VISUALIZING SOCIAL ROLES – DESIGN AND EVALUATION OF A BIRD'S-EYE VIEW OF SOCIAL NETWORK PRIVACY SETTINGS

Complete Research

Netter, Michael, University of Regensburg, Regensburg, Germany, michael.netter@ur.de

Weber, Michael, University of Regensburg, Regensburg, Germany, michael.weber@ur.de

Diener, Michael, University of Regensburg, Regensburg, Germany, michael.diener@ur.de

Pernul, Günther, University of Regensburg, Regensburg, Germany, guenther.pernul@ur.de

Abstract

The rising usage of Social Network Sites for interacting with contacts from multiple social spheres poses new privacy challenges and increasingly prompts users to manage their online identities. To convey a consistent image of the self when interacting with a group of contacts, at first awareness of previously used social roles is needed. However, existing tools on Social Network Sites to increase such awareness are often spread over different interfaces and the user is left to figure out which contacts have access to which shared items. To address these problems, we introduce the Access Policy Grid, a new visualization offering a bird's-eye view on defined privacy settings that allows identifying social roles and inconsistencies therein. To evaluate our visualization, we present the results of a laboratory experiment involving 32 participants in which we compare the Access Policy Grid to the native Facebook interface. For five out of six research questions, our results show that the APG outperforms the Facebook interface significantly in terms of at least one of the three investigated aspects (accuracy, confidence, and time-to-task completion).

Keywords: Privacy Awareness, Visualization, Social Network Sites, Privacy, Social Roles, Privacy Settings.

1 Introduction and Motivation

Social Network Sites (SNSs) play an increasingly important role for social interaction. While real-world Social Networks have always been an important part of everyday life, the ability to stay in touch with contacts from different social spheres (e.g. family members and colleagues) and to bridge spatial and temporal communication boundaries increasingly shifts social life to its online counterpart.

Despite these positive social outcomes, the use of SNSs for social interaction poses new privacy threats (Ziegele and Quiring, 2011). SNS users face the challenge to present different facets of their identity to different groups of contacts (referred to as audiences (van den Berg and Leenes, 2011), see Table 1 for an overview of terminology) in a way that shared personal items are not accessible to contacts for whom they are not intended (e.g. preventing family-related items to be visible for one's employer). Historically, managing one's self-presentation is not a SNS-specific phenomenon, but is part of everyday life. In the physical world, each individual performs multiple social roles (see Table 1) for different audiences aiming to convey a favorable image of the self and to keep these roles separated and consistent (Goffman, 1959). Privacy is violated if social roles become inconsistent such as when both family and work-colleagues have access to one's family role (cf. privacy as contextual integrity (Nissenbaum, 2010)).

Lately, the use of social roles becomes increasingly important on SNSs as these sites evolve to multi-purpose platforms where contacts from different and potentially conflicting social spheres are simultaneously present (Binder et al., 2009). SNS users face the challenge to map their multi-faceted identity onto a single profile (Peterson, 2010) and simultaneously meet the expectations of different audiences in order to keep social roles consistent. The problem increases as it has been shown that most contacts in SNSs are based on relationships previously established in the physical world (Mayer and Puller, 2008). Thus, inconsistent social roles on SNSs do not only affect the online world, but are likely to have a negative impact on the images one wants to convey in the physical world as well. Drawing on identity theory (e.g. (Zhao et al., 2008)), the disembodied environment of SNSs emphasizes the communication aspect of self-presentation rather than one's physical appearance or behavior. Similarly, boyd [sic] argues that on SNSs "people must engage in explicit acts to write themselves into being" (boyd, 2008b). As a result of the increased focus on the communication part of one's identity, being able to control the visibility of shared items becomes of paramount importance to create and manage social roles and ultimately to preserve privacy. Consequently, social roles on SNSs are implicitly created as they can be seen as the result of the privacy settings of all items.

To gain a deeper understanding of privacy on SNSs, it can be decomposed into a problem of awareness and a problem of control (Netter et al., 2013). Privacy control refers to technological means to put one's privacy preferences into practice. A large body of privacy control-related research exists, such as context-dependent (Carminati et al., 2011) and usable (Watson et al., 2009) access controls, user assistance (Fang and LeFevre, 2010), and audience management (van den Berg and Leenes, 2011). Similarly, current SNSs offer a variety of privacy settings to control the visibility of each shared item on the level of whole audiences or single contacts (Riesner et al., 2013). Privacy awareness in contrast can be seen as a prerequisite for control and refers to SNS users' understanding of how they are perceived by others (see Section 2 for an in-depth discussion of privacy awareness). Several obstacles currently impede privacy awareness on SNSs, such as the large number of items and contacts and the resulting complexity of privacy settings. Further obstacles include the static nature of privacy settings (Kauer et al., 2013) (while users' identities and their social graphs permanently evolve) and the lack of appropriate means to translate privacy settings into human-understandable representations. In particular, it is acknowledged among researchers (e.g. (Kelley et al., 2011), (Reeder et al., 2008)) that a holistic view is needed on SNSs to offer a bird's-eye view which shows the impact of all privacy settings and enables SNS users to perceive and understand their social roles and potential inconsistencies therein.

We address this issue by developing and evaluating the Access Policy Grid (APG), a sorted matrix-based visualization of SNS privacy settings (i.e. rows and columns are automatically reordered to show different clusters). Such visualization provides a bird's-eye view on a SNS account and is – to the best of our knowledge – the first privacy awareness tool that is able to visualize social roles. Thus, rather than focusing on clustering techniques, the main contribution of this paper is to make previously unrecognizable social roles explicit to SNS users. We follow a mixed methods research approach as proposed by Huysmans and De Bruyn (2013) combining design and behavioral research. The complementary nature of both paradigms is acknowledged in literature (March and Smith, 1995; Hevner et al., 2004; Gregor and Baskerville, 2012) and behavioral research methods are considered particularly useful to evaluate a designed artifact (Peffers et al., 2007; Venable et al., 2012).

Following the mixed methods research approach, we discuss related work and the theoretical background of our research in Section 2. In Section 3, we present the design of the APG visualization and discuss how it contributes to privacy awareness on SNSs. A laboratory experiment is designed and conducted in Section 4 to evaluate the APG by comparing it to the Facebook interface. Results of the experiment are presented in Section 5. We discuss limitations of the design and evaluation in Section 6, before finally presenting implications and conclusions in Section 7.

