INFORMATION SECURITY TECHNICAL REPORT XXX (2013) 1–14

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments

*Moritz Riesner**, *Michael Netter*, *Günther Pernul*

University of Regensburg, Universitätsstraße 31, 93053 Regensburg, Germany

Keywords:
Social identity management
SIdM
Social Networking Sites
Online social network
Privacy
Requirements
Privacy settings

ABSTRACT

The rising prevalence of Social Networking Sites (SNS) and their usage in multiple contexts poses new privacy challenges and increasingly prompts users to manage their online identity. To address privacy threats stemming from interacting with other users on SNS, effective Social Identity Management (SIdM) is a key requirement. It refers to the deliberate and targeted disclosure of personal attribute values to a subset of one's contacts or other users on the SNS. Protection against other entities such as the site operator itself or advertisers and application programmers is not covered by SIdM, but could be incorporated in further refinement steps. Features and settings to perform SIdM have been proposed and subsequently implemented partly by some SNS. Yet, these are often isolated solutions that lack integration into a reference framework that states the requirements for successfully managing one's identity. In this article, such a reference framework of existing and desired SIdM settings is derived from identity theory, literature analysis, and existing SNS. Based thereupon, we examine the SIdM capabilities of prevalent SNS and highlight possible improvements. Lastly, we reason about developing a metric to objectively compare the capability of SNS in regards to their support for SIdM.

1. Introduction

Social Networking Sites (SNS) on the internet are of increasing importance both in personal and professional life. According to an often-cited definition, these sites, such as *Facebook*, allow users to create personal profiles, express connections with other users and traverse the resulting social graph (Boyd and Ellison, 2007). Through their rising pervasiveness and the use of sensitive data such as geospatial information, SNS have also prompted privacy concerns. Besides the often discussed SNS providers' handling of user data, privacy concerns also need to consider the user's contacts (Ziegele and Quiring, 2011).

The need for settings that enable personal *Social Identity Management* (SIdM) has been pointed out by multiple authors (Farnham and Churchill, 2011; Lipford et al., 2009). SIdM refers to the deliberate, targeted disclosure of personal attribute values to a subset of one's contacts on SNS. From a social science perspective, the need for SIdM stems from each individual performing multiple and potentially conflicting roles in everyday life (Goffman, 1959). To keep a consistent self-image, audiences for each role performance need to be segregated in a way that people from one audience cannot witness a role performance that is intended for another audience. Maintaining consistent self-images is also referred to as contextual integrity (Nissenbaum, 2010).

* *Corresponding author.*
E-mail addresses: moritz.riesner@wiwi.uni-regensburg.de (M. Riesner), michael.netter@wiwi.uni-regensburg.de (M. Netter), guenther.pernul@wiwi.uni-regensburg.de (G. Pernul).

1363-4127/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.istr.2013.02.005

Desirable settings for SIdM, such as grouping one's contacts into audiences for later attribute disclosure have previously been described in detail (van den Berg and Leenes, 2010). Often, such settings have subsequently been implemented by SNS. For instance, automated proposal of homogenous audiences was presented in (Netter et al., 2011) and has later been adopted by SNS.

While being described in several publications and implemented partially, SIdM settings are hard to classify and to compare across various SNS. Moreover, it is a difficult task to evaluate an SNS' overall capabilities regarding SIdM. This is due to semantic differences of the information posted on SNS, and subsequently, of the particular SIdM settings. There are publications that apply access control models to SNS (Carminati et al., 2011), which provide an exact description of a usually fictional SNS' SIdM settings. While providing an accurate and precise description of a desired access control scheme, they are however often hardly applicable to the reality of current SNS (Grimmelmann, 2009). These issues underline the need for a provider-independent reference framework to compare existing and future SNS regarding their SIdM capabilities.

This article is an extended version of a paper that was accepted to the ARES-conference in 2012 (Riesner et al., 2012). It has been extended under consideration of the helpful reviewer comments and the discussion at the conference venue. Its contribution is twofold: First, we analyze literature related to SIdM settings as well as settings that are implemented in established SNS. Then, we derive a reference framework for existing and desired SIdM settings. The framework is suitable to analyze and compare the extent to which SNS support SIdM and is based on four high-level requirements for SIdM. In this extended version, the connection between the literature and the requirements is expressed in more detail. Also, the settings themselves are described more thoroughly. Secondly, we evaluate a set of selected SNS using the reference framework to demonstrate its applicability and to highlight possible improvements of their SIdM settings. Lastly, in this extended version, we propose an approach for developing a metric to quantify the SNS' support for SIdM.

The remainder of this article is structured as follows. After describing related work in Section 2, Section 3 addresses our research approach. In Section 4 we derive general requirements for SIdM from literature. In Section 5 we develop a reference framework for SIdM settings by matching these requirements with particular SIdM settings that are already implemented in SNS and discuss desirable advancements. Section 6 surveys selected SNS using the reference framework. We discuss a metric for assessing the SIdM capabilities of an SNS in Section 7, followed by the conclusion of the article in Section 8.

2. Related work

Multiple authors argue that privacy is a growing concern as SNS usage has increased over the years (Irani et al., 2009; Borcea-Pfitzmann et al., 2011). Two major threats to privacy can be distinguished, stemming either from SNS service providers or other SNS users (Ziegele and Quiring, 2011). This article focuses on the latter, which aims at managing social identities consistently to avoid privacy breaches. While this bears resemblance to managing different appearances of the self in the real world, research shows that it is difficult to transfer real-world strategies to the online world (Tufekci, 2008) due to inherent properties of mediated communication such as persistence and searchability.

To mitigate these issues, a variety of identity management and access control concepts have been published. A prototypical SNS that allows for creating multiple personas and audiences is shown (Leenes et al., 2010). Furthermore, SNS-specific access control models have been proposed that aim at improving targeted sharing of personal information (Carminati et al., 2011; Ali et al., 2007; Netter et al., 2012). Other works aim at aiding the users in their social identity management, for instance by suggesting contact groups for disclosure (Fang and LeFevre, 2010; Netter et al., 2011) or by automatically anonymizing unstructured texts and watermarking it to detect unauthorized disclosures (Nguyen-Son et al., 2012). While these works make valuable suggestions for the improvement of SNS' SIdM capabilities, this work focuses on structuring SIdM settings and evaluating the current SNS support for SIdM.

Studying the usage of privacy settings is another related research area. Publications focus on aspects such as quantifying incorrect privacy settings (Liu et al., 2011; Netter et al., 2013; Madejski et al., Mar. 2012), examining to which extent users understand privacy settings and their impact (Strater and Lipford, 2008), assessing usage strategies of privacy settings (Kelley et al., 2011; Watson et al., 2012), and predicting user attitudes from privacy settings (Lewis et al., 2008). In contrast, this work takes a more abstract point of view, aiming to determine the settings required to conduct successful SIdM.

From a practical perspective, SNS service providers have introduced a variety of settings, for example to limit the visibility of one's profile. Bonneau and Preibusch (2009) examine privacy settings of several SNS with regard to visibility and access controls, but their focus is much wider than SIdM and several of the settings identified in our work were not addressed. In another work (Ulbricht and Abraham, 2012), privacy settings are analyzed from a service provider point of view, while in contrast this work takes a user perspective. Krishnamurthy and Wills (2008) cluster personal information on SNS and discuss differences in privacy controls between several SNS regarding these clusters. Settings regarding information disclosure to contacts play only a minor role in their work and most of the advanced SIdM features discussed in our work were not implemented at the time of their publication. Additionally, a taxonomy to describe social networking data in privacy discussions has been introduced (Schneier, 2010). A legal analysis of privacy settings is provided by Kuczerawy et al. (2011).

Our work differs from the aforementioned works due to its clear focus on SIdM, which concerns the information disclosure to online contacts. Also the discussed SIdM settings are aligned by a reference framework which is based on well-defined requirements that need to be fulfilled for successful SIdM. Additional related work regarding social identity management is discussed in Section 4, which aims at elicitating requirements from literature.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

3. Research model

Our research is based on the model shown in Fig. 1. First, we derive high-level requirements for SIdM from literature, which is described in more detail in Section 4 (step (1) in Fig. 1). Relevant literature includes work from other research areas that can be applied to SNS, for instance social identity theory from the social sciences. Publications that propose improvements for the SIdM that is implemented in current SNS are also part of the analysis.

