participant. An item's disclosure setting governs which entities are eligible to view it and thus specifies its audience. Firstly, we consider the item's *actual disclosure setting*, representing the currently active setting on the OSN. The *perceived disclosure setting* refers to what the participant *believes* the current setting to be, while the *intended disclosure setting* refers to what the setting *should* be in the opinion of the participant. The directed edges in Figure 1 represent possible influences between the three perspectives. In an ideal scenario, the actual disclosure settings are the same as the perceived and intended settings for each item. We expect discrepancies however, which can be explained as follows: Differences between the perceived and actual setting indicate a lack of *awareness* by the user. Further, differences between intended and actual settings indicate a lack of *control*, which can occur either because the intended settings cannot be applied with reasonable effort (if the perceived settings match the actual settings) or because the user does not realize the need for the intended setting to be applied (due to lack of awareness). Likewise, a discrepancy between perceived and intended settings indicates the user's realization that changes to the actual settings need to be made – or, if such a discrepancy persists that the settings cannot be applied with adequate effort. We investigate this potential lack of awareness and control for three different domains on OSN, namely *default information spreading*, *active information sharing*, and *past information availability*.

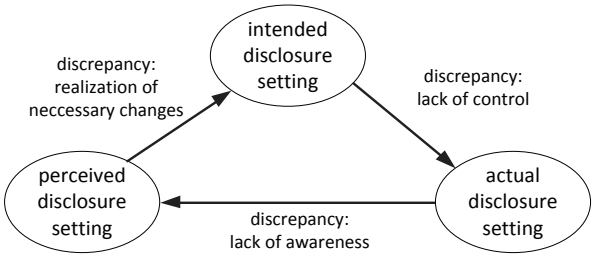

Figure 1. Conceptualization of the research problem

First, we investigate whether *default information spreading* of the physical world equates to the situation in OSN. In the former case, spreading depends on the situation the user is currently in which can easily be understood. For example, the audience is clearly defined when having a private conversation in a restaurant with friends. On typical OSN, default settings are available for different personal data categories to control visibility. If left unchanged, visibility of this information as well as its distribution within the OSN follows the rules as conceived by the OSN service provider. In this domain, we investigate possible misconceptions between the user's perceived, preferred and actual default settings for different data type categories. Particularly, we address the following two research questions:

- **RQ1a:** Are OSN users aware of default settings as set up by the OSN service providers?
- **RQ1b:** Do the users' preferred default settings differ from the actual default settings?

The second domain investigates *active information sharing* on OSN. In real life, sharing is adapted to the social norms of the user's different social contexts and targeted to people currently present. The equivalent on OSN is the access control model which is used for targeted disclosure. In this paper we examine whether OSN users understand the access control model available and are able to use it according to their wishes. In detail, we address the following research questions:

- **RQ2a:** For shared items, do OSN users understand the visibility implications of an OSN access control model?
- **RQ2b:** For shared items, do OSN users' preferred visibility settings differ from the actual visibility setting?

Lastly, we examine the misconceptions regarding *past information availability* on OSN. While information transience is an inherent property of real-life communication, information is persistently stored on OSN to enable asynchronous communication. In this domain we investigate whether the users are aware of permanent storage of information shared on OSN and if this non-transiency is according to their preferences. In detail, we address the following research questions:

- **RQ3a:** Are OSN users aware of the permanent availability of previously shared items?
- **RQ3b:** Do OSN users wish to change the visibility settings of previously shared items?

4. Methodology

This section outlines our method for recruiting participants and subsequently presents the overall study design and the design of each questionnaire in detail.

4.1 Recruiting Methods

Participants were recruited in three ways: through an announcement on the department's website and Facebook page, through an announcement on the institute's bulletin board, and through an e-mail announcement asking for participation. To increase the incentive for participation, two 25 € Amazon gift cards were raffled in a lottery among all participants.

4.2 Study Design

To investigate the research questions presented in Section 3, the study relies on the participants' Facebook profile items. The study was delivered as a Facebook-Application to gain access to the participants' Facebook profiles via the provided API. Figure 2 depicts the course of the study as well as its main components. After arriving at the study's landing page, each participant was redirected to Facebook, asking him to log into his account and grant access to the study application. If successful, the participant was redirected back to the study and asked to provide demographic information and classify a subset of his contacts (cf. Section 4.2.1). The survey itself consists of three custom questionnaires with each of them targeting one of the three domains introduced in Section 3. It is important to note that all data collected was immediately hashed and anonymized: personal items used in the questionnaires were never written to disk as we were only interested in the items' visibility settings. At the end of the study, all information stored was presented to each participant for approval.