Concept	**Description**
Item	Any personal information shared on a SNS. Examples include pictures, profile data, and status messages. Sensitivity as well as granularity of available privacy settings for each item may vary.
Contact	Any person or organization that can access (parts of) a SNS user's shared items. Contacts that have an explicitly expressed relation with the SNS user's profile are often termed "friends".
Permission	A single authorization assigned to a contact to see a particular item using a SNS's privacy settings.
Social Sphere	Refers to a particular area of life (such as family life or workplace) with distinct rules, social norms, and expectations of its people.
Audience	Comprises a set of contacts that belong to a similar social sphere (e.g. work colleagues or family members) and consequently (should) have access to a similar set of items. Audiences may be explicitly defined through the use of friend lists.
Social Role	Comprises a set of items presented to a particular audience in order to create a desired image of the self. Social roles might be overlapping, e.g. when sharing a personal photo album with both close friends and family members.

Table 1. Overview of terminology

2 Research Background and Related Work

A variety of definitions for privacy awareness exist in literature (e.g. (Pötzsch, 2009)). For SNSs, privacy awareness can be defined as the knowledge of who can access which of one's shared items. This concept is further refined by Netter et al. (2013), where a distinction is made between *actual* and *perceived* visibility of shared items. Perceived visibility refers to what a user believes a particular contact can see. Likewise, actual visibility reflects the item's currently active settings as defined on the SNS. Based on this conceptualization, privacy awareness is the degree to which perceived and actual visibility match. A discrepancy between both states can be interpreted as a lack of awareness.

Information visualization is widely used in academic approaches to reduce the discrepancy between actual and perceived visibility (and thereby increase privacy awareness). Information visualization in general aims at creating understandable representations of raw data using visual means that amplify cognition (Mazza, 2009; Card et al., 1999). Regarding SNSs, several approaches exist that visualize privacy settings in order to improve awareness. The Expandable Grid proposed by Reeder et al. (2008)

and adopted to SNSs by Lipford et al. (2010) offers a grid-based interface to edit and review SNS privacy settings. However, unlike the APG it does not implement sorting of rows and columns. While facilitating a basic understanding of assigned visibility permissions, an unsorted grid-based visualization makes it difficult to perceive and understand social roles. Besides, the Audience View proposed by Lipford et al. (2008) extends the Privacy Mirror concept (Nguyen and Mynatt, 2002), which allows to display one's SNS profile from the perspective of another user. The Audience View structures privacy settings based on what a particular audience should be able to see and compartmentalizes the SNS profile into audience-specific areas. Similarly, Anwar and Fong (2011) and Anwar et al. (2010) introduce a mirror-like graph-based visualization of privacy settings. While both approaches improve the contact-based privacy mirror concept available on many SNSs (such as Facebook's "View As…" functionality), they do not consider social roles and are insufficient to compare perceived and actual visibility in order to gain comprehensive privacy awareness.

Besides SNSs, understanding permission assignments (e.g. using access control matrices (Lampson 1971)) has been in the focus of research since the sixties (Fuchs et al., 2011). A later and advanced approach is Role-based Access Control (RBAC) (Ferraiolo et al., 2001), which is widely used in enterprise Identity Management (IdM) systems to control employees' access to protected resources. Due to the large number of permissions as well as frequent job and position changes of employees, correctly managing users and their roles becomes a tedious and error-prone task. To reduce the burden of manually evaluating the correctness and consistency of assigned roles, the concept of role mining (based on data mining techniques) emerged (Kuhlmann et al., 2003). Role mining algorithms (e.g. (Schlegelmilch and Steffens, 2005; Vaidya et al., 2007)) are used to identify a set of clusters of similar users on the basis of existing access rights. Rather than a textual representation of role candidates, lately visual role mining has been proposed by Colantonio et al. (2012) to visualize discovered clusters. Visual role mining uses a matrix-based representation of access rights and relies on human cognitive abilities to discover meaningful clusters and find erroneous permission assignments.

From the previous discussion it follows that the management of RBAC roles in the context of IdM and managing privacy settings to access items on SNSs share many characteristics. In the following, we adapt the concept of visual role mining and design a new visualization that allows detecting and understanding social roles that are currently difficult to extract from privacy settings of SNSs.

3 Access Policy Grid Design

The previous sections revealed the importance of information visualization in the context of SNSs to detect social roles and ultimately increase the users' privacy awareness. Following a design-oriented research approach, in this section we present the design of the APG and outline its characteristics.

3.1 Modelling self-presentation on SNSs

Prior to the design of a suitable visualization to enhance privacy awareness we first study how users manage their self-presentation on SNSs. For this purpose, we build upon Perceptual Control Theory (PCT) (Powers, 2005). PCT describes human behavior using a feedback loop in which a person constantly samples the results of his behavior, compares it to his preferences and again takes action if a gap exists between perception and preferences.

In Figure 1 we apply PCT to describe self-presentation on SNSs. Initially, a SNS user starts out from his preferred social roles as used in the physical world (e.g. a work role, close friends role, and family role). On SNSs, social roles consist of two fundamental entities (namely shared items and contacts) and of relations between these two entities (i.e. permissions assigned to contacts to be able to access particular items). As defined in Table 1, a social role comprises a specific set of items that is visible to a particular audience in order to convey an intended impression. Privacy settings are used to control the visibility of items and implement preferred social roles on SNSs. Over time, internal and external

disturbances change visibility preferences. Internal disturbances may comprise personal development (e.g. the user's transition from school to work life) accompanied by an evolving identity. External disturbances include changes in the user's social graph such as when making new friends.

As a result of such disturbances, preferred and actual visibility begin to diverge, i.e. due to changed preferences the actual and preferred privacy settings become inconsistent. Thus, privacy settings as provided technological means need to be adapted to reflect one's preferences. Yet, prior to make these alterations (i.e. to exercise privacy control), it is necessary to perceive and understand the current context of existing entities (contacts and items), relations between entities (permissions) and existing social roles, i.e. to align perceived and actual visibility. This is not implicitly the case, as perceived and actual visibility deviate over time due to lapses of memory, the technical nature and the complexity of visibility settings. To match perceived and actual visibility (i.e. to raise privacy awareness), technological means to visualize actual visibility are necessary. Based on the understanding gained, preferred and perceived visibility can be compared and privacy settings can be changed accordingly. The feedback loop is repetitively executed to align actual and preferred visibility.

