An Analysis of Implemented and Desirable Settings for Identity Management on Social Networking Sites

Moritz Riesner, Michael Netter and Günther Pernul
Department of Information Systems
University of Regensburg
Regensburg, Germany
{*firstname.lastname*}*@wiwi.uni-regensburg.de*

***Abstract*—To address privacy threats stemming from interacting with other users on Social Networking Sites (SNS), effective Social Identity Management (SIdM) is a key requirement. SIdM refers to the deliberate and targeted disclosure of personal attribute values to a subset of one's contacts on SNS. While a variety of privacy-enhancing approaches have been proposed, these are often isolated solutions that lack integration into a reference framework that states the requirements for successfully managing one's identity. In this paper, 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.**

***Keywords*-Social Identity Management; SIdM; Social Networking Sites; Privacy; Requirements; Privacy Settings**

I. Introduction

Social Networking Sites (SNS) on the internet are of increasing importance both in personal and professional life. These sites, such as *Facebook*, allow users to create personal profiles, express connections with other users and traverse the resulting social graph [1]. 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.

The need for settings that enable personal *Social Identity Management* (SIdM) has been pointed out by multiple authors [2], [3]. 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 [4]. 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 [5].

Desirable settings for SIdM, such as grouping one's contacts into audiences for later attribute disclosure have previously been described in detail [6]. Often, such settings have subsequently been implemented by SNS. For instance, automated proposal of homogeneous audiences was presented in [7] 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 [8], 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. These issues underline the need for a provider-independent reference framework to compare existing and future SNS regarding their SIdM capabilities.

The contribution of this paper is twofold: First, a reference framework for existing and desired SIdM settings is derived from literature analysis and established SNS. It is suitable to analyze and compare the extent to which SNS support SIdM. Second, we evaluate a set of selected SNS using the reference framework to demonstrate its applicability and to highlight possible improvements of their SIdM settings.

The remainder of this paper is structured as follows. After describing related work in Section II, Section III addresses our research approach. In Section IV we derive general requirements for SIdM from literature. In Section V 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 VI surveys selected SNS using the reference framework. Section VII concludes the paper.

II. Related Work

Multiple authors argue that privacy is a growing concern as SNS usage has increased over the years [9], [10]. Two major threats to privacy can be distinguished, stemming either from SNS service providers or other SNS users [11]. This paper 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 [12] 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 in [13]. Furthermore, SNS-specific access control models have been proposed that aim at improving targeted sharing of personal information [8], [14]. 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.

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 [15] 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. Krishnamurthy and Wills [16] 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 [17].

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 IV, which aims at elicitating requirements from literature.

III. Research Model

Our research is based on the model shown in Figure 1. First, we derive high-level requirements for SIdM from literature, which is described in Section IV (step (1) in Figure 1). Relevant literature includes work from other research areas that can be applied to SNS, for instance social identity theory from 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 V 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 IV, 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.

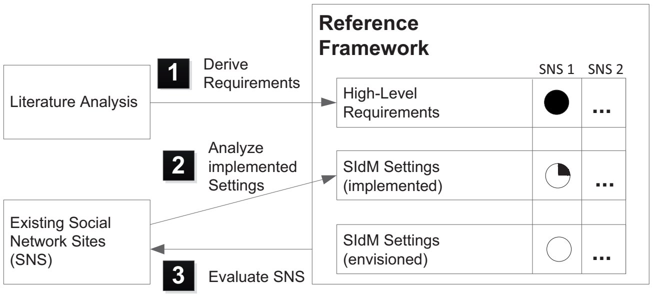

Figure 1. Research Model

The particular settings and features for SIdM are grouped by the high-level requirements presented in Section IV, resulting in a structured catalogue. 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 VI, we apply the reference framework on a selected number of SNS to evaluate and compare their support for SIdM, leading to a qualitative assessment (3). 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.

IV. 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 V. This analysis is decoupled from actually implemented SIdM features to avoid limitations that would arise from only looking at the status quo.