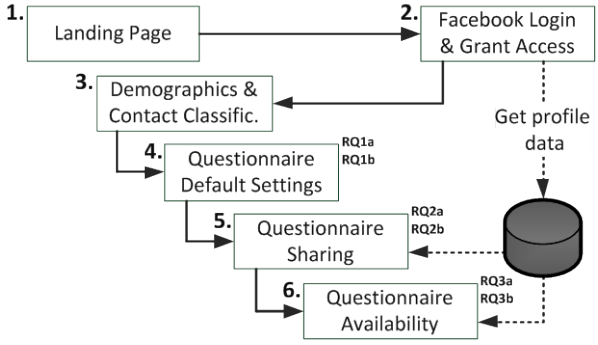

Figure 2. Study design

Despite the possibility to open the study to all Facebook users, we designed our study to required physical attendance of all participants. While the open study approach would have likely increased the number of participants, it might have been subject to intentional misentry and vandalism. The attendance approach allowed us to conduct the survey in a controlled environment and to give advice to the participants where necessary and thereby increase the quality of participant input. The study was conducted at a dedicated room of the department in groups of up to eight participants between December 2011 and April 2012. Minimum requirements were a Facebook account with at least 40 contacts and at least five user-generated items such as status posts or picture uploads.

4.2.1 Preparatory Contact Classification

In order to gain additional knowledge about the type of relationship participants had with some of their contacts, they were asked to classify a subset of their contacts into one of four predefined categories, namely *Close Friends (CF), Close Acquaintances (CA), Loose*

Acquaintances (LA), and *Respected Persons (RP)* (such as parents and other persons of authority). For each category, a description (such as criteria of suitable contacts) was displayed along with a dialog showing a list with names and profile pictures of all of the participant's contacts. The participants were asked to assign five contacts to each of the first three categories and three contacts to the RP category.

4.2.2 Default information spreading

To examine the user's awareness (RQ1a) and preferences (RQ1b) regarding default visibility settings (corresponding to perceived and preferred settings in Figure 1), a custom pie chart like questionnaire was developed (see Figure 3)[1]. It allows a participant to easily express the visibility of different data categories. On Facebook, separate default visibility settings exist for ten different categories, namely: *Contact Info, Name, Wall Posts, Networks, Profile Picture, Likes, Friendlist, Gender, Birthdate, and Other Profile Data*[2]. Each wedge of the pie represents a single personal data type. It has five partitions, representing possible audiences. The audience size increases from the innermost level outwards with the following partitions available: *Me, Friends, Friends-of-Friends (FoF), All Facebook Users,* and *All Internet Users*, whereas the next outer partition is a superset of all inner partitions (e.g. besides all friends of the participant's friends, FoF includes the audiences Me and Friends). Note that subset of friends is not available for default settings, because a newly created Facebook account does not contain any friendlists. The available privacy settings differ between each category. For example, profile picture and name can be accessed from *All Internet Users*, while for instance the loosest privacy setting (which Facebook confusingly labels public) for wall posts solely comprises *All Facebook Users*.

To examine the participants' awareness of default settings, participants were asked for what they thought is the default setting for each category. To indicate their choice, they were asked to click on the partition of the respective wedge representing the intended audience (resulting in a blue-colored background for the given partition and all inner partitions).

We employed the same type of questionnaire to assess the participants' preferred default settings, asking them to express their preferred audiences for each data type. After finishing both questionnaires (targeting our research questions RQ1a and RQ1b), we compared the results to Facebook's actual default visibility settings.