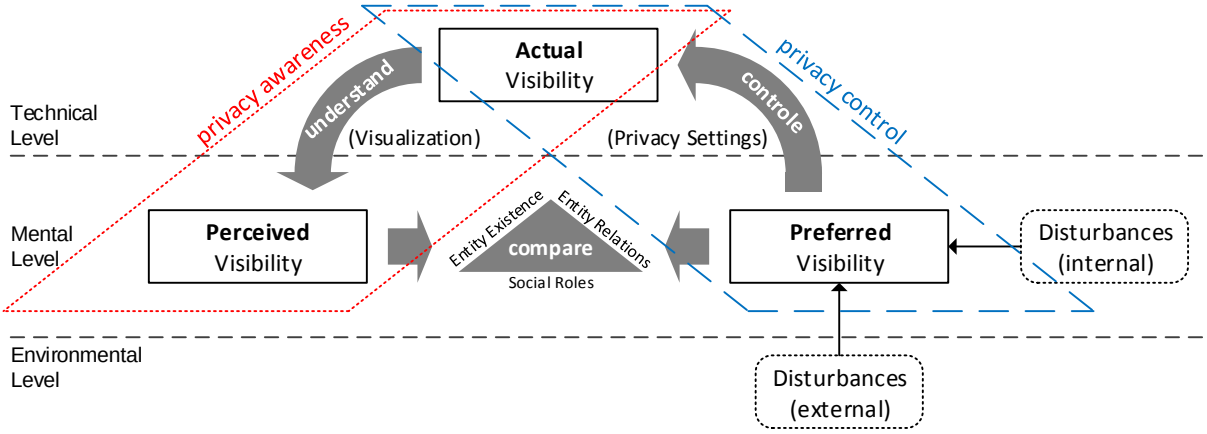

Figure 1. Feedback loop of SNS self-presentation

Two technological challenges for privacy, already mentioned in Section 1, can be identified within this feedback loop. First, to provide appropriate technological means of privacy control, allowing users to change actual visibility according to their preferences. Second, to offer technological means to raise privacy awareness, enabling users to align perceived visibility and actual visibility. For the design of the APG, we solely focus on the second challenge (red-dotted area of the feedback loop in Figure 1). The goal is to facilitate the user's understanding of social roles as defined on a SNS by translating privacy settings into a visual representation to use human cognition to facilitate the comparison with his preferences. Prospectively, the APG could be useful to enhance privacy control to solve the first challenge (blue-dashed area in Figure 1), yet this is not addressed in this paper.

3.2 Conceptual design of the Access Policy Grid

The APG is designed to fulfill the requirements for aligning actual and perceived visibility in SNSs, as described above. In general, choosing a suitable visualization technique is crucial to convey relevant information. The APG uses a matrix-based representation as such a visualization allows to explore the relation between a large number of objects without reducing the number of dimensions (Chen et al., 2008). In an initial step (see Figure 2), privacy settings of all items of a particular SNS account are gathered and subsequently converted into a matrix representation. Rows represent all shared items (i_1, ..., i_m) while all contacts (c_1, ..., c_n) are depicted as columns. A cell c_{ij} is colored if contact c_j has the permission to see item i_i. Note that rather than showing several permission operations (such as create, update, and delete) the APG is designed to visualize only read permissions as this operation is almost

exclusively used on SNSs. In more detail, sharing personal items on SNSs ultimately means assigning read permissions to one's contacts, while contacts are seldom able to modify a user's items.

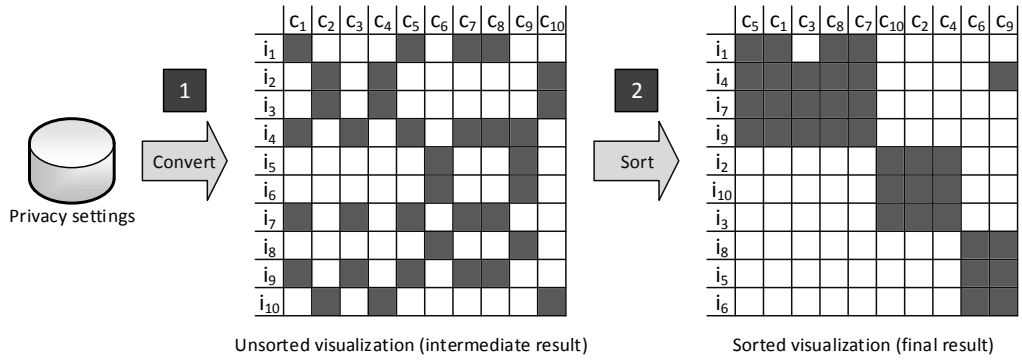

Figure 2. Access Policy Grid generation process on a conceptual level

In a second step (see Figure 2), rows and columns need to be sorted in order to visualize clusters of contacts that are able to access a similar set of items. As sorting the APG is an optimization problem, choosing an appropriate algorithm is crucial to reveal patterns and inconsistencies that are relevant in the context of SNSs. In general, the technique of discovering homogenous groups of objects in a matrix is known as biclustering which was first introduced by Hartigan (1972). Various optimality criteria exist, such as finding an optimal set of non-overlapping clusters or to prioritize clusters with specific attributes. However, as in most cases, the problem of finding an optimal set of clusters is NP-complete (Madeira and Oliveira, 2004), most algorithms use heuristic approaches. Due to the similar characteristics of RBAC roles and social roles, we employ the ADVISER algorithm (Colantonio et al., 2012). In a nutshell, the algorithm operates as follows: data mining algorithms are initially applied to create clusters of similar items/contacts. Subsequently, the algorithm determines the position of each cluster starting with the largest cluster. Finally, clusters that share items/contacts are positioned next to each other using a similarity measure.

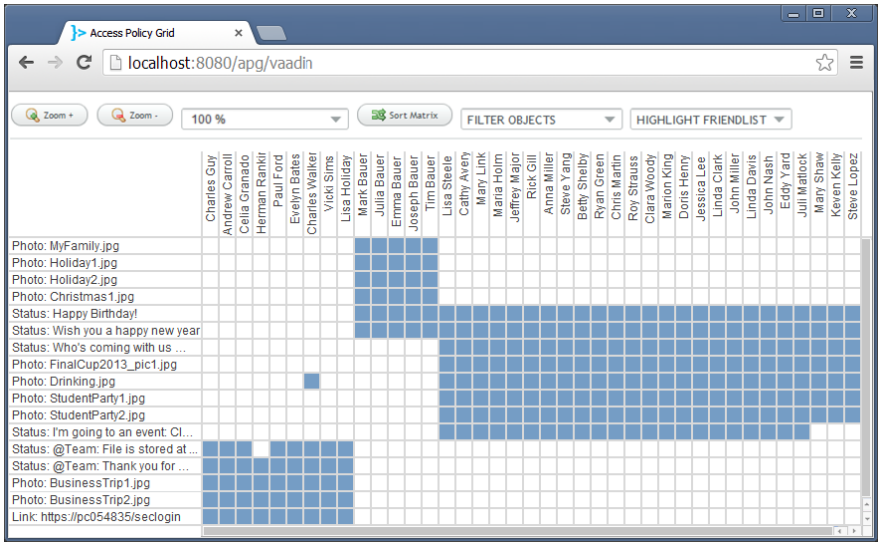

Figure 3. Access Policy Grid interface

3.3 Detection of Social Roles and Inconsistencies

Based on the conceptual design of the previous section, we implemented the APG as a web-based Facebook application to use the Facebook API to import profile data. Figure 3 depicts the sorted APG

interface after gathering permission data from a dummy Facebook profile. By depicting shared items (such as photographs, status messages, and links) as rows and all contacts as columns, the APG provides a holistic view that captures all currently active visibility permissions.