Table I
High-Level Requirements for SIDM derived from Literature

No.	Requirement	Sources
1	Unrestricted identity creation and control	[4]
2	Create and maintain multiple representations of the self	[4] [18] [19]
3	Create and maintain multiple social circles	[4] [20] [21]
4	Contact permission assignment	[2] [22] [12] [18] [23]

A variety of theories has been published 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 concept of impression management [4], a person performs different roles to present an image of the self which is favorable and appropriate for the current situation. The presented identity depends on the relationship to present people. Impression management allows for having multiple, potentially conflicting roles that are bound to different social contexts and their corresponding audiences. This conceptualization of identity can be applied to SNS since the primary functions of these sites are impression- and relationship management [1]. In the following, we derive requirements for SIdM in SNS based on this conceptualization (Table I).

As shown in the previous paragraph, identities are constructs rather than ready-made essences [24]. Thus, an essential requirement for successful social identity 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 I). 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, as SNS evolve from single- to multi-purpose platforms, where contacts from different social contexts are present at the same platform [19], 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 [18]. 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 [20]. Within an SNS, it should be possible to partition the user's contacts into different, potentially overlapping groups [18]. 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 [21]. Thus, there is a need for assisting the user in grouping contacts into social circles [7].

Contact permission assignment (4) is a further requirement for social identity management that results from 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 [2]. 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 [22].

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 [12]. 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 [18]. 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 [23].

V. 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 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.

Figure 2 shows the scope of the requirements identified in Section IV. 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

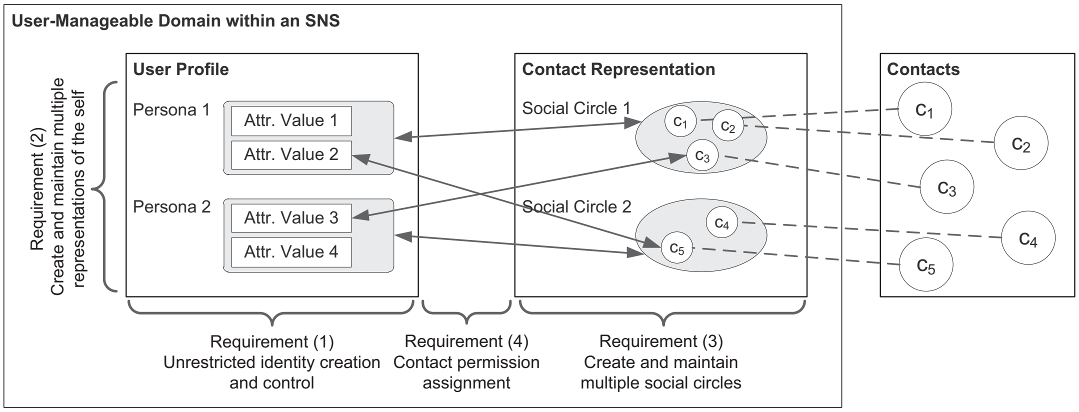

Figure 2. Scope of the Requirements and Settings Analysis

representation of self. It may be broken down into *personas* that are subsets of the profile and the technical pendant 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 Figure 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.

Even in the user-manageable domain, user control may be limited by available settings within the SNS. Hence, all SIdM requirements derived in the previous section concern the user-manageable domain. While users may also be able to influence their contact's profile in the SNS, permissions to do this lay in the manageable domain of that contact. Each of the following subsections addresses one of the requirements identified in Table I.

A. Unrestricted Identity Creation and Control

SIdM settings related to *unrestricted identity creation and control* allow users to create and shape their SNS profile and to control its contents.

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 II identifies four SIdM-settings directly related to control over the attributes within a user profile. First, the user should be the final authority over each attribute's value (Setting 1a). Especially this concerns 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. Further, users should be able to leave attribute values empty as they wish (1b). We suggest that maximum control over one's online representation could be achieved through users being able to freely add custom attribute types to their profile (1c).

Depending on the SNS, these settings may be available only for some attributes. Hence the column *Possible Options* denotes that the availability of each setting may be defined separately for each attribute. It is also possible in particular SNS that a setting is only available for certain attribute categories.

Table II
SETTINGS FOR REQUIREMENT 1: UNRESTRICTED IDENTITY CREATION AND CONTROL

No.	SIdM-Setting or Feature	Possible Options
1a	User has complete control over attribute value	yes/no (for each attribute)
1b	User may leave attribute value empty	yes/no (for each attribute)
1c	User may define and use custom attribute types	yes/no
1d	User may view how profile appears to others	yes/no

The 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. As such an analysis is very implementation-dependent, it is performed together with the provider survey in Section VI, 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* [25], 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.