[1]Inspired by: http://www.mattmckeon.com/facebook-privacy/

[2]Other profile data comprises for instance place of birth and family members

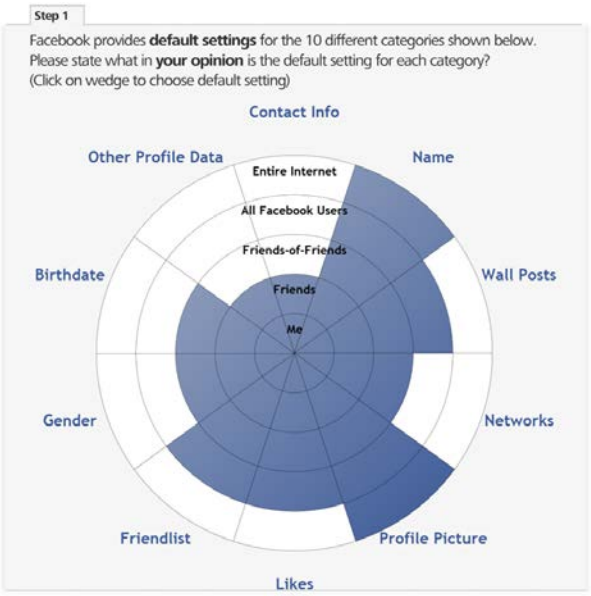

Figure 3. Developed pie chart questionnaire

4.2.3 Active information sharing

To assess the participant's awareness (RQ2a) for the permissions granted to other users regarding shared information and the participant's preferred permissions (RQ2b) for this information, a dynamic questionnaire based on the participants' shared personal items was developed (see Figure 4). The upper part of the questionnaire shows a personal item. Items were chosen from the participants' Facebook profile in the following order and quantity: Three *Wall Pictures*, three *Album Pictures*, two *Mobile Pictures*, two *Status Posts*, and two *Links*. If fewer items were available for a category, additional items from another category were chosen based on the order outlined above. Status posts were required to have a minimal length of 150 characters to contain sufficient information. Pictures account for a large number of items (eight) in this study as previous studies show that they are most likely to contain sensitive, i.e. privacy-relevant information [15], while the remaining items are chosen equally from other categories. The lower part of Figure 4 contains a set of 15 users. The set of users consists of three randomly chosen users from each of the categories of the preclassified contacts (see Section 4.2.1) as well as three randomly chosen strangers. Unlike [15], we opted only for a subset of the participant's contacts because answering the question for all contacts would be too time consuming and might have a negative impact on the quality of the survey results. Also we chose not to provide the participant's existing friendlists as a choice to avoid bias. To assess the participants' awareness, they

were asked to select those contacts that, in their opinion, have access to the shown item. Internally, the input was compared to the actual access rights for this item. The same questionnaire was employed to assess the participants' preferred visibility settings.

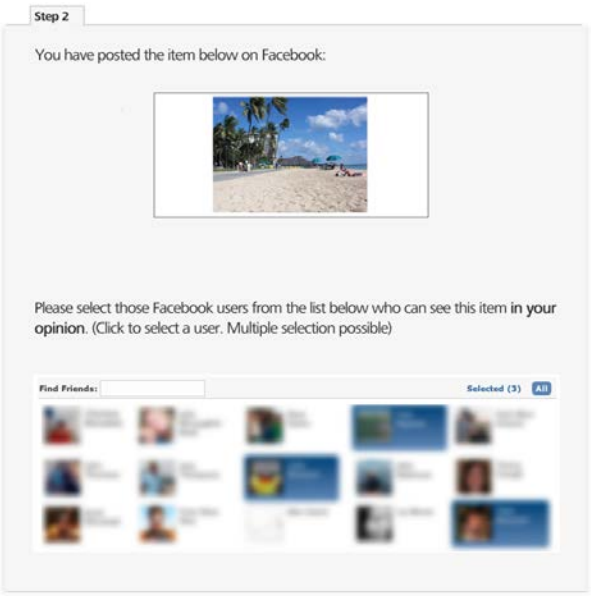

Figure 4. Information sharing questionnaire

4.2.4 Past information availability

In order to investigate the participants' perceived availability (RQ3a) of items they shared previously and to find out their intended visibility settings (RQ3b) of these items, older items (i.e. items shared at least one year ago) were shown to the participants. It can be assumed that people in general know that information shared on OSN is persistently stored. Yet, this analysis examines a potential lack of awareness of permanent availability for *particular* items rather than general awareness of persistence on OSN. A five point Likert scale was used to state the level of surprise with the following options available: *very surprised*, *surprised*, *have no opinion*, *are a little surprise*d, and *not surprised*. If (*very*) *surprised*, the participants were asked to explain whether the surprise was due to absence of memory or due to changes in their personality for instance caused by growing up or changing their self-conception. Subsequently, participants were asked to state whether the item should still be available in the future. As for the previous questionnaire, items were chosen from the participants' profiles in the following order and quantity: Three *Wall Pictures*, three *Album Pictures*, two *Mobile Pictures*, two *Status Posts*, and two *Links*. If fewer items were available for a category, additional items were chosen from other categories if available based on the order outlined above. Otherwise, the questionnaire was executed with fewer items.

5. Results

In this section, we present the results of our study which are publicly available[3]. First, we discuss the participants' demographics and data statistics. Subsequently, we outline the results of the previously proposed research questions.

5.1 Demographics and data statistics

Demographics are presented in Table 1. Of 74 persons taking part in the study, 68 data sets remained after cleansing erroneous or incomplete datasets. Of the 68 participants, females account for 38.24 % which leads to a slight male bias (61.76 %). The participants' age ranges from 18 to 31 years ($\mu = 23.93$; $\sigma = 2.66$). Compared to the age distribution on Facebook[4], we observe an overrepresentation of the early- to mid-twenties group, which can be attributed to the academic context of our study (95.59 % of the participants indicate to have an academic background). The majority of participants (64.71 %) reports to have neither professional- nor academic IT-related training.

Table 1. Participant demographics

Demographic variable	Category	Percent.
Gender	Female	38.24 %
	Male	61.76 %
Age	≤ 20	4.41 %
	21-23	41.18 %
	24-26	41.18 %
	27-29	8.82 %
	≥ 30	4.41 %
Academic Background	yes	95.59 %
	no	4.41 %
IT Background	yes	35.29 %
	no	64.71 %

In total we analyzed 924 items (567 in the active information sharing questionnaire (cf. Section 4.2.3) and 357 in the past information availability questionnaire (cf. Section 4.2.4)) that can be distributed to the following five categories: 540 (58.44 %) status posts, 86 (9.31 %) link posts, 53 (5.74 %) mobile-, 115 (12.45 %) album-, and 130 (14.07 %) wall pictures.