As with most visualizations, the amount of input data often exceeds the information that can conveniently be displayed (Cockburn et al., 2008). The APG integrates several functions to cope with large datasets and maintain usability and scalability. Pan and zoom functionalities (with scrollbars being displayed as needed) allow to focus on interesting segments (such as potential excessive permission assignments) or take a bird's-eye view to understand the impact of privacy settings in a wider context. Moreover, filtering functionalities are available to focus on particular item types (such as pictures) and to highlight existing friend lists (if defined on the SNS account). Upon mouseover, additional information for a particular cell is displayed in an overlay window.

Following our conceptual model of SNS self-presentation (Figure 1), the APG facilitates privacy awareness in three ways. Firstly, the uncluttered interface allows to easily perceiving all shared items and all contacts connected to the SNS profile, i.e. to check the existence of fundamental entities (see Figure 4). In addition, relations between shared items and contacts can be easily understood, providing insights to questions such as: is contact c_1 able to see item i_2? Which items are visible to contact c_1? Which contacts can see item i_1?

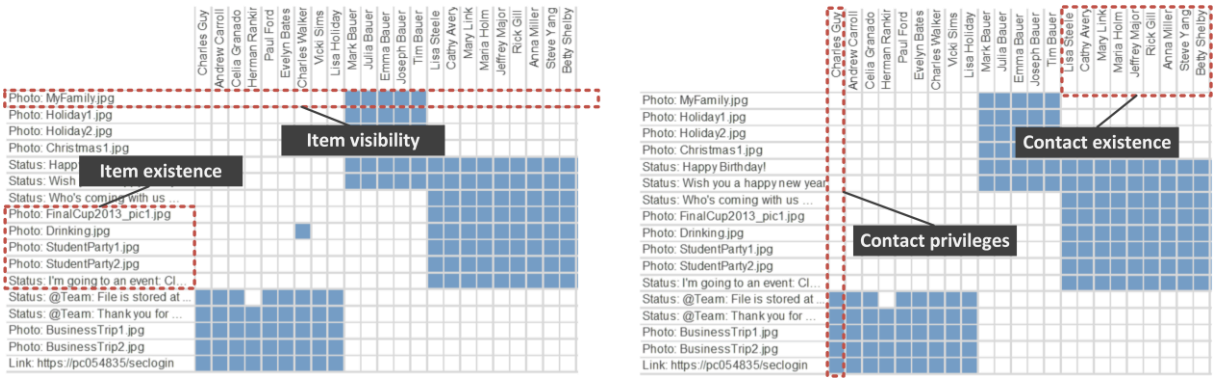

Figure 4. Visualization of fundamental entities and permission relations between entities

Secondly, the sorted matrix-based representation is particularly useful to uncover a SNS user's social roles. Similar items assigned to be visible to particular contacts form a social role candidate and can be easily detected by focusing on clusters of blue-colored cells. For illustrative purposes, potential social roles are highlighted in Figure 5. As can be seen, social roles can be overlapping (such as when sharing a photograph with both family members and close friends).

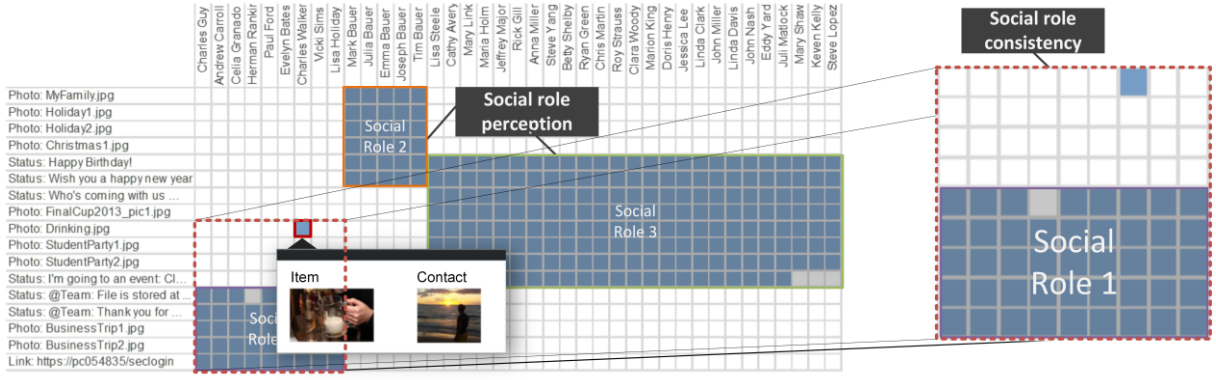

Figure 5. Visualization of social roles and their consistency

Thirdly, the APG facilitates the detection of inconsistencies such as missing or excessive permissions. Such permissions lead to inhomogeneous social roles and can be easily identified as cells of a cluster that are not colored or stray colored cells. To further investigate such potential misconfigured visibility settings, cells can be selected and additional information on the respective item and contact is displayed in an overlay window (see Figure 5).

4 Evaluation

Following the mixed methods research approach (Huysmans and De Bruyn, 2013) outlined in Section 1, we rely on behavioral research methods to evaluate the designed artifact. In particular, we conducted a laboratory experiment (Siau and Rossi, 2011) to assess the efficacy of the APG and its impact on privacy awareness by comparing it to the standard Facebook interface[1]. Therefore, the interface under investigation constitutes the independent variable while dependent variables include times-to-task completion, accuracy rates, and the participants' confidence in their answers.

4.1 Research Questions

Based on the theoretical understanding of privacy awareness (see Section 2) and self-presentation (see Section 3.1), we decompose privacy awareness on SNSs into smaller pieces that can be addressed through several research questions.

Awareness of fundamental entities revolves around a SNS user's knowledge of the mere existence of items and contacts and can be considered as a prerequisite for more complex questions. The first research question consequently assesses the participants' ability to check the existence of items and contacts when using both interfaces (APG and the Facebook interface):

- **RQ1a (Item existence)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to check the existence of particular items?
- **RQ1b (Contact existence)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to check the existence of particular contacts?

Besides mere existence, understanding the *relation between fundamental entities* contributes to a SNS user's privacy awareness. Such a relation describes the permissions assigned to contacts to see particular items. The second research question thus assesses the users' understanding of <1:1>, <1:n>, and <n:1> relations between items and contacts.