B. 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 III lists three SIdM settings to achieve multiple

Table III
SETTINGS FOR REQUIREMENT 2: CREATE AND MAINTAIN MULTIPLE REPRESENTATIONS OF THE SELF

No.	SIdM Setting or Feature	Possible Options
2a	User may allocate attribute values freely to personas	yes/no (for each attribute)
2b	Implicit multiple representations of self through selective disclosure of attribute values	yes/no (for each attribute)
2c	User may disclose different values for the same attribute to different contacts	yes/no (for each attribute)

personas in an SNS. Setting 2a is the most exhaustive one and uses the explicit construct of a persona [13]. It allows users to create multiple personas by grouping attribute values.

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). 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 possible audiences and is discussed in the first two items of Section V-D.

C. 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 IV. Setting 3b denotes whether social circles may overlap, meaning that one contact may be the member of two or more circles. Finally, as nowadays some SNS users have several hundred contacts, 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 as described in [7].

D. Contact Permission Assignment

Building on the previous two subsections and referring to requirement 4 in Table I, 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 V.

Table IV
SETTINGS FOR REQUIREMENT 3: CREATE AND MAINTAIN MULTIPLE SOCIAL CIRCLES

No.	SIdM Setting or Feature	Possible Options
3a	User may group contacts to form social circles	yes/no
3b	Social circles may overlap	yes/no
3c	SNS assists user with creating circles	yes/no

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 V-C. Figure 3 shows further possible settings for targets that permissions can be assigned to.

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 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. The *friend of a friend (FoF)*-setting grants the permission to the 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. Even though the latter two settings limit that number of entities to a certain degree, it is still beyond the user's control, who in particular is actually granted a permission. As shown in Figure 3, we suggest a setting *friends of some friends* to reduce the reach of the regular FoF-Setting.

The setting granting permissions to *all contacts* is commonly used. 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 V-C. For disclosure settings regarding content created by contacts, 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/not available* don't assign permissions to any third entity and are shown for the sake of completeness only.

2) Fine Grained Sharing Decisions for Attribute Values: 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

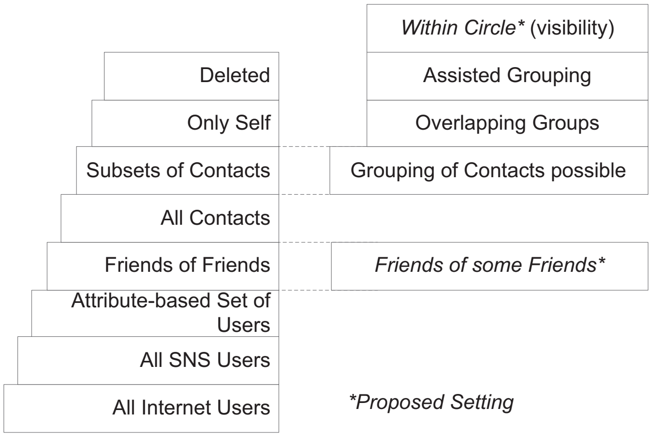

Figure 3. Possible Targets for Permissions

Table V
SETTINGS FOR REQUIREMENT 4: CONTACT PERMISSION ASSIGNMENT

No.	SIdM Setting or Feature	Possible Options
4a	Possible targets for permissions (set T)	*refer to Figure 3*
4b	Fine grained sharing decisions for attribute values A	$SD = \{A \times T\}$, consider restrictions
4c	Control how contacts can shape the user's profile	$T \times \{$ allow, individual approval, deny$\}$
4d	Control incoming references to the user's profile	$T \times \{$ allow, individual approval, deny$\}$
4e	Time-based sharing decisions	posted items with expiry date/ tool to delete older items (for each attribute)
4f	Limit the number of accesses of information items	yes/no (for each attribute)

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.

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 V, 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.

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 IV, 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.

VI. 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 summarized in Table VI, 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 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.

A. Unrestricted Identity Creation and Control

The surveyed SNS allow for modestly unrestricted identity creation and control, with Google+ being slightly superior than the others 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 automatically leads to a corresponding posted item created for the user, which 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.

B. 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.

C. 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.

D. 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,

[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

Table VI
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 complete control over attribute value		●	●	●	●	◑
1b	User may leave attribute value empty		◕	●	◑	●	◕
1c	User may define and use custom attribute 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 values 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 decisions		○	○	○	○	◔
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

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.