[3] http://www-ifsresearch.wiwi.uni-regensburg.de/paper/HICSS/

[4] http://www.socialbakers.com/facebook-statistics/, retrieved on May 21, 2012

Table 2. Privacy settings per object type (percentages, default settings shaded gray)

	ME	CU	AF	FF	NF	EV
Status Post	0.0	12.2	34.7	2.5	0.2	3.0
Link	0.0	2.8	8.1	0.2	0.0	1.1
Mobile Pic.	0.0	3.0	4.6	0.4	0.2	1.2
Album Pic.	0.0	3.5	8.6	0.7	0.0	1.6
Wall Pic.	0.4	3.0	6.5	0.9	0.0	0.7

ME = Me, CU= Custom subset of friends, AF = All friends, FF = Friends of friends, NF = Networks and friends, EV = Everyone

Considering the participants' actual privacy settings per item type as depicted in Table 2, it is notable that most items were shared with all contacts or a custom list of contacts, while only 7.6 % were shared using the default settings. This differs from a previous study's results, stating that 36 % of items are shared using default settings [15] and might be due to regionally differing privacy attitudes [11] or increased awareness.

5.2 Default Information Spreading

This section discusses possible mismatches between perceived, preferred, and actual *default* visibility settings (cf. Section 3). First, we investigate the participants' *expectations* of default settings (RQ1a).

The results presented in Table 3 suggest that for six out of ten data categories available on Facebook the highest percentage of participants correctly estimated the default visibility settings. This indicates a basic awareness of the default personal information flows on OSN. On average, 22.1 % (± 9.9 %)[5] overestimated the default visibility settings. Overestimation is highest for data categories with restrictive default settings (such as *Contact Info* and *Birthdate*). It is notable that more than a third of the participants (AVG 37.6 % ± 11.5 %) expected the default settings to be more restrictive than the actual settings. However, we are aware that participants' awareness might be distracted due to Facebook's frequent changes of their default settings which should be subject to further investigation.

For seven of ten data categories, a higher percentage of participants underestimated the default visibility settings instead of overestimating them (see TOT BLW and TOT ABV in Table 3). The sign test ($\alpha = 0.05$) confirms a strong significant lower median for participant estimated settings than for default settings, i.e. a significant underestimation, for the five data categories *Name*, *Wall Posts*, *Profile Picture*, *Likes*, and *Other Profile Data*. Furthermore, the sign test also approves a significant overestimation for the data categories *Contact Info*, *Gender*, and *Birthday*.

[5]Subseq., confidence intervals are stated in brackets for $\alpha = 0.05$ %

Table 3. Expected default settings (percentages, default settings shaded gray)

	ME	AF	FF	FB	EV	TOT BLW	TOT ABV
Cont.	27.9	19.1	19.1	23.5	10.3	27.9	52.9
Name	2.9	4.4	7.4	16.2	69.1	30.9	0.0
Wall	1.5	23.5	23.5	39.7	11.8	48.5	11.8
Netw.	8.8	8.8	13.2	52.9	16.2	30.9	16.2
Prof. Pic.	1.5	2.9	5.9	27.9	61.8	38.2	0.0
Likes	2.9	19.1	19.1	39.7	19.1	80.9	0.0
Frien.	4.4	8.8	16.2	50.0	20.6	29.4	20.6
Gend.	2.9	5.9	4.4	41.2	45.6	13.2	45.6
Birth.	1.5	17.7	19.1	41.2	20.6	19.1	61.8
Other	5.9	25.0	26.5	30.9	11.8	57.4	11.8
					AVG	**37.6**	**22.1**

ME = Me, AF = All friends, FF = Friends of friends, NF = Networks and friends, EV = Everyone, TOT BLW = Total below default setting, TOT ABV = Total above default setting

Table 4. Preferred default settings (percentages, default settings shaded gray)

	ME	AF	FF	FB	EV	TOT BLW	TOT ABV
Cont.	36.8	50.0	11.8	1.5	0.0	36.8	13.2
Name	5.9	16.2	20.6	54.4	2.9	97.1	0.0
Wall	4.4	85.3	8.8	1.5	0.0	98.5	0.0
Netw.	13.2	44.1	32.4	10.3	0.0	89.7	0.0
Prof. Pic.	2.9	25.0	35.3	33.8	2.9	97.1	0.0
Likes	10.3	63.2	25.0	0.0	1.5	98.5	0.0
Frien.	13.2	35.3	45.6	5.9	0.0	94.1	0.0
Gend.	13.2	25.0	25.0	27.9	8.8	63.2	8.8
Birth.	14.7	63.2	16.8	5.9	0.0	78.0	5.9
Other	11.8	73.5	11.8	2.9	0.0	97.1	0.0
					AVG	**85.0**	**2.8**

ME = Me, AF = All friends, FF = Friends of friends, NF = Networks and friends, EV = Everyone, TOT BLW = Total below default setting, TOT ABV = Total above default setting

Subsequently, we investigate possible mismatches between actual and *preferred* default settings (RQ1b).