- **RQ2a (Item visibility)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to understand which contacts have access to a particular item?
- **RQ2b (Contact privileges)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to understand which items a particular contact has access to?

Finally, we assess a SNS users' understanding of <n:m> relations between items and contacts. Such a relation can be interpreted as a social role, i.e. a set of particular items which should be visible to a particular audience in order to convey an intended image of the self. Hence, the third research question is concerned with being aware of one's *social roles and inconsistencies* therein:

- **RQ3a (Social role perception)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to identify existing social roles that are used to convey certain self-images to particular audiences?

[1] An overview of Facebook's privacy settings is provided at: https://www.facebook.com/help/325807937506242/

- **RQ3b (Social role consistency)**: Compared to the Facebook interface, does the APG improve the SNS users' ability to determine potential inconsistencies in a given social role such as excessive or missing permissions?

4.2 Recruiting Methods

To answer these research questions, we recruited participants for our laboratory experiment in four ways: through an announcement on the department's website and Facebook page, through an announcement on the institute's bulletin board, through an e-mail announcement, and through word of mouth. In the announcement we asked for participation in a SNS-related usability experiment. Neither the announcement nor the introduction of the participants to the experiment contained any reference to privacy or privacy awareness as literature has indicated (Braunstein et al., 2011) that there is a potential bias in replies to privacy-related questions.

4.3 Experiment Design

To investigate the research questions presented in Section 4.1, we developed two scenarios. These scenarios are used during the experiment rather than the participants' own Facebook profile in order to provide equal conditions. Each scenario represents an artificial SNS profile that contains a set of items shared with contacts. Scenarios were designed to resemble a typical SNS profile and contain contacts from different social spheres (e.g. family members, close friends, and colleagues) and both sensitive (e.g. pictures) and non-sensitive items (e.g. status messages) shared with these contacts in a targeted manner. Different items and contacts were used for each scenario but each scenario consisted of an equal number of items and contacts.

Hereunto, we created a hardcopy explanation sheet for each scenario, illustrating in detail contacts, their belonging social sphere, and which items they are able to access. These hardcopy sheets are used to represent the participant's perceived visibility. In addition, we crafted corresponding Facebook profiles for both scenarios (representing the actual visibility) and purposefully manipulated these profiles to contain some minor deviations (e.g. slightly different visibility settings) from the hardcopy. The experiment was conducted in a dedicated room of the department in groups of up to three participants between September and October 2013. Figure 6 depicts the course of the experiment as well as its main components. In the first step, we used a presentation to introduce each group of participants to the experiment and explicate relevant concepts such as self-presentation on SNSs, items, audiences and social roles. In a second step, we gathered basic demographic information. During the preparation phase, we explained the functionality of both the Facebook interface and the APG and pointed out where to find relevant information (such as privacy settings). Subsequently, participants were given unlimited time to play with both interfaces (based on a dummy Facebook account). During the second part of the preparation phase, participants had unlimited time to study the hardcopy explanation sheets in order to become familiar with both scenarios.

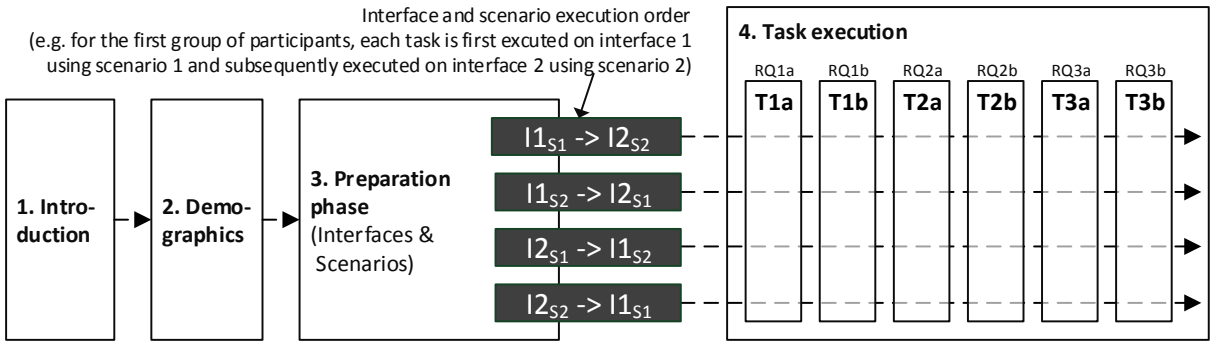

Figure 6. Experiment Design

Upon completing the preparatory phase, participants were asked to complete a set of tasks on both interfaces, following a within-subject design. To avoid carryover effects, we counterbalanced[2] both the interfaces and the scenarios, resulting in four groups of participants (see Figure 6).

To answer the research questions posed in Section 4.1, we designed the following six tasks that had to be executed on both interfaces. Each task addresses one research question.

- **T1a (Item existence):** Check the existence of a set of given items. The task examines basic awareness of the availability of single entities, addressing research question RQ1a.
- **T1b (Contact existence):** Check the existence of a set of given contacts. The task examines basic awareness of the availability of single entities, addressing research question RQ1b.
- **T2a (Item visibility):** Determine which contacts have access to a particular item. The task examines awareness of the impact of a relation (permission assignment) between an item and some contacts, addressing research question RQ2a.
- **T2b (Contact privileges):** Identify which items a particular contact is able to access. The task examines awareness of the impact of a relation (access privileges) between a contact and some items, addressing research question RQ2b.
- **T3a (Social role perception):** Identify existing social roles that are used to convey certain self-images to particular contacts. The task examines the participant's awareness of previously used social roles, addressing research question RQ3a.
- **T3b (Social role consistency):** For a given social role, determine potential inconsistencies such as excessive or missing permissions. The task examines the participant's awareness of inconsistent social roles that may have a negative impact on his self-presentation, addressing research question RQ3b.

For each task, we measured time-to-task completion, accuracy rate, and the participants' confidence in their answers (using a five point Likert scale). To arrive at a reasonable length of the overall experiment, each task had to be executed within a time-frame of two minutes for each interface.

5 Results

In this section, we present the results of our experiment. First, we discuss the participants' demographics. Subsequently, we outline the results of the previously proposed research questions. Hereunto, we present the results of the previously described tests ($\alpha = 0.05$) where we investigated significant differences in accuracy rate, time-to-task completion, and reported confidence between the APG and the Facebook interface.

5.1 Demographics

In total, we recruited 32 participants. The participants' age ranges from 24 to 52 years ($\chi = 29.03$; $\sigma = 6.879$). Females account for 46.88 %, which leads to a slight male bias (53.13 %). The majority of participants (81.25 %) stated to use Facebook regularly (more than three times a week).