Step (2) is presented in Section 5 and aims at deriving a reference framework for particular SIdM settings and features that can be implemented in SNS. For each high-level requirement from Section 4, we identify and describe corresponding SIdM settings or features that are suitable to satisfy it. The origins of these features vary: Mostly they were observed as implemented on one or more of the existing SNS. Other settings and features were proposed in analyzed literature or, as a result of the analysis, by the authors of this work as a possible solution to improve fulfillment of the previously stated high-level requirements.

The particular settings and features for SIdM are grouped by the high-level requirements presented in Section 4, resulting in a structured catalog. It forms a reference framework that is suitable for the evaluation of the extent to which particular SNS support SIdM. Thus the contribution of this work lies not only in presenting particular settings necessary for SIdM, but also in a reference framework that can be adapted to future developments, for instance the introduction of new SIdM features.

Our approach is to make the reference framework independent of particular SNS implementations while describing SIdM settings in a fashion that makes them applicable to current and future SNS. While an accurate and precise description is necessary to enable a clear decision whether the setting is provided by an SNS or not, the description must also be fairly generic to be widely applicable.

Further in Section 6, we apply the reference framework to a selected number of SNS to evaluate and compare their support for SIdM, leading to a qualitative assessment (3). This is exemplified in Fig. 1 through pie-symbols which indicate the degree of fulfillment for a certain SIdM feature. This analysis serves as a validation for the developed reference framework. It allows to draw conclusions on whether the identified SIdM settings and their descriptions are actually applicable or if there is need for adjustment. Thus, the approach has an iterative character allowing for further improvement and for adapting to future developments. Lastly, we reason about extending our research by developing a metric to analyze the SIdM support of SNS quantitatively.

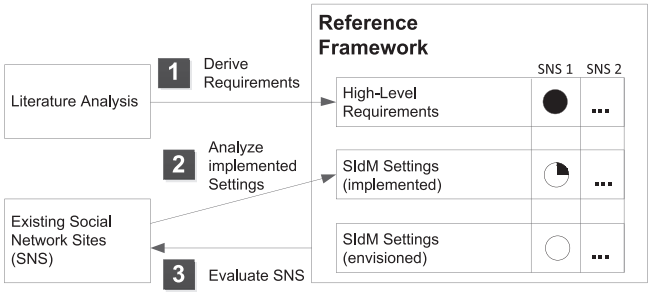

Fig. 1 – Research model.

4. SIDM requirements from literature

In this section, we derive requirements for SIdM from literature. Note that while it is difficult to arrive at an exhaustive list of requirements, we are confident to cover the most important aspects regarding SIdM. This will be the basis for a subsequent analysis of SIdM functionality in SNS as presented in Section 5. This analysis is decoupled from actually implemented SIdM features to avoid limitations that would arise from only looking at the status quo.

Revisiting SIdM, it can be regarded as a concept that mainly builds upon two theories: Social identity and privacy theory. While the former refers to conveying a *favorable* image of the self to a particular audience, the latter aims to present a *consistent* self-image. In the following, the theoretical foundations of both theories are outlined, constituting the basis for elicitating requirements for successful SIdM.

Identity theory consists of a variety of theories to describe the construction and management of social identities. From an interactionist perspective, identities are constructed and reshaped through interaction with other people. According to Goffman's (1959) concept of impression management, a person performs different roles to present an image of the self which is favorable for the current situation. A controlled self-representation involves two parties, namely the individual performing a particular role and an audience which reacts to the performance (Bilbow and Yeung, 2010). To adapt one's performance to an audience, impression management allows for having multiple, potentially conflicting roles that are bound to different social contexts. This conceptualization of identity can be applied to SNS since the primary functions of these sites are impression- and relationship management (Boyd and Ellison, 2007).

Besides impression management, a major focus of SIdM is on privacy, i.e. to present an image of the self which is appropriate in a given context and to respect the social norms of this situation. In more detail, privacy here refers to Nissenbaum's (2010) concept of contextual integrity, making a distinction between appropriateness and distribution of shared personal information. Privacy is violated if either of both terms is ignored. Appropriateness refers to only disclosing personal information which is acceptable in the current situation, taking existing social norms and present people into consideration. For instance, information shared with fellow students may be inappropriate when talking with one's grandparents. By distribution, the author states that privacy is violated if shared personal information leaves its intended context and becomes available in another context, e.g. by health-related information appearing in a work context. In the following, we derive requirements for SIdM in SNS based on this conceptualization (Table 1).

As shown in the previous paragraphs, identities are constructs rather than ready-made essences (PrimeLife, 2010), which are shaped in social interaction with others. Thus, an essential requirement for successful social identity

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

Table 1 – High-level requirements for SIDM derived from literature.

No.	Requirement	Sources
1	Unrestricted identity creation and control	(Goffman, 1959; Agre and Rotenberg, 1998; Rouvroy, 2008)
2	Create and maintain multiple representations of the self	(Goffman, 1959; Peterson, 2010; DiMicco and Millen, 2007; Binder et al., 2009)
3	Create and maintain multiple social circles	(Goffman, 1959; Lampinen et al., 2009; Palen and Dourish, 2003)
4	Contact permission assignment	(Farnham and Churchill, 2011; Tufekci, 2008; Peterson, 2010; Mayer-Schönberger, 2009)

management in SNS is to provide means for *unrestricted identity creation and control* over the presentation of self on a specific platform ((1) in Table 1). From a privacy perspective, Agre and Rotenberg (1998) argue that privacy can be seen as "*(…) the freedom from unreasonable constraints on the construction of one's own identity.*" In more detail, it "*(…) protects lawful, but unpopular, lifestyles against social pressures to conform to dominant social norms. Privacy as freedom from unreasonable constraints in the construction of one's identity, serves to prevent or combat the 'tyranny of the majority'.*" (Rouvroy, 2008) On a technical level, the user should be able to use both predefined and custom personal attributes and their values and be able to change them to reshape his identity. Additionally, the user should be able to approve or deny non-user generated content that relates to his identity such as links to his identity on pictures uploaded by others. Also, means to view one's representation of self as it appears to others are necessary.

A second requirement results from the fact that people act in different roles to adapt themselves to different social situations. Similarly, SNS evolve from single- to multi-purpose platforms, where contacts from different social contexts are present at the same platform (DiMicco and Millen, 2007). As a result, the problem of conflicting social spheres emerges (Binder et al., 2009), stating that it is difficult to simultaneously meet the expectations of multiple audiences. For instance, in terms of Goffman's impression management, at the same time playing the role of a caring husband, a professionally acting employee, and a capricious friend on a single SNS might be difficult. Hence, the requirement for being able to *create and maintain multiple representations of the self (2)* gains importance. In more detail, users of SNS should be given the possibility to create an arbitrary number of partial identities, also known as personas on the same platform (Peterson, 2010). Additionally, users should be able to keep these identities separated if desired as some identities might be conflicting. For instance, in a personal social setting, one might wish to appear more outgoing than in a strictly professional setting, and the attributes chosen for each situation may be contradictory.

Based on Goffman's conceptualization, identities are selected according to the situation a user is currently in, which is to a large extent defined by present people. Thus, a further requirement for social identity management in SNS is to *create and maintain multiple social circles (3)* which are both the audience and the decision-making basis for choosing an appropriate identity (Lampinen et al., 2009). Within an SNS, it should be possible to partition the user's contacts into different, potentially overlapping groups (Peterson, 2010). However, unlike in the real world, in SNS social circles are not inherently present but instead only a single list of contacts exists at the beginning (Palen and Dourish, 2003). Thus, there is a need for assisting the user in grouping contacts into social circles, which has been highlighted by several researchers (Kelley et al., 2011; Madejski et al., 2011) and also implemented in applied research (Netter et al., 2011).

