Privacy in Social Networks: Existing Challenges and Proposals for Solutions

Michael Netter, Günther Pernul(✉), Christian Richthammer, and Moritz Riesner

Department of Information Systems, University of Regensburg, Regensburg, Germany
{michael.netter,guenther.pernul,christian.richthammer, moritz.riesner}@wiwi.uni-regensburg.de
http://www-ifs.uni-regensburg.de

Abstract. The significant change in our social lives and communication habits caused by the rise of Social Network Sites (SNSs) has not only brought along benefits but is also accompanied by privacy threats. In this paper we present our research efforts on SNS privacy and social identity management. First, we outline the results of an empirical study showing significant discrepancies between Facebook users' actual privacy settings and their perception as well as their preferences. Based on this evident need for improving privacy, we present a novel conceptualization of privacy that serves as the basis for tackling the challenges. Finally, the paper provides an overview of solutions we developed as part of our research efforts on privacy in SNSs.

Keywords: Social network sites · Privacy · Social identity management

1 Motivation

Since their emergence more than a decade ago, Social Network Sites (SNSs) are increasingly changing our social lives and communication habits. While social networks have always been an important part of human life, the advent of easy-to-use services and their ability to bridge boundaries – regarding both space and time – increasingly shifts social life to the online world. These networks enable communication with people from different social spheres (e.g. family, close friends, colleagues), ease interaction, and allow their users to stay in touch with existing contacts as well as to create new relationships.

However, the rise of SNSs also threatens the privacy of their users. On the one hand, people on SNSs inconsiderately share many personal items (e.g. status updates, location updates, photos) while they are not fully aware of their audience. There are numerous examples of SNS users posting inappropriate pictures and status updates and consequently offending people that have access to these items (such as one's boss or parents). On the other hand, few SNS providers exist that have collected a large amount of personal data in their databases raising surveillance and data protection concerns.

O. Camp et al. (Eds.): ICISSP 2015, CCIS 576, pp. 16–27, 2015.
DOI: 10.1007/978-3-319-27668-7_2

In [11], a differentiation is made between two types of privacy: protecting users from overly powerful SNS service providers and from other SNS users. Figure 1 clarifies the interdepencencies between SNS stakeholders and their implications on privacy. As can be seen, SNS service providers and SNS users are the two main stakeholders. From the provider perspective, the underlying business model is often based on selling services based on personal data of their users. Hence, the primary goal is to attract as many users as possible. At the same time, users have the contrary goal of preventing the disclosure of personal data to the SNS service provider. Yet simultaneously, SNS users depend on the functionality of the SNS platform to manage their social identities. In more detail, they are reliant on the provided functions to control the visibility of shared items in order to protect their privacy against other SNS users. In addition, users of SNSs need to cope with the properties of mediated communication such as persistence and searchability and take these into consideration [11].

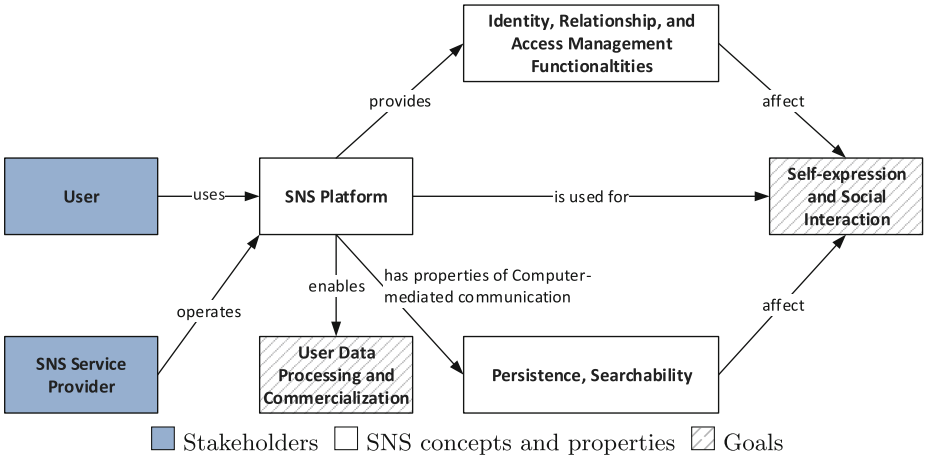


Fig. 1. Relation between SNS stakeholders, their goals, and core concepts [11]

While a variety of research focuses on protecting SNS users' privacy from overly powerful SNS service providers (e.g. [1–3,12]), this work concentrates on means to protect personal data from other SNS users. Its aim is to present existing challenges for SNS privacy and proposals for solutions by presenting our research efforts in this area. In the remainder, we conceptualize the problem of SNS privacy in Sect. 2. In Sect. 3, we further decompose it into sub-problems and present solutions to them. Finally, Sect. 4 concludes the paper.