Compared to the demographics of all Facebook users (Sage, 2013), we observe an overrepresentation of the mid-twenties group, which can be attributed to the academic context of our study (90.63 % of the participants indicated to have an academic degree).

[2] Providing two scenarios and alternating the order of interfaces and scenarios reduce potential bias related to a practice and fatigue effect.

		Accuracy		Confidence			Time-to-task completion	
Task	**Interface**	**Rate**	**McNemar (p-value)**	**Quartiles x_{25},x_{50},x_{75}**	**Wilcoxon (p-value)**	**Sign Test (p-value)**	**Mean (sec.)**	**t-test (p-value, power)**
T1a	APG FB	94 % 72 %	**0.033**	4, 4, 4 $^1/_4$, 3, 4	< **0.001**	< **0.001**	54.81 111.69	< **0.001,** 1.00
T1b	APG FB	100 % 100 %	n/a	4, 4, 4 4, 4, 4	1.000	1.000	46.16 45.56	0.912, 0.05
T2a	APG FB	100 % 100 %	n/a	4, 4, 4 4, 4, 4	0.564	1.000	29.94 48.38	**0.001,** 0.95
T2b	APG FB	100 % 94 %	0.250	4, 4, 4 2, 4, 4	< **0.001**	< **0.001**	40.69 83.38	< **0.001,** 1.00
T3a	APG FB	81 % 19 %	< **0.001**	3, 3, 4 0, 1, $2^3/_4$	< **0.001**	< **0.001**	40.47 104.41	< **0.001,** 1.00
T3b	APG FB	97 % 59 %	< **0.001**	4, 4, 4 1, 3, 4	< **0.001**	< **0.001**	36.59 102.38	< **0.001,** 1.00

Table 2. Summary of statistical tests (bold p-values indicate statistical significance)

5.2 RQ1: Existence of Fundamental Entities

Based on time-to-task completion, accuracy, and confidence we investigate to which extent both interfaces allow checking the existence of items and contacts (cf. Section 4.1). First, we discuss the results for task T1a, examining the participants' awareness of the existence of particular items (RQ1a).

Drawing upon the results depicted in Table 2, a McNemar-Test (one-tailed) shows that the accuracy is significantly higher for the APG ($\pi = 94\,\%$) compared to the Facebook interface ($\pi = 72\,\%$). Moreover, both Wilcoxon and Sign Test (one-tailed) confirm that participants were significantly more confident in their answer when using the APG instead of Facebook. Finally, measuring the time-to-task completion, a t-test shows that participants were able to solve task T1a significantly faster when using the APG ($\bar{x} = 54.81, s = 28.44$) instead of Facebook's interface ($\bar{x} = 111.69, s = 19.05$). Based on these results, we infer that the APG's uncluttered visualization is superior to the Facebook interface, where items are spread over several categories and sites are often paginated.

Subsequently, we investigate the capabilities of both interfaces to check the existence of a particular contact (RQ1b). Results in Table 2 show that all participants were able to execute task T1b correctly with both interfaces ($\pi = 100\,\%$). Likewise, the time-to-task completion ($\bar{x} \approx 46, s_{APG} = 16.77, s_{FB} = 22.97$) and the participants confidence ($x_{med} = 4$) were almost identical on both interfaces. As a consequence, no statistically significant differences could be determined and as both interfaces offer a list of all contacts, similar results concerning RQ1b could be expected. We deduce from these results that both interfaces are equally suitable to gain an understanding of which contacts are connected to one's SNS profile.

5.3 RQ2: Relations between Fundamental Entities

Next, we investigate to which extent both interfaces facilitate the participants' awareness of relations between entities, i.e. their understanding of permissions assigned to contacts to see particular items.

At first, we investigate the participants' understanding of which contacts are able to see a particular item (RQ2a). Results in Table 2 show that all participants were able to execute task T2a correctly with both interfaces ($\pi = 100\,\%$) and were highly confident in their answers ($x_{med} = 4$). However, a t-test shows significantly that participants were able to solve the task faster using the APG ($\bar{x} = 29.94, s = 18{,}72$) than when using Facebook's interface ($\bar{x} = 48.38, s = 26.77$). From these results we infer that both interfaces offer a good visual representation of an item's privacy settings that is easy to

understand. However, the lack of an overview of all items on Facebook makes looking up particular items a time-consuming task.

Subsequently, we investigate the extent to which each interface facilitates the participants' understanding of which items a particular contact is able to access (RQ2b). Results (see Table 2) for the corresponding task T2b show that no significant differences exist in accuracy rates between the Facebook interface ($\pi = 94\,\%$) and the APG ($\pi = 100\,\%$). However, confidence is significantly higher for the APG. Results additionally show that participants were able to execute the task more than twice as fast using the APG ($\bar{x} = 40.69, s = 22.49$) compared to Facebook ($\bar{x} = 83.38, s = 29{,}79$). A t-test confirms that time-to-task completion results are significantly better for the APG. From these results we infer that both interfaces offer the required functionality to complete this task. Yet, results also suggest that Facebook's "View as…" function, which is used to assess which items a particular contact is able to see, makes it more difficult (and time-consuming) for users to get an overview of all items visible to a specific contact.

5.4 RQ3: Social Roles and Inconsistencies

In this section, we investigate the capabilities of both interfaces to understand <n:m> relations between items and contacts, i.e. the perception of social roles used on the SNS to convey a particular image of the self to a particular audience (RQ3a). Table 2 depicts the results of the corresponding task T3a. Accuracy rates are significantly higher for the APG ($\pi = 81\,\%$) compared to the Facebook interface ($\pi = 19\,\%$). Similarly, statistical tests confirm that confidence (APG ($x_{med} = 3$), Facebook ($x_{med} = 1$)) and time-to-task completion (APG ($\bar{x} = 40.47, s = 36.09$), Facebook ($\bar{x} = 104.41, s = 33{,}61$)) results are significantly better for the APG. From these results we infer that despite the increasing importance of social roles on SNSs, the Facebook interface lacks any means to visualize one's social roles. Rather, to do so, Facebook requires a user to manually check the privacy settings of all shared items which is not feasible in a real-world scenario.

Finally, we analyze both interfaces regarding their capabilities to discover inconsistencies (such as missing or excessive visibility permissions) (RQ3b). Results for the corresponding task T3b presented in Table 2 show that the APG ($\pi = 97\,\%$) leads to a significantly higher accuracy rate than the Facebook interface ($\pi = 59\,\%$). Similarly, both Wilcoxon (one-tailed) and Sign Test (one-tailed) confirm the participants' higher confidence when using the APG. Lastly, the time-to-task completion was significantly lower for the APG ($\bar{x} = 36.59, s = 23.14$) than when using the Facebook interface ($\bar{x} = 102.38, s = 34{,}39$). These results suggest that the APG's visual representation of social roles using clustered permissions eases the identification of cluster inhomogeneities which indicate potentially misconfigured privacy settings.