Lastly, *contact permission assignment (4)* is a further requirement for social identity management that emerges due to the fact that the majority of communication on SNS is asynchronous and results in combining the notions of *(2)* and *(3)* to govern access to the user's online identities. On a technical level, access control models are needed to map contacts to personal attributes and assign permissions. SNS should provide means to enable the user to share different identity representations with different contacts, i.e. provide read permission to selected contacts for specific personal attribute values (Farnham and Churchill, 2011). Note that for achieving selective information disclosure, neither explicit modeling of different identities (2) nor explicit expression of social circles (3) is strictly necessary. Selective information disclosure can still be achieved by assigning the visibility of certain attribute values to single contacts. Upon closer examination, contact permission assignment also extends to controls over how others shape one's identity. In SNS, settings for more extensive permissions (e.g. write permissions) need to be in place, for example to control comments by others on the user's profile, which might convey an unintended identity impression.

Unlike Goffman's concept of role performances that can only be witnessed by the present audience, the persistence of personal information – an inherent property of digitally mediated communication – shifts temporal and spatial boundaries (Tufekci, 2008). In SNS, audiences can be distant, invisible, and may exist in the future. However, Peterson argues that people rely on real-world heuristics to estimate personal information distribution which leads to the need for advanced controls for permission assignment for online SIdM (Peterson, 2010). For example, SNS need to provide technical means to allow for forgetting personal information as in the real world, e.g. by automatically changing the visibility of information based on its age (Mayer-Schönberger, 2009).

5. Implemented and desirable settings to fulfill SIDM requirements

Following our research model, in this section we match the requirements derived in the previous section with particular

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

SIdM settings that are either already implemented in SNS or can be described as desirable advancements. Settings that are not indicated as being introduced in this work or other literature were observed in current SNS.

Fig. 2 shows the scope of the requirements identified in Section 4. It contains the main concepts within an SNS that are of concern for the user who is conducting SIdM. Depicted on the left hand side is the user's profile, which can be seen as the technical implementation of the user's representation of self. It may be broken down into *personas* that are subsets of the profile and the technical pendent to partial identities. Depicted on the right hand side are the user's contacts. Permissions governing the relationship between profile content and contacts are shown in the middle of Fig. 2. The user profile and permissions lie in the user-manageable domain, meaning that the SNS user is in control over them. Also shown in the user-manageable domain are representations for each contact that are used to assign permissions.

Hence, all SIdM requirements derived in the previous section concern the user-manageable domain. Even here, user control may be limited by available settings within the SNS. The user may be able to perform changes on other contacts' profiles as well, thus extending the user-manageable domain beyond one's own profile. This is however not depicted in Fig. 2 because this work is only concerned with the management one's own identity on SNS. Changes made by the user in question would lie in the manageable domain of the contact and is thus not relevant here.

Note that corresponding to the term *social* identity management, this work is only concerned with managing one's online identity in regards to other users of the SNS. Further actors such as the site operator, advertisers or application providers are not explicitly considered. Yet, the model could be extended to actors by considering them as a special type of contact and analyzing whether SIdM settings are applicable to them. It is however questionable whether SIdM controls provided by the site operator can reasonably protect against said operator.

Each of the following subsections addresses one of the requirements identified in Table 1. To describe interdependencies between SIdM features, we use the following relationships:

- *a* refines *b*: the functionality of feature *a* refines that of feature *b* and improves its quality. Feature *b* could function without feature *a*, but not to its fullest extent.
- *a* extends *b*: the functionality of feature *b* is complemented by feature *a*, but the quality of feature *a* would not be compromised by the absence of b.
- *a* is alternative for *b*: feature *a* replaces the compete or partial functionality of feature *b*, however not necessarily with the same quality.

5.1. *Unrestricted identity creation and control*

SIdM settings and related properties regarding *unrestricted identity creation and control* describe to what extent users are able to create and shape their SNS profile and to control its contents as they wish. We acknowledge that there are always limitations to the extent that the users' may shape their online representation, possibly not only through restrictions by the SNS, but also by technical boundaries, such as bandwidth and screen resolution.

We see the user's SNS profile as the set of all properties or attribute values of that user in the SNS that may be disclosed to contacts or other entities. Table 2 identifies four SIdM settings directly related to the user's control over the attributes within the profile.

First, the user should be the final authority over each attribute's value (Setting 1a). This concerns especially user data that is not deliberately entered by the user. For instance, the SNS platform may automatically add information to the profile based on user activity. Other limitations occur when there is only a predefined set of possible values for an attribute, or when the values have to be verified. Related to this property is the possibility of users leaving the attribute values empty as they wish (1b). Table 2 denotes the scope for which a setting is applicable: Settings 1a and 1b for instance may not be available for all attributes in the SNS. Instead it is possible that they are only available for certain attributes. The availability of the following settings 1c and 1d on the other hand does not have to be defined for each attribute. Also, dependencies between available settings are denoted in the rightmost column of the table. Setting 1b is refined in 1a, because one doesn't have complete control over an attribute value if it can't be set as empty.

It is conceivable that the control over one's representation of self exceeds merely filling out predefined fields that are

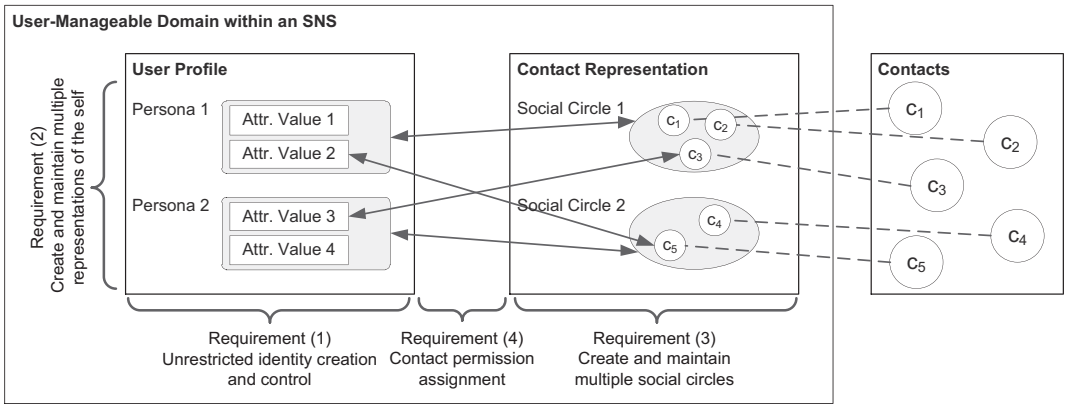

Fig. 2 – Scope of the requirements and settings analysis.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

Table 2 – Settings for requirement 1: unrestricted identity creation and control.

No.	SIdM setting or feature	Availability	Scope/target	Dependency
1a	User has control over attribute value	Yes/no	For each attribute	Refined by 1b, extended by 1c–d
1b	User may leave attribute value empty	Yes/no	For each attribute	Refines 1a
1c	User may define and use custom attribute types	Yes/no	User profile	Extends 1a
1d	User may view how profile appears to others	Yes/no	User profile	Extends 1a

provided by the SNS. While creating one's profile completely from scratch similarly to a personal web page is not feasible in a structured environment such as an SNS, we suggest that control over one's online representation could be increased through users being able to freely add custom attribute types to their profile (1c).

As stated before, depending on the SNS, settings 1a and 1b may only be available for some attributes. It is also possible in particular SNS that a setting is only available for certain attribute categories. This possible dependence between available SIdM settings and the implementation of certain attributes in a particular SNS merits further analysis of the implementation of profile elements for each SNS (Riesner and Pernul, 2012). As such an analysis is very implementation-dependent, it is performed together with the provider survey in Section 6, where necessary.

Lastly, for control over their profile, users also need to be able to view whether their settings and modifications were applied as desired (1d). This concerns settings regarding attribute types and values as well as the disclosure settings that are discussed further below. Also known as *privacy lens* (Aïmeur et al., 2010) or *mirror*, the related SIdM feature shows how the user's profile appears from the point of view of others, such as a particular contact or the public.

5.2. *Create and maintain multiple representations of self*

Creating multiple representations of self refers to allowing the user to perform several roles on a single SNS in order to adapt to different social situations. In SNS, such roles could be implemented through personas which we see as a subset of all attribute values of a user profile in a given SNS. Table 3 lists three SIdM settings to achieve multiple personas in an SNS.