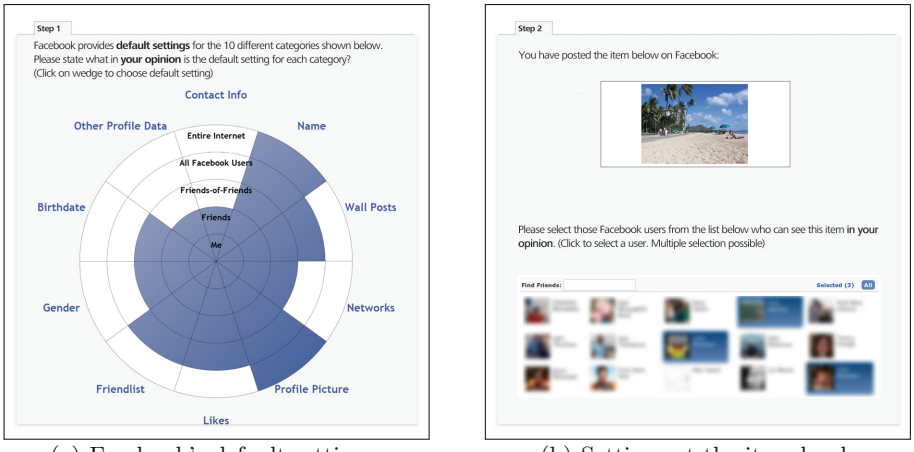
2 Conceptualization of SNS Privacy

In this section, we conceptualize the notion of SNS privacy. First, we motivate the need for improving privacy by presenting the results of an empirical study. After

that, we introduce three different perspectives to look at SNS privacy settings and decompose privacy into the two sub-problems of awareness and control.

2.1 The Need for Improving SNS Privacy

As already pointed out, SNSs require active participation and the disclosure of personal information. The more information the users share on the platform the more valuable the SNS becomes – both for the service provider who has more data for analyses at his disposal and for the users who can see more information about others. Since not every piece of personal information should be disclosed to all users of the platform (or to the entire Internet) but rather to one's personal contacts or a subset of them, SNS providers have introduced privacy settings that are similar to access control models known from identity and access management. Users can employ them to control who is able to see a shared item, which renders these settings the primary means to manage the information flow on SNSs. In general, these privacy settings enable the users to create multiple social roles for different audiences (such as family, friends, and professional life), to keep their roles separated and consistent, and thus to protect their privacy. However, in a study we were able to show that this idealized conception of managing information flows on SNSs is far from reality [14]. Access control models and privacy settings are difficult to understand and to use, especially for less technically-savvy users. As a consequence, the user's desired visibility of a particular item may differ from who can actually see the item.



(a) Facebook's default settings (b) Settings at the item level

Fig. 2. Conceptual designs of the questionnaires on visibility settings

In this study, we employed several questionnaires regarding privacy settings on Facebook. The first questionnaire targets Facebook's default visibility

settings[1] (see Fig. 2(a)). The inner circles represent the different possible default settings on Facebook. The wedges of the circle represent the different categories of information on Facebook. First, the participants were asked to state how they believe the default settings to be for each information category by clicking in the respective area of the corresponding wedge. In a next step, they should state their preferred default settings for each category using the same interface. In our analysis we compared the perceived and actual visibility as well as preferred and actual visibility. The major findings are that users underestimated the scope of the default visibility settings and that they prefer more restrictive default visibility settings. The second questionnaire is concerned with the visibility settings of personal items (see Fig. 2(b)). At the top, the users are shown a personal item that they have disclosed on Facebook. At the bottom, they are shown a selection of contacts as well as randomly selected Facebook users. Similar to the first questionnaire, we gathered their perceived visibility by asking the participants to click on the contacts that in their opinion are able to see the item (perceived settings). Subsequently, the users should express their preferred visibility by clicking on the contacts to which they would actually like to show the item (preferred settings). Using real personal items instead of generic ones makes it easier for the participants to identify themselves with these tasks and thus constitutes an important difference to related studies. Our results show that for 17.9 % of the 8,505 binary visibility perceptions analyzed, there is a mismatch between the perceived and the actual settings. Moreover, 45 % of the 68 participants underestimate the visibility of at least one item. They also show that for 24.6 % of the 8,505 binary visibility perceptions analyzed, there is a mismatch between the preferred and the actual visibility settings. Moreover, 64 % of the 68 participants want more restrictive visibility settings for at least one item [14].