6 Limitations

One can argue that some limitations exist concerning the design of the APG as well as its evaluation. The APG is conceived as a tool to raise privacy awareness, i.e. to close the gap between perceived and actual visibility of shared items but does not allow to change privacy settings accordingly (due to the inability to modify privacy settings via the Facebook API). Besides, SNSs allow sharing a variety of data types whereas the matrix-based visualization of the APG is optimized for text-based items. To address this issue, the APG uses the item's description as a textual representation within the matrix and provides an overlay window to display non-text based content (such as pictures and videos). To address scalability issues, the APG relies on the ADVISER algorithm for sorting, which is used for large data sets in enterprise IdM systems. Furthermore, zoom and scroll functionality is integrated in the APG interface to maintain usability when dealing with a large number of contacts and items.

Concerning the APG evaluation, we compared the APG only to a single SNS interface, namely Facebook which we see however as the most representative at this time. The sample of our laboratory

experiment was overrepresentative of mid-twenty year old participants and largely consisted of regular Facebook users. However, solely analyzing participants in our sample that are 30 years or older (8 participants) leads to comparable results. Similarly, the APG outperformed the Facebook interface when only considering participants that are non-regular Facebook users (6 participants). Also, the comparably small sample size (32 participants in total) limits statistical significance, though we argue that by opting for conducting the experiment in a controlled environment with personal supervision, we achieved a better quality of responses compared to an open and remote survey. Moreover, an ongoing discussion exists concerning the number of participants in user experience related studies (e.g. Albert and Tullis (2013) suggest five to ten participants). Besides, it might be argued that using the participants' Facebook profiles instead of scenarios would have offered a more realistic setting to measure privacy awareness, however we opted for a scenario-driven evaluation to ensure comparability of results. Finally, the Hawthorne effect, stating that participants are motivated to perform better when under observation, might impact our results. Yet, later research has shown that there is little to no evidence of such an effect on participants' behavior (Jones, 1992).

7 Conclusion

In this paper we presented the APG, a new visualization of SNS visibility permissions in order to improve privacy awareness. To the best of our knowledge, the sorted matrix based APG is the first approach to visualize SNS users' different social roles, enabling them to understand how they are seen by different groups of contacts. To evaluate the designed artifact, we decomposed the notion of privacy awareness into six research questions and conducted a laboratory experiment with 32 participants, comparing the APG to the Facebook interface. For five out of six research questions, our results show that the APG outperforms the Facebook interface significantly in terms of at least one of the three investigated aspects (accuracy, confidence, and time-to-task completion).

Drawing on these results, both theoretical and practical implications can be inferred. From a scientific perspective, SNSs research often concentrates on improving privacy controls (such as fine-grained access control models). Yet, our results emphasize the importance of conducting research in the field of privacy awareness, which can be seen as a prerequisite for privacy control (SNS users first need to be aware of a potentially privacy-threatening item visibility and understand the need to take action before refining their privacy settings). Moreover, visualizing social roles to enhance privacy awareness opens areas for further research. Examples include the use of colors to indicate the frequency of item access by a contact (e.g. to refine social roles), displaying only a subset of social roles to optimize their visualization, and exploring the results of different biclustering algorithms on the user's awareness. With regards to privacy control, the APG may be used as a user-friendly interface to change privacy settings and reshape social roles (provided that appropriate SNS APIs are available).

From a practical point of view, our results imply that current SNSs lack functionality to visualize one's social roles. Yet, without understanding social roles users may increasingly proceed to only share personal items that are acceptable to contacts from all social spheres, leading to flat characters. In the long term, such social convergence (boyd, 2008a) may negatively impact the business model of SNSs as these sites become less interesting for its users when only dull or unimportant information is shared. As a consequence, we believe that SNS operators should have an inherent self-interest to provide appropriate means to visualize social roles and to technically empower its users to use SNSs as a medium for targeted and context-dependent social interaction.

8 Acknowledgements

The authors wish to thank Christian Richthammer for his implementation support. Parts of this research are based on previous work presented in Netter (2013) and were partly funded by "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007-2013 (EFRE) as part of the SECBIT project.

References

Albert, W., and Tullis, T., 2013. Measuring the User Experience, Second Edition: Collecting, Analyzing, and Presenting Usability Metrics (2 edition., p. 320). Waltham, MA: Morgan Kaufmann.

Anwar, M. and Fong, P.W.L., 2011. Access Control Policy Analysis with a Visualization Tool for Social Network Systems, Technical Report.

Anwar, M., Fong, P.W.L., Yang, X.-D. and Hamilton, H., 2010. Visualizing Privacy Implications of Access Control Policies in Social Network Systems. In Proc. of the 2nd International Conference on Data Privacy Management and Autonomous Spontaneous Security (DPM '09). Springer, pp. 106–120.

Binder, J., Howes, A. and Sutcliffe, A., 2009. The Problem of Conflicting Social Spheres: Effects of Network Structure on Experienced Tension in Social Network Sites. In Proc. of the 27th International Conference on Human Factors in Computing Systems (CHI '09). ACM, pp. 965–974.

boyd, danah, 2008a. Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. Convergence: The International Journal of Research into New Media Technologies, 14(1), pp. 13–20.

boyd, danah, 2008b. Taken Out of Context: American Teen Sociality in Networked Publics. University of California, Berkeley.

Braunstein, A., Granka, L. and Staddon, J., 2011. Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It. In Proc. of the 7th Symposium on Usable Privacy and Security (SOUPS '11). ACM, pp. 15:1–15:14.

Card, S.K., Mackinlay, J.D. and Shneiderman, B., 1999. Readings in Information Visualization: Using Vision to Think, Morgan Kaufmann Publishers Inc.

Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M. and Thuraisingham, B., 2011. Semantic web-based Social Network Access Control. Computers & Security, 30(2-3), pp. 108–115.

Chen, C., Härdle, W. and Unwin, A., 2008. Handbook of Data Visualization, Springer.

Cockburn, A., Karlson, A. and Bederson, B.B., 2008. A review of overview+detail, zooming, and focus+context interfaces. ACM Computing Surveys, 41(1), pp. 2:1–2:31.

Colantonio, A., Di Pietro, R., Ocello, A. and Verde, N.V., 2012. Visual Role Mining: A Picture Is Worth a Thousand Roles. IEEE Transactions on Knowledge and Data Engineering, 24(6), pp. 1120–1133.