Setting 2a is the most exhaustive one and uses the explicit construct of a persona (Leenes et al., 2010). It allows users to create multiple personas by grouping attribute values. We see its scope as being dependent on the attributes, as it may be possible to allocate only some of one's attributes to personas while other attributes remain part of a base-persona that cannot be shared selectively. A further possible restriction may lie in the number of personas that one is able to create.

Even when the construct of dedicated personas is not available, multiple representations of self may be achieved implicitly through selecting the target audience for each individual attribute value (Setting 2b). Here, the availability of the setting may also not be available for all attributes, thus the scope is again defined as *for each attribute*.

Setting 2c extends the former settings by explicitly addressing the possibility to disclose different, possibly contradictory values for the *same* attribute.

Currently, the most prevalent way of achieving multiple representations of self consists of utilizing SIdM setting 2b or, if unavailable, through creating multiple accounts at one or more SNS. Note that this section only addresses the content that is to be disclosed. The actual disclosure has to consider the granularity of available access control settings, possible audiences and is discussed in the first two items of Section 5.4.

5.3. *Create and maintain multiple social circles*

The selective disclosure of personas or only a subset of one's attribute values as discussed in the previous section requires means to determine to whom such profile elements should be disclosed to.

One construct to specify such an audience for one's attribute values is grouping one's contacts into *social circles* which can in turn be used for selective attribute disclosure. It is denoted by SIdM setting 3a in Table 4. The target for this setting is the set of the user's contacts. Similar to the number of personas, it is conceivable that the number of social circles

Table 3 – Settings for requirement 2: create and maintain multiple representations of the self.

No.	SIdM setting or feature	Availability	Scope/target	Dependency
2a	User may allocate attribute values freely to personas	Yes/limited number of personas/no	For each attribute	Extended by 2c, refines 4b
2b	Implicit multiple representations of self through selective disclosure of attribute values	Yes/no	For each attribute	Partial alternative for 2a, extended by 2c, refines 4b
2c	User may disclose different values for the same attribute to different contacts	Yes/no	For each attribute	Extends 2a, 2b

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

Table 4 – Settings for requirement 3: create and maintain multiple social circles.

No.	SIdM setting or feature	Availability	Scope/target	Dependency
3a	User may group contacts to form social circles	Yes/limited number of circles/no	Contacts	Refined by 3b, extended by 3c, refines 4a–d
3b	Social circles may overlap	Yes/no	Circles	Refines 3a, 4a–d
3c	SNS assists user with creating circles	Yes: smart list suggestions/yes: attribute-based lists/yes: advanced user interfaces/no	Contacts, circles	Extends 3a, 4d

is limited. Also, akin to personas, even if there is no explicit construct to create social circles, groups of contacts that are able to view the same attribute values can be considered as implicit social circles or audiences. An example for the friend list management on the site Facebook is illustrated in Fig. 3.

Setting 3b denotes whether social circles may overlap, meaning that one contact may be the member of two or more circles. Such a feature would extend the expressiveness of setting 3a by allowing users to express that some of their contacts are part of multiple areas of their life. If overlapping circles are not available in the SNS, the users may resort to creating a third circle consisting of those contacts that are part of both existing circles and disclosing attributes accordingly.

Finally, as nowadays many SNS users have several hundred contacts (Kelley et al., 2011), grouping all of them into circles may become a tedious task. Setting 3c indicates whether the SNS provides means to assist the user with allocating contacts to circles. There are multiple possible means of assistance. Sophisticated approaches suggest complete contact lists to the user based on the contacts' attributes or relationships among them (Netter et al., 2011). Intuitive user interfaces such as advanced visualizations of one's circles or drag and drop-commands can also be considered as assistance for grouping contacts. Fig. 4 shows the approach on the site Google+, employing a dynamic visualization of social circles in conjunction with a drag and drop interface.

5.4. *Contact permission assignment*

Building on the previous two subsections and referring to requirement 4 in Table 1, we discuss SIdM settings allowing the allocation between permissions and contacts or other entities in this section. First, we introduce possible targets for the assignment of permissions beyond the previously discussed social circles. Then we analyze permissions, which refer to contacts being allowed either to read or to manipulate certain attribute values in the user's manageable domain. This is followed by a discussion of advanced controls for permission assignment. The settings are summarized in Table 5.

5.4.1. *Possible targets for permissions*

Permissions to read or modify attribute values in the user's profile may not only be assigned to social circles as discussed in Section 5.3. Fig. 5 shows further possible settings for targets that permissions can be assigned to. They are ordered from very large audiences to small ones.

The broadest and least restrictive setting is *all internet users*, making the permission available to the public. The setting *all SNS users* grants the permission only to registered users of the SNS, which is of marginal difference, as signing up at most SNS is free. Still, it may prevent automated requests by search

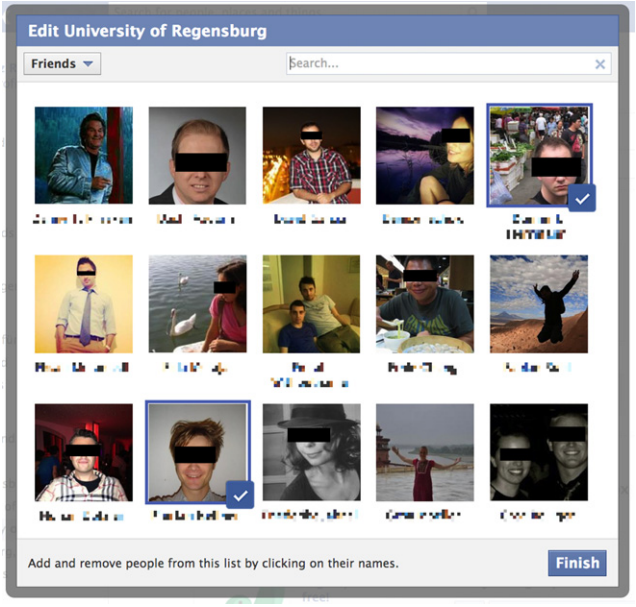

Fig. 3 – Friend lists on Facebook.

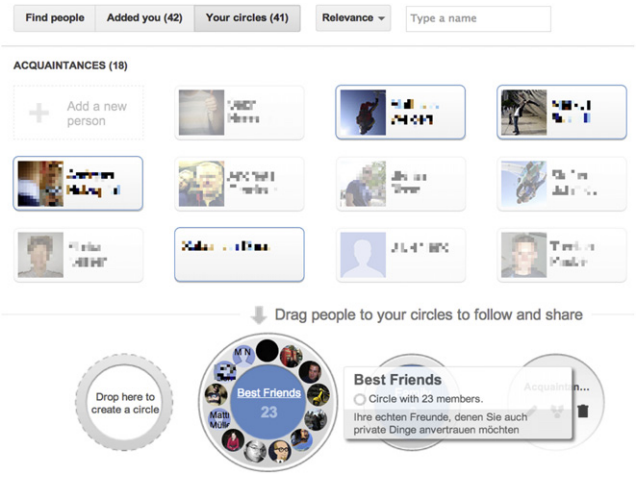

Fig. 4 – Social circles in Google+.

Table 5 – Settings for requirement 4: contact permission assignment.

No.	SIdM setting or feature	Availability	Scope/target	Dependency
4a	Possible targets for permissions (set T)	Refer to Fig. 5	Users of the SNS and the public	Refined by 3a–b, extended by 3c, refines 4b
4b	Fine grained sharing decisions for attribute values A	$SD = \{A \times T\}$, consider restrictions	Sharing decisions	Refined by 4a, 3a–b, 2a, 2c, extended by 4e–f
4c	Control how contacts can shape the user's profile	$T \times$ {allow, individual approval, deny}	Permission granting decisions (modifications)	Refined by 3a–b, extended by 3c
4d	Control incoming references to the user's profile	$T \times$ {allow, individual approval, deny}	Permission granting decisions (incoming references)	Refined by 3a–b, extended by 3c
4e	Time-based sharing decisions	No/expiry date for posted items/tool to delete older items (for each attribute)	Granted permissions to view attributes	Extends 4b
4f	Limit the number of accesses of information items	Yes/no (for each attribute)	Granted permissions to view attributes	Extends 4b

engines and the like. A little bit more restrictive, permissions may be granted to other users based on their *attributes*, for instance their place of education. However, it has to be considered that an access control decision based on attributes of the subjects is potentially weak, if they are able to change such attributes themselves. Hence it has to be considered whether there are means of verification for such attributes or if they can be chosen freely by the other user.