2.2 Decomposing Privacy into Awareness and Control

The results presented in [14] reveal two fundamental problems. First, users on Facebook underestimate the default visibility of items shared on the platform as well as the visibility of their own shared items. This shows that SNS users do not fully understand the privacy implications of the SNS access control models. The discrepancy between perceived and actual visibility can be interpreted as a lack of privacy awareness (see Fig. 3). Second, the demand for more restrictive privacy settings demonstrates that SNS users' preferred visibility settings differ from the actual ones. It shows that SNS users are not able to apply the preferred settings at all or at least with reasonable effort. This inability to align preferred and actual visibility can be seen as a lack of control. The interdependencies between perceived, preferred, and actual visibility are depicted in Fig. 3 and constitute one of the main contributions in [14]. In the following section, we show how to address the problems of awareness and control by developing new solutions for SNSs.

[1] The default settings used in the study were those of December 2011 and may have changed since then.

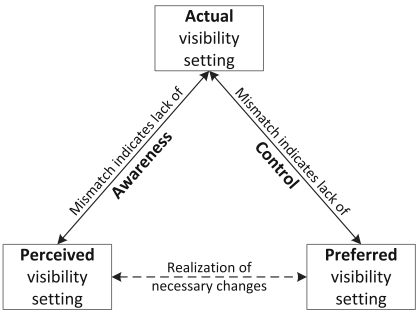


Fig. 3. Conceptualization of privacy as perceived, preferred and actual visibility [11]

3 Solutions to Address SNS Users' Lack of Awareness and Lack of Control

The previous sections demonstrate that the lack of awareness and the lack of control over who can see which personal items are one of the main threats to privacy on SNSs. We refer to these challenges of presenting different facets of the self to different contacts and keeping them consistent as *social identity management* [13]. Further decomposing these challenges shows that social identity management involves the management of one's different identities, one's relations to other users, and who has access to which identities [11].

In the following, we present solutions to address the problems of awareness and control and show how these improve identity, relationship, and access management in particular and social identity management in general.

3.1 Improving Awareness

Since users first need to know about SNS privacy risks and the effects of SNS privacy settings before making any adjustments, privacy awareness can be seen as a prerequisite for privacy control. In the following, we present approaches we developed to inform SNS users about SNS data types, assisting them with their privacy settings and educating them about privacy implications.

Understanding Social Network Data Types: A Taxonomy. Despite the large body of research regarding privacy issues in SNS, there are rather fundamental aspects that have received little attention and that should be addressed first such as the differentiation of social network data types. Since the lack of a generally accepted terminology may lead to confusion in related discussions, we fill this gap by proposing a comprehensive taxonomy in [18,19]. This is particularly important considering the fact that the popularity of SNSs has lead to an increased quantity and availability of sensitive data. The basis for our taxonomy is a thorough literature analysis clarifying discussions among researchers and

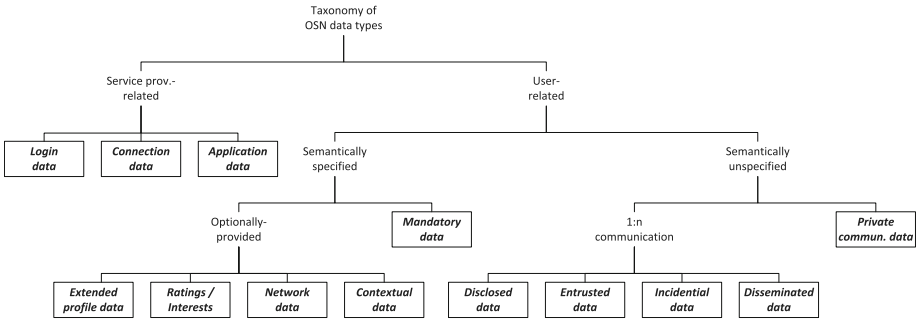


Fig. 4. Taxonomy of SNS data types

benefiting the comparisons of data types within and across platforms. However, we also include a conceptualization of common user activities on SNSs in the development process. We explicitly take the end users into consideration and aim at educating them about the characteristics and implications of different data types, thus raising their awareness regarding privacy in SNSs. Our proposed taxonomy is depicted in Fig. 4. We discover that privacy implications mainly depend on the interplay of a data element's content, the extent and the granularity of user control, and the concrete implementations of these factors on the respective platform. In the course of demonstrating the applicability of our taxonomy, we reveal the implementation-specific differences in privacy settings [18,19].