Fang, L. and LeFevre, K., 2010. Privacy Wizards for Social Networking Sites. In Proc. of the 19th International Conference on World Wide Web (WWW '10). ACM, pp. 351–360.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R., 2001. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 4(3), pp. 224–274.

Fuchs, L., Pernul, G., and Sandhu, R., 2011. Roles in information security – A survey and classification of the research area. Computers & Security, 30(8), 748–769.

Goffman, E., 1959. The Presentation of Self in Everyday Life, Anchor.

Gregor, S. and Baskerville, R., 2012. The fusion of design science and social science research. In Information Systems Foundation Workshop.

Hartigan, J. A., 1972. Direct clustering of a data matrix. Journal of the American Statistical Association, 67(337), 123–129.

Hevner, A.R., March, S.T., Park, J. and Ram, S., 2004. Design science in information systems research. MIS Quaterly, 28(1), pp. 75–105.

Huysmans, P. and De Bruyn, P., 2013. A Mixed Methods Approach To Combining Behavioral And Design Research Methods In Information Systems Research. In Proc. in 21st European Conference on Information Systems (ECIS '13). p. 29.

Jones, S.R.G., 1992. Was There a Hawthorne Effect? American Journal of Sociology, 98(3), pp. 451–468.

Kauer, M., Franz, B., Pfeiffer, T., Heine, M. and Christin, D., 2013. Improving privacy settings for facebook by using interpersonal distance as criterion. In Proc. of the 31st International Conference on Human Factors in Computing Systems, extended abstracts (CHI '13). ACM, pp. 793–798.

Kelley, P.G., Brewer, R., Mayer, Y., Cranor, L. and Sadeh, N., 2011. An Investigation into Facebook Friend Grouping. In Proc. of the 13th IFIP TC 13 International Conference on Human-computer Interact (INTERACT '11). Springer, pp. 216–233.

Kuhlmann, M., Shohat, D. and Schimpf, G., 2003. Role mining - revealing business roles for security administration using data mining technology. In Proc. of the 8th ACM Symposium on Access Control Models and Technologies (SACMAT '03). ACM, pp. 179–186.

Lampson, B. W., 1971. "Protection". In Proc. of the 5th Princeton Symposium on Information Sciences and Systems, Princeton University, pp. 437-443, reprinted In Operating Systems Review, 8 (1), January 1974, pp. 18-24.

Lipford, H.R., Besmer, A. and Watson, J., 2008. Understanding Privacy Settings in Facebook with an Audience View. In Proc. of the 1st Conference on Usability, Psychology, and Security (UPSEC '08). USENIX Association, pp. 2:1–2:8.

Lipford, H.R., Watson, J., Whitney, M., Froiland, K. and Reeder, R.W., 2010. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proc. of the 28th International Conference on Human Factors in Computing Systems (CHI '10). ACM, pp. 1111–1114.

Madeira, S. C., and Oliveira, A. L., 2004. Biclustering algorithms for biological data analysis: a survey. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 1(1), 24–45.

March, S.T. and Smith, G.F., 1995. Design and Natural Science Research on Information Technology. Decision Support Systems, 15(4), pp. 251–266.

Mayer, A. and Puller, S.L., 2008. The Old Boy (and Girl) Network: Social Network Formation on University Campuses. Journal of Public Economics, 92(1-2), pp. 329–347.

Mazza, R., 2009. Introduction to Information Visualization, Springer.

Netter, M., 2013. Privacy-preserving Infrastructure for Social Identity Management, PhD thesis, Shaker publishing, 2013

Netter, M., Riesner, M., Weber, M. and Pernul, G., 2013. Privacy Settings in Online Social Networks - Preferences, Perception, and Reality. In Proc. of the 46th Hawaii International Conference on System Sciences (HICSS '13). IEEE, pp. 3219–3228.

Nguyen, D.H. and Mynatt, E.D., 2002. Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems, Technical Report.

Nissenbaum, H., 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press.

Peffers, K., Tuunanen, T., Rothenberger, M. and Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), pp. 45–77.

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

Pötzsch, S., 2009. Privacy Awareness: A Means to Solve the Privacy Paradox? In V. Matyáš et al., eds. The Future of Identity in the Information Society. Springer, pp. 226–236.

Powers, W.T., 2005. Behavior: The control of perception 2nd ed., Benchmark Publications.

Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Bacon, K., How, K. and Strong, H., 2008. Expandable Grids for Visualizing and Authoring Computer Security Policies. In Proc. of the 26th International Conference on Human Factors in Computing Systems (CHI '08). ACM, pp. 1473–1482.

Riesner, M., Netter, M. and Pernul, G., 2013. Analyzing Settings for Social Identity Management on Social Networking Sites: Classification, Current State, and Proposed Developments. Information Security Technical Report, 17(4), pp. 56–69.

Sage, A., 2013. The Facebook Platform and the Future of Social Research. In Social Media, Sociality, and Survey Research. Wiley, pp. 87–106.

Schlegelmilch, J. and Steffens, U., 2005. Role mining with ORCA. In Proc. of the 10th ACM symposium on Access Control Models and Technologies (SACMAT '05). pp. 168–176.

Siau, K. and Rossi, M., 2011. Evaluation techniques for systems analysis and design modelling methods - a review and comparative analysis. Information Systems Journal, 21(3), pp. 249–268.

Vaidya, J., Atluri, V. and Guo, Q., 2007. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles. In Proc. of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT '07). ACM, pp. 175–184.

Van den Berg, B. and Leenes, R., 2011. Keeping Up Appearances: Audience Segregation in Social Network Sites. In S. Gutwirth et al., eds. Computers, Privacy and Data Protection: an Element of Choice. Springer, pp. 211–231.

Venable, J.R., Pries-Heje, J. and Baskerville, R., 2012. A Comprehensive Framework for Evaluation in Design Science Research. In Proc. of the 7th International Conference on Service-Oriented Perspectives in Design Science Research (DESRIST '12). Springer, pp. 423–438.

Watson, J., Whitney, M. and Lipford, H.R., 2009. Configuring Audience-Oriented Privacy Policies. In Proc. of the 2nd ACM Workshop on Assurable and Usable Security Configuration. ACM, pp. 71–78.

Zhao, S., Grasmuck, S. and Martin, J., 2008. Identity Construction on Facebook: Digital Empowerment in Anchored Relationships. Computers in Human Behavior, 24(5), pp. 1816–1836.

Ziegele, M. and Quiring, O., 2011. Privacy in Social Network Sites. In Privacy Online - Perspectives on Privacy and Self-Disclosure in the Social Web. Springer, pp. 175–189.