The *friend of a friend (FoaF)*-setting grants a permission to all contacts of the user's contacts. It may be extended further, for instance to contacts of the second or third degree. These broadest possible settings assign permissions to other entities beyond the user's set of contacts. The latter two settings limit that number of entities to a certain degree. Yet, it is beyond the user's control, which individuals in particular are actually granted a permission and using these settings, it is unlikely to anticipate the exact set of individuals that are granted a permission.

As shown in Fig. 5, we suggest a setting *friends of some friends* to reduce the reach of the regular FoaF-Setting. Using such a setting, the user could define a very limited set of contacts whose contacts are then granted the permission in turn. The regular FoaF on the other hand, would grant the permission to the contacts of all of the user's contacts.

The setting granting permissions to *all contacts* is very common and often the predefined disclosure setting. However, with users having more than a hundred contacts, such a setting grants permissions to a very broad group of individuals and the probability of unintended information disclosure rises.

The user has even more control when granting a permission only to *subsets* of her contacts. Defining such subsets may be performed either manually or using constructs like social circles as discussed in Section 5.3.

Another aspect that isn't considered by currently implemented settings for information disclosure is the intended audience for information that has been posted by the user's contacts. While current settings may allow the user to predefine a static audience for information posted by contacts, this setting doesn't consider *by whom* this information was posted. This information may in fact be relevant, as information posted by a contact may for instance only be intended for contacts that are in the same circle. To incorporate this information, we propose the setting *within circle* that limits the visibility of such content only to contacts that are in the same circle of the contact that created the content.

The settings *only self* and *deleted* don't assign permissions to any third entity and are shown for the sake of completeness

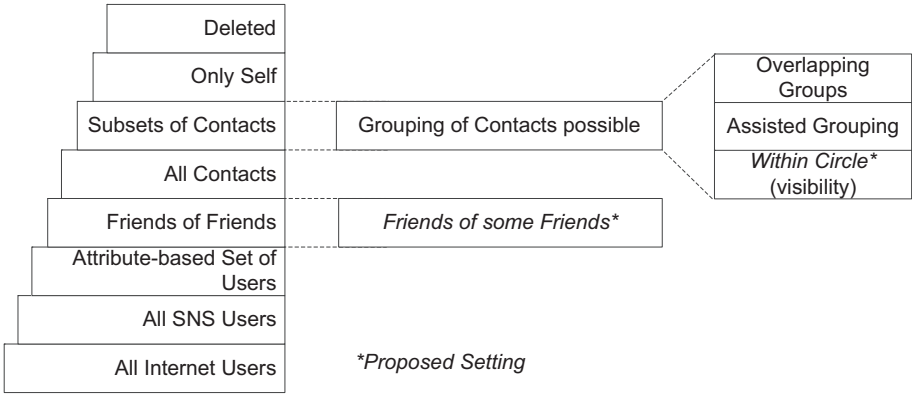

Fig. 5 – Possible targets for permissions.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

only. *Deleted* refers to attribute values that are no longer stored in the SNS.

5.4.2. *Fine grained sharing decisions for attribute values*

Fine-grained sharing decisions for attribute values means that the user should be able to make decisions regarding the disclosure of profile attributes with as few limitations and as fine-grained as possible. To state this more precisely, we introduce a set A containing all attribute values from the user's profile. If the construct of personas is available in the SNS, they are also included in A. Next, consider a set T that includes all targets for permissions that are available through available SNS settings. For instance, if the SNS allows distinguishing between subsets of contacts, every contact is part of T. If the construct of social circles is available, each circle is also part of T.

Trivially, the disclosure settings are limited by the available items in A and T. But there may be even more limitations regarding the sharing settings. Precisely, let us specify a set of binary sharing decisions SD that can be enumerated by the Cartesian product $SD = \{A \times T\}$. SD contains every possible combination of an attribute value and a disclosure target. The user has no limitations in her disclosure decisions when she is able to make an individual, independent sharing decision for every element in SD.

Such limitations may occur when the sharing decision for elements in SD cannot be changed by the user. In most SNS for instance, the profile picture is always set to be visible to the public, thus the sharing decision for the tuple *(profile picture, all internet users)* is always *true* and cannot be changed.

Further limitations occur when the decisions for several elements in SD cannot be made separately, implying that a sharing decision can only be applied to a group of attribute values and not to individual values. For instance, in some SNS, the visibility setting of comments made by contacts on a certain item are inherited from that item and cannot be modified separately. Note that some elements in SD are dependent on other elements not due to restrictions posed by the SNS, but because elements in A and T may intersect with or include other elements.

5.4.3. *Control how contacts shape the users profile*

There are two possibilities of how contacts may shape the user's profile and thus her identity on SNS.

One of them are SNS-features that allow contacts to post text messages or multimedia items to the user profile. Such items may be posted independently or as a comment to an existing object. SIdM settings determine whether a contact is allowed to post items to the user profile. As stated by setting 4c in Table 5, SIdM settings should enable the user to control items posted to the user's profile. If posted as a comment, items may inherit the visibility setting of the parent object. For other posted items, treating them as regular attribute values allows applying the line of thought presented in the previous section.

Another way for contacts and even other users of the SNS to shape the user's online profile is by referencing it from entries in their own profiles. Often also known as *tagging* or *linking*, such a reference provides a shortcut to the user's profile, for example for identification of a person in a picture. As the reference is created in another user's profile, it exists outside of the user's manageable domain and is not influenced by visibility settings of the user that is referenced. However, depending on the SNS, settings that prohibit other users from creating incoming links may exist (4d). Incoming references may be controlled indirectly by restricting direct access for visitors of the user profile.

Note that due to the technical implementation of SNS, user profiles are represented by alphanumerical strings and often also by URLs that are accessible to at least all SNS users. Thus, in most cases, SIdM settings cannot effectively prevent creating incoming references on a technical level, but they can reduce the convenience of doing it.

5.4.4. *Advanced controls for permission assignment*

We suggest the following advanced controls for permission assignment to add additional dimensions to the user's sharing decisions.

As suggested in Section 4, time-based considerations may play a role for sharing decisions, as information that was added to the profile in the past may not accurately reflect the user's currently desired presentation of self. A strong SIdM setting to incorporate the time-based dimension into sharing decisions is to assign a (possibly default) expiration date to each attribute value that is added to the user's profile (4e). After that date has passed, the attribute value is either removed or the user is asked to extend its lifetime. A somewhat similar but weaker, manually-invoked SIdM function that has been implemented by Facebook, checks and possibly alters the audience of posted items that have passed a certain age.

A further dimension that is conceivable to be incorporated into sharing decisions would limit the number of times the user profile may be accessed (4f). Such a setting could enable other SNS-users to find and view the user's profile for purposes of identification and contact initiation. They would however be prevented from repeatedly monitoring that profile without consent of the user. Note that information might be copied while available, but advanced controls limit the general availability of that information.

6. Provider SIDM survey

We applied the reference framework presented in the previous section by surveying five selected SNS for SIdM support.[1] We chose the SNS Facebook and Twitter due to their high number of members and their international importance both in the public perception and in academic publications. Google+ was selected due to its widely noticed introduction in mid-2011 and its focus on privacy controls. While Google+ and Facebook can be classified as general purpose-SNS, LinkedIn serves as an example for a smaller, still popular SNS that focuses on a particular topic, namely managing business relationships. Finally, we chose Diaspora as a representative for the decentralized SNS-paradigm. The survey results are

[1] Websites of the surveyed SNS: http://www.facebook.com, http://www.twitter.com, https://plus.google.com, http://www.linkedin.com and https://joindiaspora.com/; Survey conducted on March 19–23, 2012.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

summarized in Table 6, structured by the four high-level requirements for SIdM identified earlier.