Raising Awareness Through Visualization: The Access Policy Grid. One major issue in connection with SNS privacy settings is that translating them into human-understandable representations is not straightforward, especially considering the large number of items and contacts. Consequently, researchers (e.g. [9,17]) agree on the need for a holistic view on them. This is supposed to show the impact of users' privacy settings and to enable them to understand their social roles (i.e. their identity facets presented to different audiences) as well as to detect potential inconsistencies therein. In [15], we develop a novel matrix-based visualization approach called Access Policy Grid (APG) providing the users with a bird's-eye view on their privacy settings. This explicitly addresses the problem that users easily lose track of the visibility of items they have disclosed. The matrix-based visualization is appropriate for this purpose because it allows to examine the relations between a large number of objects without having to reduce the number of dimensions [5]. The concept of the APG along with the steps necessary to arrive at the final reordered matrix are illustrated in Fig. 5. In an initial step, the user's items as well as their visibility settings are retrieved from the SNS database. Then, the visibility settings are converted to a contact-permission matrix. The user's shared items $(i_1, \ldots, i_m)$ are represented as rows, while the user's contacts $(c_1, \ldots, c_n)$ are represented as columns. A cell c_{ij} is filled if item i_i is visible to contact c_j. Illustrating the visibility settings in a matrix already provides the user with a bird's-eye view on them. However, we

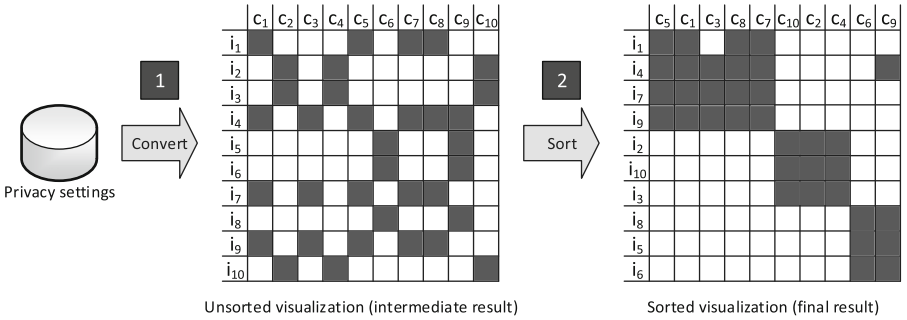


Fig. 5. Access Policy Grid generation process on a conceptual level [15]

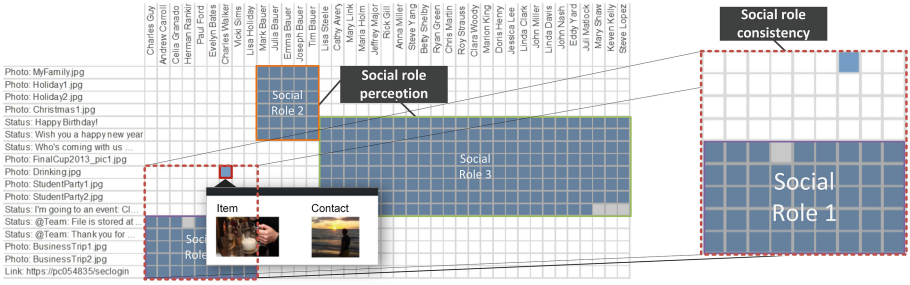


Fig. 6. Visualization of social roles and their consistency [15]

further sort the APG using a visual role mining algorithm presented in [6]. The algorithm arranges contacts with similar access rights next to each other. Thus, similar contacts are visualized in clusters and different social roles can easily be perceived by the user [15].

Figure 6 shows the implementation of the APG. In the given dataset, three social roles are easily conceivable. In addition, this visualization facilitates the discovery of possible errors such as missing privileges on the one hand and excessive privileges on the other hand. Figure 6 illustrates the discovery of such errors. As can be seen, item *Photo: Drinking.jpg* is visible to contact *Charles Walker* which makes *Social Role 1* inconsistent as this contact is the only contact of the role who can see the item [15].

Raising Awareness by Education: Friend Inspector. In order to playfully educate the users about SNS privacy settings, we introduce a serious game called "Friend Inspector" in [4]. The application relies on real Facebook data of the users, which makes it easier for them to identify themselves with the tasks that they are confronted with in the course of the application. Friend Inspector is developed for Facebook because it currently is the most popular SNS and offers very fine-grained privacy settings to its users. The reason for choosing the concept of a serious game is that we want to lay the focus on younger users (e.g.

teenagers, students) because they are the ones that are affected the most by threats like Internet mobbing, cyber stalking, and employers' online background research. Friend Inspector is based on the experiential gaming model introduced in [10], which combines experiential / inductive learning, flow theory, and game design [4].