E. Survey Analysis and Reflection

We see Facebook and Google+ as providing the most advanced SIdM settings and features among the surveyed 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 towards 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 already clearly observable. 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.

F. 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. 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 towards a quantitative metric. This would enable a quick classification and comparison of newly introduced SNS and allow assessing quickly how new SIdM settings impact the overall support of an SNS. A naive approach would consist of simply adding up the level of fulfillment of the SIdM settings, denoted by the circles in Table VI, resulting in a score for each SNS. A more advanced approach would assign weights to the particular settings, as they are of different importance. Likewise, dependencies between the settings could be considered. In our reference framework for example, setting 4b, the fine-grained sharing options, is of major importance, but it also builds on setting 4a, the permission targets. An even more advanced approach would consider if SIdM settings are available for the most critical and sensitive attributes of a given SNS.

VII. Conclusions

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 paper 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 proposed by the authors, resulting in a SNS-independent reference framework 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.

Future work aims at developing a quantitative metric to assess the SIdM capabilities of existing and newly introduced SNS and facilitate their comparison. We further plan to extend 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.

References

[1] D. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, 2007.

[2] S. D. Farnham and E. F. Churchill, "Faceted identity, faceted lives: social and technical issues with being yourself online," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work*, 2011.

[3] H. R. Lipford, G. Hull, C. Latulipe, A. Besmer, and J. Watson, "Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites," in *Proceedings of the International Conference on Computational Science and Engineering*, 2009.

[4] E. Goffman, *The Presentation of Self in Everyday Life*. Anchor, 1959.

[5] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books, 2010.

[6] B. van den Berg and R. Leenes, "Audience Segregation in Social Network Sites," in *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, 2010.

[7] M. Netter, M. Riesner, and G. Pernul, "Assisted Social Identity Management - Enhancing Privacy in the Social Web," in *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, 2011.

[8] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Semantic web-based social network access control," *Computers & Security*, vol. 30, pp. 108–115, 2011.

[9] D. Irani, S. Webb, K. Li, and C. Pu, "Large online social footprints–an emerging threat," in *Proceedings of the International Conference on Computational Science and Engineering*, 2009.

[10] K. Borcea-Pfitzmann, A. Pfitzmann, and M. Berg, "Privacy 3.0 := Data Minimization + User Control + Contextual Integrity," *it - Information Technology*, vol. 53, pp. 34–40, 2011.

[11] M. Ziegele and O. Quiring, "Privacy in Social Network Sites," in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer, 2011.

[12] Z. Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society*, vol. 28, pp. 20–36, 2008.

[13] R. Leenes, "Context is Everything - Sociality and Privacy in Online Social Network Sites," in *Privacy and Identity, IFIP AICT 320*, 2010.

[14] B. Ali, W. Villegas, and M. Maheswaran, "A trust based approach for protecting user data in social networks," in *Proceedings of the Conference of the center for advanced studies on Collaborative research*, 2007.

[15] J. Bonneau and S. Preibusch, "The Privacy Jungle: On the Market for Data Protection in Social Networks," in *Proceedings of the 8th Workshop on the Economics of Information Security*, 2009.

[16] B. Krishnamurthy and C. E. Wills, "Characterizing privacy in online social networks," in *Proceedings of the first workshop on Online social networks*, 2008.

[17] B. Schneier, "A taxonomy of social networking data," *IEEE Security and Privacy*, vol. 8, p. 88, 2010.

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

[19] J. M. DiMicco and D. R. Millen, "Identity management: multiple presentations of self in facebook," in *Proceedings of the International ACM Conference on Supporting group work*, 2007.

[20] A. Lampinen, S. Tamminen, and A. Oulasvirta, "All My People Right Here, Right Now: management of group copresence on a social networking site," in *Proceedings of the ACM International Conference on Supporting Group Work*, 2009.

[21] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *Proceedings of the SIGCHI Conference on Human factors in computing systems*, 2003.

[22] N. Haferkamp, "Authentische Selbstbilder, geschönte Fremdbilder," in *StudiVZ*. VS Verlag für Sozialwissenschaften, 2011.

[23] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009.

[24] PrimeLife, "D1.2.1 - Privacy Enabled Communities," 2010.

[25] E. Aïmeur, S. Gambs, and A. Ho, "Towards a Privacy-Enhanced Social Networking Site," in *Proceedings of the Fifth International Conference on Availability, Reliability and Security*, 2010.