Before we discuss the most interesting observations in the study, we want to give a refined definition of the concept of attributes and attribute values in conjunction with SNS. So far, for simplification purposes, we used the term *attribute value* uniformly to describe any information object within the user's profile. However, we also stated that there are differences in how attributes are implemented within and between SNS. In the survey we observed that in many cases the availability of SIdM settings depends on how the attribute is implemented. Thus, for a precise analysis of the SNS' SIdM capabilities we need to distinguish further between different attribute categories found in SNS.

We identified three major categories of attributes, which are applicable to all surveyed SNS. First, *single value-attributes* refer to a fixed attribute that is part of the user's profile and can be assigned at most one value. They are often used for static information that changes only rarely or never such as the user's birthdate or elements of the address. On the other hand, for *multi value- attributes*, the user may enter several entries. Examples of multi value-attributes are lists of favorite books or past employers.

In contrast to these two types, we see *posted items*, which are not assigned to fixed regular attributes such as *birthdate* or *favorite books*. Rather, for each user, there is a dynamic log of posted items with new items being created at the top. Depending on the SNS, posted items are for instance short

Table 6 – Survey of SNS and classification into the reference framework for SIdM.

No.	Requirement/SIdM Setting or Feature	Google+	Diaspora	LinkedIn	Twitter	Facebook
1	***Unrestricted identity creation and control***	◕	◑	◑	◑	◑
1a	User has completed control over attribute value	●	●	●	●	◑
1b	User may leave attribute value empty	◕	●	◑	●	◕
1c	User may define and use custom attributes types	○	○	○	○	○
1d	User may view how profile appears to others	●	○	○	○	●
2	***Create and maintain multiple representations of the self***	◔	◔	○	○	◔
2a	User may allocate attribute values freely to personas	○	○	○	○	○
2b	Implicit multiple representations of self through selective disclosure of attribute values	◕	◑	◔	○	◕
2c	User may disclose different value for the same attribute to different contacts	○	○	○	○	○
3	***Create and maintain multiple social circles***	◕	◕	◔	○	●
3a	User may group contacts to form social circles	●	●	◔	◔	●
3b	Social circles may overlap	●	●	n/a	n/a	●
3c	SNS assists user with creating circles	○	○	◔	○	●
4	***Contact permission assignment***	◑	◔	◔	○	◑
4a	Possible targets for permissions (set *T*)	◕	◑	◔	◔	◕
4b	Fine grained sharing decisions for attribute values *A*	◕	◑	◔	○	◕
4c	Control how contacts can shape the user's profile					
	New item	n/a	n/a	n/a	n/a	◑
	Comment on existing item	◑	◑	◑	n/a	◑
4d	Control incoming references to the user's profile	●	○	n/a	○	◕
4e	Time-based sharing decision	○	○	○	○	◔
4f	Limit the number of accesses of information items	○	○	○	○	○

Support of SIdM setting or feature by SNS: ● full ◕ with minor limitations ◑ partial ◔ very limited ○ none.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

texts (*status updates*), pictures or multimedia items and often allow appending additional information such as the current location, a reference to SNS users or comments.

6.1. Unrestricted identity creation and control

The surveyed SNS allow identity creation and control by the user that is mostly unrestricted, albeit with a few exceptions. Google+ is slightly superior than the other sites mostly due to more liberal requirements on mandatory attributes. Generally, users have complete control over their attribute values among the surveyed SNS. Yet we observed that on Facebook, editing one's single- or multi value-attributes is automatically announced to the contact by a corresponding posted item. It is created for the user and has to be removed manually, if undesired. None of the SNS allow custom, user-defined attributes, thus restricting the contents of the profile to the predefined scheme.

6.2. Create and maintain multiple representations of the self

Multiple representations of self, referring to the explicit creation and management of multiple personas, are not directly supported by any of the surveyed SNS and can be achieved implicitly at best. When performed through selective disclosure of single- or multi value-attributes, it comes at the cost of being only able to use at most one value (set) per attribute among various personas. This is because none of the SNS supports SIdM setting 2c, which refers to the ability to disclose different values for the same attribute to different contacts. Thus, at this time, creating and maintaining complete distinct and independent personas is only possible through creating multiple SNS-accounts.

6.3. Create and maintain multiple social circles

The SNS support for managing multiple social circles is generally better than that for multiple representations of self. Google+, Diaspora and Facebook all provide constructs to group contacts that may be used for later permission assignment. The remaining SNS allow grouping contacts, but the provided constructs cannot be used for SIdM purposes. Only Facebook provides meaningful assistance for creating social circles by automatically creating suggestions for often used circles such as *close friends* and *family*. Also, contacts that may fit into existing circles are suggested by the platform.

6.4. Contact permission assignment

Google+ and Facebook turned out to have the most fine grained and least restrictive settings for contact permission assignment. Regarding SIdM setting 4a, both provide a very rich set of possible target settings for permission assignment. Both miss however the two proposed target settings, *within circle* and *friends of some friends*. LinkedIn lacks the ability of assigning permissions only to subsets of one's contacts, and on Twitter, the only possible permission targets are the public and approved followers.

All surveyed SNS except LinkedIn force the username and the profile picture to be visible to the public. Besides that, Google+ and Facebook have few limitations regarding sharing decisions (Setting 4b). Both allow individual disclosure settings for every single- and multi value-attribute as well as for each posted item. There is no distinct setting for each value of a multi value-attribute however. Comments inherit the visibility setting of the posted item they were appended to and have no distinct setting. Lacking the proposed permission target *within audience*, comments and posted items from one audience are visible to other audiences. This also applies to the contact list in both SNS, which can be treated as another attribute value in this context: While the contact list may be disclosed only to certain audiences, these audiences may then view *all* other contacts.

While the possible sharing decisions on Diaspora come close to those on Google+ and Facebook, they are very limited on the remaining two SNS. On LinkedIn, this is due to the inability to distinguish between subsets of one's contacts for attribute disclosure. On Twitter, the visibility can only be set globally for all attributes and posted items (here known as *Tweets*), lacking an individual setting for each posted item.

Regarding controls over how contacts may shape the user's profile, we distinguish between items posted to the user profile by contacts, comments on existing items, and references pointing to the user profile. Only Facebook has a feature that allows contacts to post new items into the user profile (known as *Wall*). The user may disable this, but only for all contacts or none of them. Yet, for the visibility of such items, rich audience settings including subsets of one's contacts are available. As discussed with the sharing decisions, for all surveyed SNS except Twitter, comments inherit the visibility setting of the posted item they were appended to and have no distinct visibility setting. They may be removed manually by the user.

References created by other users of an SNS that point to a user's profile associate her presentation of self with external content and lie outside of her manageable domain. Facebook and Google+ provide settings to control incoming references. On Facebook, a setting is available to require user approval before externally posted items referencing to the user's profile are shown to her contacts. Also, the visibility of such items can be restricted to the previously discussed permission targets. On Google+, a similar setting exists, but additionally, the user may specify a group of contacts whose references are visible instantly without further approval. On Twitter, external references to a profile are conducted simply by including the name of the user-account in one of the text-based posted items. Since all publicly posted items may be searched for that account name, it is not technically feasible to restrict references to a user-account on Twitter.

None of the proposed advanced controls for permission assignment were implemented by the surveyed SNS with the exception of Facebook providing a function to change the audience of *old posts* to one's contacts. The limitation of this feature is that the audience cannot be specified more fine grained.

6.5. Survey analysis and reflection

We see Facebook and Google+ as providing the most advanced SIdM settings and features among the surveyed

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

SNS. For Facebook, we reason that while being the market leader, a corresponding amount of public scrutiny regarding privacy settings has been a continuous force pushing toward better SIdM controls. Several SIdM settings included in our survey that Facebook provides have been introduced only lately, with user assistance for creating circles being the most recent example. Google+ was launched at a time when this ongoing trend was clearly observable already. Advanced SIdM controls were necessary to compete on par with Facebook.