Drawing from the results of Table 4, it can be inferred that OSN users want privacy settings to be more restrictive (on average, 85.0 % (± 8.5 %) prefer more restrictive privacy settings) compared to the actual settings. A standard sign test ($\alpha = 0.05$) confirms for all ten data categories a strong significant preference of more restrictive settings. Nevertheless, it is notable that 54.4% (± 11.8 %) wish that by default, their name should be accessible by all users. Hence, we deduce that while users want more restrictive defaults they also want to be found by other OSN users. Additionally, it is notable that the desire for names to be public interferes with the wish for gender to be comparatively private, as gender can usually be deduced from a name.

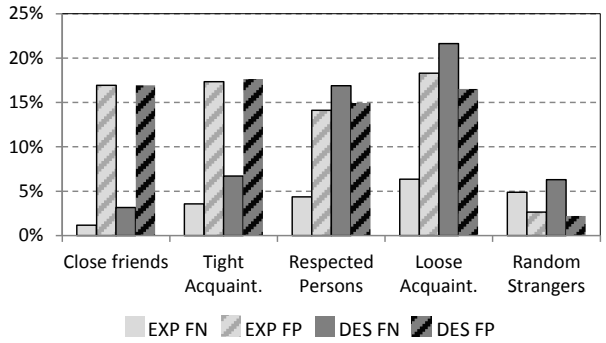

Figure 5. False Positive and False Negative Rate for Expected and Preferred Visibility

5.3 Active Information Sharing

At first, we investigate whether the participants understood the implications of access control settings for their shared items, i.e. whether *expected* and actual visibility settings match (RQ2a).

For 567 objects in total, participants provided their expected visibility setting for each of the 15 contacts displayed, resulting in 8505 visibility decisions. The results show that 82.1 % (± 0.8 %) of all assumed visibility settings match with the actual settings which indicates that OSN users are in general well aware of their privacy settings. It is notable that this value increases to 92.5 % (± 1.8 %) when focusing only on the visibility for complete strangers.

The remaining 17.9 % (± 0.8 %) of all visibility decisions are analyzed in detail, i.e. the cases in which the expected and actual settings do not match. Two types of errors can be distinguished (see Figure 5): A *False Negative* (FN) error occurs if the actual visibility of an item for a given contact is true while the participant assumes that the visibility is false, i.e. the participant underestimates the visibility. Similarly, a *False Positive* (FP) error occurs if the item is not visible for a given contact, while the participant thinks it is, i.e. the participant overestimates the visibility.

First analyzing underestimation (EXP FN), we observe a negative connection to tie strengths. Starting with 1.2 % (± 0.5 %) for the Close Friends category the value increases to 6.4% (± 1.2 %) for *Loose Acquaintances*. From this, we infer that participants are well aware which of their best friends have access to which parts of their profile, while they are less sure about people they rarely interact with. Regarding overestimation (EXP FP) of visibility, it can be seen that overestimation ranges between 14.1 % (± 1.7 %) - 18.3 % (± 1.8 %) for all visibility decisions in all contact categories, except for the *Random Strangers* (2.7 % ± 0.8 %), i.e. participants have no completely well-defined non-visibility awareness for their contacts, yet they are well aware that shared items are not accessible by strangers. Using a standard binominal test, it can be shown that ≥ 45 % of OSN users significantly underestimate the actual visibility settings for at least one of their items.

Subsequently, we investigate possible discrepancies between preferred and actual visibility settings (RQ2b). Similar to the previous research question, we received 8505 preferred visibility decisions that were compared with the actual visibility setting. Preferred and actual visibility setting matched in 75.4 % (± 0.9 %) of all cases. From this fact we deduce that OSN users largely set the visibility of shared items according to their preferences, i.e. they make use of the access control options provided by the OSN.

Analyzing the mismatch between preferred and actual visibility settings (24.6 % ± 0.9 %), we observe that FP errors - the desired setting is less restrictive than the actual setting - range between 14.9 % (± 1.7 %) - 17.6 % (± 1.8 %) for the first four contacts categories while it decreases to 2.2 % (± 0.7 %) for *Random Strangers*. Thus we observe that besides pure privacy considerations there are also several cases in which users actually prefer less restrictive disclosure settings. Hence, misconceptions about an access control model of an OSN do not exclusively relate to information oversharing. However, we add for consideration that - for preserving privacy - instances of preferred looser disclosure settings do not outweigh cases where more restrictive visibility settings are preferred.