Diaspora's SIdM controls are less rich which can be explained by the prototypical character of the current implementation of the decentralized network. Also, one has to consider that while Diaspora was designed with the goal of improving privacy, the decentralized architecture is mostly concerned with protecting user data from centralized SNS, leaving SIdM a side issue.

The available SIdM settings on LinkedIn can be characterized as very limited. One might argue that the single purpose of such an SNS might implicitly lead to using it only in the proper context. However, we think that nowadays fast-paced work environments with ever-changing business relationships will eventually require advanced SIdM controls.

According to our reference framework, Twitter has the least advanced SIdM controls. Yet, one has to consider that while it fits the definition of an SNS, it can also be characterized as a microblog with the focus on short, publicly available status posts. Thus, for the purposes of many of its users, more advanced SIdM controls might not even be necessary.

Thus, the survey shows that differences in the extent to which various SNS support SIdM can be observed. While some SNS can be classified as providing very advanced SIdM controls, there are still suggested SIdM features that have not been implemented yet. We see room for improvements especially in the dedicated support for multiple personas by one SNS-account and in advanced privacy controls.

6.6. *Research limitations*

When developing the reference framework, we maintained a clear focus on settings related to the management and selective disclosure of profile information to multiple contacts or other users on the SNS. The possible disclosure of personal information to other parties, such as the site operator, advertisers and application providers was out of scope.

We did not cover the adjacent topic of the usability of SIdM settings to its full extent. It was only addressed briefly in conjunction with assistance for the management of circles (Setting 3c). The view on one's profile from the perspective of one's contacts is also closely related to usability (Setting 1d). We acknowledge that the usability of privacy controls greatly influences the effectiveness of their usage and possibly whether they are used at all. Yet, the assessment of an SNS' usability cannot be performed as clear-cut as with the settings presented in this work. A reliable usability assessment would require further empirical studies.

So far, the reference framework allows for a qualitative assessment of SIdM support by SNS. We suggest advancing the reference framework toward a quantitative metric in the following section.

7. Toward a metric for assessing SIdM-support of SNS

A qualitative analysis of the capabilities for SIdM as performed in Section 6 is only a first step toward a metric for assessing and comparing various SNS in regards to their support for SIdM. In contrast, a quantitative metric would enable a quick classification and comparison of existing and newly introduced SNS. Also, it would allow assessing quickly how new SIdM settings impact the overall support of an SNS.

A naive *bottom-up*-approach for a quantitative assessment would consist of simply adding up the level of fulfillment of the SIdM settings, denoted by the circles in Table 6, resulting in a score for each SNS. Omitting the high level-requirements, which are aggregates of the fine-grained SIdM settings leaves 16 settings for which a score between 0 and 4 can each be reached. Thus, the SIdM-support of a given SNS n could be described by a score between 0 and 64. Factoring in that the contribution of settings to SIdM may differ, the score for each setting is further multiplied with a predefined setting-dependent factor in this basic approach:

$$\sum_{i=1..s} \text{settingscore}_i(\text{SNS}_n) \times \text{settingfactor}_i$$

This approach does however not consider the interdependencies between SIdM-features. As discussed in Section 5, settings refine or contribute to other settings and may even be interchangeable. A *top-down*-approach could consider these observations by focusing on the four high-level requirements. It could assign weights to the contribution of particular SIdM-features to the high-level requirements and deliver a score for each requirement. Further, analyzing the interdependencies between the particular SIdM-features leads to the observation that settings 1a (control over attribute values) and 4b (fine grained sharing decisions) together have transitive dependencies with all other features. They could be used as a central measure for assessing the SIdM-capabilities of an SNS. The other SIdM features would then influence the final SIdM score based on the impact on settings 1a and 4b.

As noted before, SIdM-features are not always uniformly available for all attributes on an SNS. Thus, it is feasible to decrease an SNS' score if it carries attributes for which some SIdM-features are not available. This could be achieved by calculating an independent SIdM-metric for each attribute in an SNS and aggregating these numbers. Such an approach raises the question of how to weigh the attributes, because attributes on SNS differ in sensitivity of their values, relevance and usage. While the sensitivity of an attribute could be predefined, its usage and perceived sensitivity, and thus its relevance for SIdM, depends largely on the user, the context and individual SNS usage.

For instance, it is possible to assess the criticality especially of static attributes such as the birthday or the email-address to a certain extent. This is because such attributes are structured and the meaning of their possible content is known in advance. This allows to determine their inherent sensitivity and critically beforehand. Often, it is also possible to consider the purpose and usage context of an SNS for the sensitivity of the information expressed there. One might argue for example

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

that information posted on a business-oriented site such as LinkedIn is less likely to compromise one's privacy than information posted on a more leisure-oriented site such as Facebook. Yet, it is necessary to consider the actual information that is posted and its context, which cannot be anticipated by the designer of an SIdM-metric. For instance, updating one's CV might hint at the intent of changing one's occupation. Also the content and criticality of attributes with no fixed semantics such as status updates varies widely. Therefore, to be individually applicable, a possible SIdM-metric has to be adjusted to the usage patterns and preferences.

Hence, for assisting a potential SNS user evaluating a particular site's SIdM capabilities, the SIdM metric could be split up into a general part and a customized user-dependent part. The general part would measure SIdM capabilities and calculate the score using predefined weights for the particular attributes. This part is generally applicable, does not have to be customized to the user and could be published as a first reference.

For calculating the user-dependent part of the score, weights are assigned to certain attributes and SIdM-settings available for them. This requires additional information, mainly consisting of the usage intensity and frequency of each attribute and also the perceived criticality of the corresponding value in regards to privacy. This information could be queried using a basic tool asking the user for these values for each attribute and calculating a customized SIdM assessment for each SNS.

A more advanced version of the tool could even make use of account data that is directly available through programming interfaces from the SNS that are currently used. Thus the tool would be able to assess the usage quantity of attributes automatically and potentially achieve higher data quality than a self-assessment by the user. Further, the user could be queried about the criticality of particular posted items. We expect this to lead to a more accurate assessment of an attribute value's criticality than querying only the user's stance on an attribute but not its actual value. An interactive study on privacy expectations in SNS (Netter et al., 2013) has shown that an interactive questionaire incorporating the user's SNS account data is a feasible way to query the user about particular profile items.

These considerations lead to the outcome that deriving a metric that evaluates the SIdM-capability of an SNS objectively is a very challenging task. This is partly the result of the differences between SNS and their attribute implementations. Another reason is that such a metric would have to be adjusted in order to be applicable to the particular user's situation and usage. The proposed tool could aid users in calculating a customized value for the SIdM capabilities of a given site. A possible alternative for an SIdM-metric would be the construction of a maturity model for the provider-support for SIdM that doesn't return numerical values, but only broad maturity categories.

8. Conclusions

Due to the increasing shift of social life to SNS, a large number of personal information is available online. To manage their identities online, users often rely on real-world heuristics and norms of distribution such as spatial and temporal boundaries. However, these boundaries are no longer existent in SNS due to the permanency of digitally mediated communication and the presence of people from different social circles on one platform.

To effectively manage social identities, online SNS service providers have introduced a variety of settings, such as limiting the visibility of the user's profile. Over time, these settings have evolved to complex privacy models which are difficult to understand and differ between different SNS in terminology used and amount of settings provided.

To facilitate understanding of required SIdM settings, in this article we first derived high-level requirements for SIdM from literature. These requirements were broken down into concrete settings or features that stem from existing SNS or were proposed by the authors, resulting in an SNS-independent frame of reference for SIdM as the first contribution. To evaluate its applicability, the frame of reference was used to examine the SIdM capabilities of five selected SNS, constituting the second contribution. Results showed that popular SNS provide advanced SIdM settings, yet leave room for improvements for managing multiple personas and further advancing privacy controls.

Lastly, we discussed steps toward a quantitative metric to assess the SIdM capabilities of existing and newly introduced SNS and to facilitate their comparison. We identified issues that have to be considered when developing such a metric and aim at refining it. Further future work consists of extending the survey to additional SNS. Regarding existing SNS, the ongoing evolution to multi-purpose SNS, i.e. having different social circles on one platform, will increase incentives for SNS service providers to cover the settings developed in the reference framework for SIdM. Otherwise, users might limit the personal information to the least common denominator which is acceptable for all circles to avoid oversharing of information. Also, we aim at specifying the identified SIdM settings on a more precise and technical level.

REFERENCES

Agre PE, Rotenberg M. Technology and privacy: the new landscape. Cambridge, MA, USA: MIT Press; 1998.

Aïmeur E, Gambs S, Ho A. Towards a privacy-enhanced social networking site. In: Proc. of the fifth international conference on availability, reliability and security 2010.

Ali B, Villegas W, Maheswaran M. A trust based approach for protecting user data in social networks. In: Proc. of the conference of the center for advanced studies on collaborative research 2007.

Bilbow G, Yeung S. Learning the pragmatics of 'successful' impression management in cross-cultural interviews. Pragmatics 2010;8(3):405–17.

Binder J, Howes A, Sutcliffe A. 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. New York, NY, USA: ACM; 2009. p. 965–74.

Bonneau J, Preibusch S. The privacy jungle: on the market for data protection in social networks. In: Proc. of the 8th workshop on the economics of information security 2009.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005

Borcea-Pfitzmann K, Pfitzmann A, Berg M. Privacy 3.0 := data minimization + user control + contextual integrity. IT – Information Technology 2011;53:34–40.

Boyd D, Ellison NB. Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication 2007;13:210–30.

Carminati B, Ferrari E, Heatherly R, Kantarcioglu M, Thuraisingham B. Semantic web-based social network access control. Computers & Security 2011;30:108–15.

DiMicco JM, Millen DR. Identity management: multiple presentations of self in facebook. In: . Proc. of the international ACM conference on supporting group work 2007.

Fang L, LeFevre K. Privacy wizards for social networking sites. In: Proc. of the 19th international conference on world wide web (www). ACM; 2010. p. 26–30.

Farnham SD, Churchill EF. Faceted identity, faceted lives: social and technical issues with being yourself online. In: Proc. of the ACM conference on computer supported cooperative work 2011.

Goffman E. The presentation of self in everyday life. Anchor Books 1959.

Grimmelmann J. Saving facebook. Iowa Law Review 2009;94(4):1137–206. URL, http://www.uiowa.edu/wilr/issues/ILR_94-4_Grimmelmann.pdf.

Irani D, Webb S, Li K, Pu C. Large online social footprints–an emerging threat. In: Proc. of the international conference on computational science and engineering 2009.

Kelley PG, Brewer R, Mayer Y, Cranor LF, Sadeh N. An investigation into facebook friend grouping. In: . Proc. of the 13th IFIP TC 13 international conference on human-computer interaction, vol. part III. Berlin, Heidelberg: Springer-Verlag; 2011. p. 216–33. INTERACT'11.

Krishnamurthy B, Wills CE. Characterizing privacy in online social networks. In: Proc. of the first workshop on online social networks 2008.

Kuczerawy A, Coudert F. Privacy settings in social networking sites: Is it fair? In: Fischer-Hübner S, Duquenoy P, Hansen M, Leenes R, Zhang G, editors. Privacy and identity management for life. IFIP advances in information and communication technology, vol. 352. Boston: Springer; 2011. p. 231–43.

Lampinen A, Tamminen S, Oulasvirta A. All my people right here, right now: management of group co-presence on a social networking site. In: Proc. of the ACM international conference on supporting group work 2009.

Leenes R. Context is everything: sociality and privacy in online social network sites. In: Bezzi M, Duquenoy P, Fischer-Hübner S, Hansen M, Zhang G, editors. Privacy and identity management for life. IFIP advances in information and communication technology, vol. 320. Springer; 2010. p. 48–65.

Lewis K, Kaufman J, Christakis N. The taste for privacy: an analysis of college student privacy settings in an online social network. Journal of Computer-mediated Communication 2008;14(1):79–100.

Lipford HR, Hull G, Latulipe C, Besmer A, Watson J. Visible flows: contextual integrity and the design of privacy mechanisms on social network sites. In: Proc. of the international conference on computational science and engineering 2009.

Liu Y, Gummadi KP, Krishnamurthy B, Mislove A. Analyzing facebook privacy settings: user expectations vs. reality. In: Proc. of the 2011 ACM SIGCOMM conference on internet measurement conference. New York, NY, USA: IMC '11. ACM; 2011. p. 61–70.

Madejski M, Johnson M, Bellovin SM. The failure of online social network privacy settings. Tech. rep.. Columbia University; 2011

Madejski M, Johnson M, Bellovin SM. A study of privacy settings errors in an online social network. In: Proc. of 2012 IEEE international conference on pervasive computing and communications workshops (PERCOM workshops). IEEE; Mar. 2012. p. 340–5.

Mayer-Schönberger V. Delete: the virtue of forgetting in the digital age. Princeton University Press; 2009.

Netter M, Hassan S, Pernul G. An autonomous social web privacy infrastructure with context-aware access control. In: Proc. of the 9th international conference on trust, privacy & security in digital business (TrustBus) 2012.

Netter M, Riesner M, Pernul G. Assisted social identity management – enhancing privacy in the social web. In: Proc. of the 10th international conference on wirtschaftsinformatik 2011.

Netter M, Riesner M, Weber M, Pernul G. Privacy settings in online social networks – preferences, perception, and reality. In: Proc. of the 46th Hawaii international conference on system sciences (HICSS). IEEE Computer Society; 2013.

Nguyen-Son H-Q, Nguyen Q-B, Tran M-T, Nguyen D-T, Yoshiura H, Echizen I. Automatic anonymization of natural languages texts posted on social networking services and automatic detection of disclosure. In: Proc. of the 7th international conference on availability, reliability and security (ARES) 2012. p. 358–64.

Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life. Stanford Law Books; 2010.

Palen L, Dourish P. Unpacking "privacy" for a networked world. In: Proc. of the SIGCHI conference on human factors in computing systems 2003.

Peterson C. Losing face: an environmental analysis of privacy on facebook. SSRN eLibrary; 2010.

PrimeLife. D1.2.1-Privacy enabled communities 2010.

Riesner M, Netter M, Pernul G. An analysis of implemented and desirable settings for identity management on social networking sites. In: Proc. of the 7th international conference on availability, reliability and security (ARES) 2012.

Riesner M, Pernul G. Maintaining a consistent representation of self across multiple social networking sites – a data-centric perspective. In: Proc. of the 2012 ASE/IEEE international conference on social computing and 2012 ASE/IEEE international conference on privacy, security, risk and trust. IEEE Computer Society Press; 2012. p. 860–7.

Rouvroy A. Privacy, data protection, and the unprecedented challenges of ambient intelligence. Studies in Ethics, Law, and Technology 2008;2(1).

Schneier B. A taxonomy of social networking data. IEEE Security and Privacy 2010;8:88.

Strater K, Lipford HR. Strategies and struggles with privacy in an online social networking community. In: . Proc. of the 22nd British HCI group annual conference on people and computers: culture, creativity, interaction, vol. 1. Swinton, UK: BCS-HCI '08. British Computer Society; 2008. p. 111–9.

Tufekci Z. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society 2008;28:20–36.

Ulbricht M-R. Privacy settings in online social networks as a conflict of interests: regulating user behavior on facebook. In: Abraham A, editor. Computational social networks. Springer London; 2012. p. 115–32.

van den Berg B, Leenes R. Audience segregation in social network sites. In: Proc. of the 2010 IEEE second international conference on social computing 2010.

Watson J, Besmer A, Lipford HR. +Your circles: sharing behavior on google+. In: Proc. of the eighth symposium on usable privacy and security. Soups '12. New York, NY, USA: ACM; 201212:1–12:9.

Ziegele M, Quiring O. Privacy in social network sites. In: Privacy online. Perspectives on Privacy and Self-Disclosure in the Social Web. Springer; 2011.

Please cite this article in press as: Riesner M, et al., Analyzing settings for social identity management on Social Networking Sites: Classification, current state, and proposed developments, Information Security Technical Report (2013), http://dx.doi.org/10.1016/j.istr.2013.02.005