Next, we analyze false negative (FN) errors, i.e. the preferred setting is to deny visibility for a given contact while in reality, access is granted. Similar to the previous research question RQ2a, demands for more restrictive settings is negatively connected to tie strength, starting from 3.2 % (± 0.8 %) for *Close Friends* to 21.63 % (± 2.0 %) for *Loose Acquaintances*. From these results we deduce oversharing for contacts that are not in the user's inner circle while settings are more likely to be correct for close friends. A binominal test proves significantly that ≥ 64 % of OSN users wish the actual visibility settings to be more restrictive for at least one of their items.

In summary, comparing the results of RQ2a and RQ2b it is noteworthy, that FN error rates for RQ2b are higher than those of RQ2a, which is interpretable as the wish to further restrict visibility of shared items.

5.4 Past information availability

First, we analyze the users' awareness of the persistence of shared items (RQ3a). The study participants expressed their level of surprise for a total of 357 items. With 86.3 % (± 3.6 %) the majority of items was no or only a little surprise, while 9.8 % (± 3.1 %) led to a surprised reaction (no opinion 3.9 % ± 2.07 %). If

reasons for surprise were stated by the participants, lack of memorization accounted for 68.6 % (± 15.4 %), changes on personality for 28.6 % (± 15.0 %), and both for the rest. Relating to the 68 test participants instead of items, 29.4 % (± 9.6 %) of the participants were (very) surprised about at least one of their items.

Note that the results for surprise should be interpreted as the lower bound. It cannot be ruled out that by showing an item the participant's memory was refreshed leading to lower reported levels of surprise.

Nevertheless, conclusions can be drawn from the results. The majority of OSN items shared at least a year ago are of no surprise for their creators. Still, a binominal test shows significantly that at least every fifth OSN user lacks awareness for the permanent availability of at least one shared item.

Finally, we analyze preferred visibility changes (RQ3b). As can be seen in Table 5, of the total of 357 items, participants prefer 9.5 % (± 3.0 %) to be deleted, 27.2 % (± 4.6 %) to be restricted in their visibility and 63.3 % (± 5.0 %) to be left unchanged. As a result, the users preferred more restrictive visibility settings for 36.7 % (± 5.0 %) of the items. The probability of participants choosing more restrictive visibility settings was 82.9 % (± 12.5 %) for surprising or very surprising items and 32.1 % (± 5.2 %) for non-surprising items.

Considering the different item categories in Table 5 in more detail, it is notable that no participant wanted to delete any album pictures while wishes for deletion were expressed for other categories especially when the participants were surprised. Relating to the 68 test participants instead of items, 57.4 % (± 11.8 %) wanted to limit the visibility of at least one item while 19.1 % (± 9.4 %) even wanted to delete at least one item.

These results suggest that OSN users demand to reduce the visibility of every third item that they shared at least one year ago. A binominal test proves significantly that ≥ 46 % of OSN users would prefer to restrict the visibility of at least one of their items. Therefore, it seems reasonable to suppose that the OSN users demand more aid and support to limit the visibility settings for older items.

6. Research Limitations

One can argue that a number of factors limit making generalizations based on the study results: Our study solely relies on profile data of a single OSN, namely Facebook which we see however as the most representative at this time. The sample of this study was overrepresentative of early- to mid-twenty year old participants. Additional limitations comprise the regional focus of participants, the academic background of the study and self-reported demographics.

Table 5. User awareness of previously shared items and preferred action (percentages)

	Action	Status Posts	Links	Wall Pic.	Abum Pic	all
All Items	Delete	10.7	23.5	6.2	0.0	9.5
	Limit vis.	25.6	11.8	33.8	33.3	27.2
	Keep	63.6	64.7	60.0	66.7	63.3
Surp.	delete	42.3	66.7	50.0	0.0	40.0
	Limit vis.	42.3	0.0	50.0	75.0	42.9
	Keep	15.4	33.3	0.0	25.0	17.1
Not surp.	delete	7.2	7.7	5.1	0.0	6.2
	Limit vis.	24.2	15.4	33.9	27.6	26.0
	Keep	68.6	76.9	61.0	72.4	67.9

Users with less than the required numbers of contacts and profile items were excluded from participation, thus our results are only applicable to Facebook users with a level of activity on the platform that exceeds these criteria. It can be argued that those people fulfilling the requirements to participate might be more active on OSN and familiar with privacy settings than the average user, posing a threat to external validity. Also, the comparably small sample size limits statistical significance, though we argue that by opting for conducting the study in person, we achieved a better quality of responses compared to a remote survey.

As noted in [15], privacy is hard to measure, which we alleviate to a certain extent by comparing and quantifying disclosure settings. Still, putting these measures into statistical terms is not trivial. The audience settings *friends* and *everyone* for instance differ in orders of magnitude and thus cannot be put on a metric scale.

One can argue that compared to conventional surveys, adapting the questionnaire to the participants' Facebook profiles leads to issues of comparability between samples. While we acknowledge for instance that users who are more active on Facebook may be more challenged in managing their disclosure settings, we also assert that such differences would also occur when using a static survey, as such a survey is also dependent on the participants' experiences on OSN. On the level of profile items, we argue that posing questions about real items yields more honest answers than asking about the general attitude towards privacy.

7. Discussion and Implications

In the following, results are discussed based on our conceptualization of perceived, preferred, and actual visibility setting (see Figure 1). First, possible discrepancies between perceived and actual visibility settings are investigated, indicating a lack of user awareness. Regarding default information flows, on the one hand a general awareness of default settings on OSN can be

attested, yet on the other hand minor over- and stronger underestimation tendencies can be observed. Focusing on underestimation, which is statistically significant for five data categories (see Section 5.2), further investigation is required to identify root causes. Similar, our results for active information sharing show that perceived and actual visibility settings match to a large extend, i.e. users are generally well aware of the visibility of shared personal items to other users. Mismatches split to both over- and underestimation, while we significantly showed that almost every other user underestimates the visibility of at least one item. Likewise, regarding awareness of past information availability, participants' perceived and actual visibility settings matched in most cases. Yet, one in five participants significantly underestimates one or more items, which might be attributed to limited mental capacities or to a change in personality but needs to be further investigated in future work.

Second, possible mismatches between preferred and actual visibility settings are discussed, indicating a lack of control (see Figure 1). Targeting default information sharing, our study shows significantly for all data categories that users prefer more restrictive default visibility settings. Regarding shared items, our analysis shows a reasonable matching rate of preferred and actual visibility settings. Yet, it is statistically significant that 64% of users wish to reduce the visibility of at least one item. Regarding the users' preferences of past information availability, results show that the preferred visibility setting is more restrictive than the actual visibility for every third item and that significantly almost every other user wants to restrict visibility, indicating a strong demand for more control over older items. In summary, a gap has been identified between preferred and actual visibility settings which can be interpreted as the users' demand for more control over shared items, yet being currently unable to accurately adjust the visibility according to their wishes. Additional research is required to analyze whether this gap is due to a lack of available means to control visibility or due to difficulties in making use of the settings available.

Discussing the results from a general point of view, fewer discrepancies between actual and either perceived or preferred visibility settings exist than one might possibly expect but instead the settings often match. Yet, concluding that privacy threats stemming from other users are minor or do not exist at all would fall short. Rather, the crucial point here is to define the term privacy violation. In other words, to be regarded a privacy violation, how many shared items must be unintentionally visible to other users? We argue that no universally valid answer to this question exists, but it rather depends on the shared item and the people being able to see it. Thus, for this work, gaps between actual and either perceived or preferred visibility settings are regarded a *potential* violation of privacy.

Additionally, it might be argued that a negative impact on the results might stem from participants who, even if they are highly privacy-conscious, do not engage in better privacy protection for various reasons (e.g. in cases where the privacy paradox applies). Yet, this does not influence our results, as the mismatch between perceived and preferred visibility is not investigated in this study. Instead, even if privacy-conscious people use loose visibility settings, they are firstly aware of these settings and secondly they intentionally defined the settings to be loose.

From a theoretical point of view, this work contributes by providing a conceptual framework (see Figure 1) that decomposes privacy threats stemming from other OSN users to a lack of awareness and a lack of control. Hence, this conceptual model can be used to quantify and thereby operationalize privacy problems by reducing them to the difference between actual and either perceived or preferred visibility settings. To mitigate awareness problems, expected and actual settings need to become closer. Likewise, to overcome issues of insufficient control, one needs to equalize preferred and actual settings.

Drawing from the results of this study, several theoretical and research implications can be deduced. It seems that social identity theory [9], which is commonly used to describe interaction between people in the physical world, cannot fully capture the problems of managing identities on OSN, due to inherent properties of mediated communication (e.g. persistence) and to limitations posed by SIdM tools provided by OSN service providers. Hereunto, research could evolve by incorporating these inherent properties of OSN into social identity theory and thus facilitate the theoretical understanding of OSN privacy. For practical research implications, these inherent properties of OSN (such as digital availability) provide opportunities to improve on privacy, e.g. by developing automation techniques to assist the user in managing identities online.

From a practical point of view, several implications emerge. While studies show [19] that OSN service providers have few incentives to improve default settings, regulatory measures might be enacted to enforce implementation. For sharing decisions, a shift from traditional access control models to sharing along social contexts could help to close the gap between preferred and actual visibility settings, such as by dividing the platform into separate spaces. In addition, automation techniques, as proposed in [18, 20], could relieve the burden to define the audience every time an item is shared. Besides legal and technical solutions, better education of OSN users could also help to reduce existing discrepancies.

Acknowledgements

The authors wish to thank Tobias Amann, Tobias Burger, Johannes Sänger, Santiago Suppan, and Tao Yang for their assistance at various stages of this study. This research is partly funded by the European Union within the PADGETS project (no. 248920).

References

[1] A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", Proc. of the 6th international Workshop on Privacy-Enhancing Technologies, Springer, 2006, pp. 36-58.

[2] E. Aïmeur, S. Gambs and A. Ho, "Towards a Privacy-Enhanced social Networking Site", Proc. of the 5th International Conference on Availability, Reliability and Security (ARES), IEEE, 2010, pp. 172-179.

[3] J. Binder, A. Howes and A. Sutcliffe, "The Problem of Conflicting Social Spheres: Effects of Network Structure on Experienced Tension in Social Network Sites", Proc. of the 27th International Conference on Human Factors in Computing Systems (CHI), ACM, 2009, pp. 965–974.

[4] J. Bonneau and S. Preibusch, "The Privacy Jungle: On the Market for Data Protection in Social Networks", Proc. of the 8th Workshop on the Economics of Information Security (WEIS), 2009, pp. 121-167.

[5] d. boyd, "Taken Out of Context: American Teen Sociality in Networked Publics". PhD thesis, University of California, Berkeley, 2008.

[6] d. boyd and N. Ellison, "Social Network Sites: Definition, History and Scholarship", Journal of Computer-Mediated Communication 13(1), 2008, pp. 210-230.

[7] B. Debatin, J. P. Lovejoy, A.-K. Horn and B. N. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", Journal of Computer-Mediated Communication, 2009, pp. 83–108.

[8] J. M. DiMicco and D. R. Millen, "Identity Management: Multiple Presentations of Self in Facebook", Proc. of the International Conference on Supporting Group Work, ACM, 2007, pp. 383-386.

[9] E. Goffman, "The Presentation of Self in Everyday Life", Anchor,1959.

[10] D. Irani, S. Webb, K. Li and C. Pu, "Large Online Social Footprints – An Emerging Threat", Proc. of the 2009 International Conference on Computational Science and Engineering, IEEE, 2009, pp. 271-276.

[11] H. Krasnova, N. F. Veltri and O. Günther, "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture - Intercultural Dynamics of Privacy Calculus", Business & Information Systems Engineering, Springer, 2001, 4(3), pp. 127– 135.

[12] R. Leenes, "Context is Everything: Sociality and Privacy in Online Social Network Sites", Privacy and Identity, IFIP AICT 320, 2010, pp. 48-65.

[13] K. Lewis, J. Kaufman, N. Christakis: "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network", Journal of Computer-Mediated Communication 14(1), 2008, pp. 79-100.

[14] H.R. Lipford, A. Besmer and J. Watson, "Understanding privacy settings in facebook with an audience view", Proc. of the 1st Conference on Usability, Psychology, and Security (UPSEC), USENIX Association Berkeley, 2008.

[15] Y. Liu, K. P. Gummadi, B. Krishnamurthy and A. Mislove, "Analyzing Facebook Privacy Settings: User Expectations vs. Reality", Proc. of the Internet Measurement Conference (IMC), ACM, 2011, pp. 61–70.

[16] M. J. M. Madejski and S. Bellovin, "The Failure of Online Social Network Privacy Settings", Technical report, Columbia University, NY, USA, 2011.

[17] B. Marder, A. Joinson and A. Shankar, "Every Post You Make, Every Pic You Take, I'll be Watching You: Behind Social Spheres on Facebook", Proc. of the 45th Hawaii International Conference on System Sciences (HICSS), IEEE, 2012, pp. 859-868.

[18] A. Mayer and S. L. Puller, "The Old Boy (and Girl) Network: Social Network Formation on University Campuses", Journal of Public Economics (92), Elsevier, 2008, pp. 329- 347.

[19] M. Netter, S. Herbst and G. Pernul, "Analyzing Privacy in Social Networks - An Interdisciplinary Approach", Proc. of the 3rd International Conference on Social Computing (SocialCom), IEEE, 2011, pp. 1327-1334.

[20] M. Netter, M. Riesner and G. Pernul, "Assisted Social Identity Management - Enhancing Privacy in the Social Web", Proc. of the 10th International Conference on Wirtschaftsinformatik (WI), 2011, pp. 1093-1103.

[21] C. Peterson, "Losing Face: An Environmental Analysis of Privacy on Facebook", SSRN eLibrary, 2010.

[22] M. Riesner, M. Netter, G. Pernul, "An Analysis of Implemented and Desirable Settings for Identity Management on Social Networking Sites", Proc. of the 7th International Conference on Availability, Reliability and Security (ARES), IEEE, 2012.

[23] F. Stutzman and J. Kramer-Duffield: "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook", Proc. of the 28th International Conference on Human Factors in Computing Systems (CHI), 2010, pp. 1553-1562.