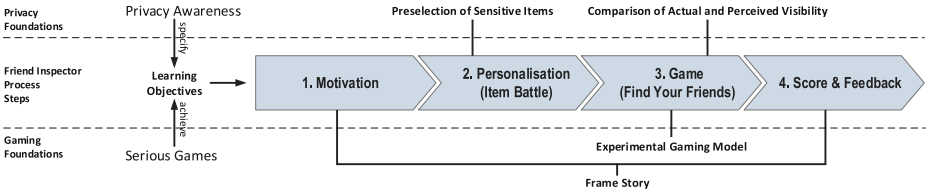


Fig. 7. Four-step process design of Friend Inspector [4]

The starting point of the experiential gaming model is the definition of the learning objectives. For Friend Inspector, the first of the two main goals is to enhance the users' privacy awareness. We want them to recognize the effects of their privacy settings, thereby decreasing the gap between perceived and actual visibility. The second goal is to educate the users about privacy settings. We want to empower them to improve their settings by providing them with personalized recommendations. With these learning objectives in mind, we design Friend Inspector as a four-step process. As can be seen in Fig. 7, the process integrates the concept of privacy awareness, which specifies the learning objectives, and the concept of serious games, which is used to achieve these objectives. Figure 8 shows the main game interface of Friend Inspector where users are asked to quickly choose the contacts that can see the item displayed [4].

3.2 Improving Control

Control over personal data in SNSs is enabled by offering SNS users' the functionality they need to manage their social identities in a privacy-preserving manner. This comprises the management of one's identities, one's relationships to other users, and the visibility of shared items. In the following, we outline our solutions for these three types of personal data control.

Managing Identities: Consistent Social Identities Across Multiple Platforms. On SNSs, the user is responsible to manage his various identities in a way that an appropriate facet is shown to a particular audience. However, we show in [20–22] that existing SNSs lack the required functionality to manage identities appropriately. This comprises the lack of means to create multiple representations of the self (i.e. multiple identity facets) and restrictions in shaping identities (e.g. providing only predefined SNS profile attributes). The problem increases when users aim to create consistent social identities across multiple

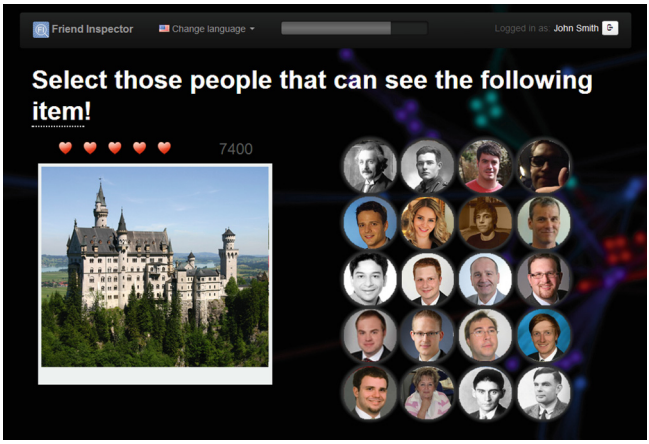


Fig. 8. Main game interface of Friend Inspector [4]

SNSs, such as Facebook, Twitter, and LinkedIn. In [23,24], we outline a single, global and provider-independent social identity model and show how to implement and decompose these identities on existing SNSs. Therein, decisions in the global model (e.g. sharing a particular item to a set of contacts) are translated to the local model of the SNS. In order to check if the changes have been implemented correctly, the provider-specific model is derived and compared to the global model. This results in a continuous cycle that applies changes from the global model to connected SNSs, evaluates the correct implementation, and updates the global model if necessary. We also show how the implementation of such a global model depends on the availability of suitable APIs on existing SNSs.

Managing Contacts: Assisted Audience Segregation. One of the major problems of existing SNSs is that all contacts (which are commonly referred to as friends) are treated equally and stored in one flat list [16]. Moreover, the default visibility of shared items is set to all contacts. This lack of differentiation between contacts from different social spheres (such as family, work, and close friends) hampers the targeted sharing of personal data. In [13], we propose to support users in pointing out segregated audiences among their SNS contacts. In more detail, a clustering algorithm is developed that discovers segregated audiences using the relationship between contacts as a criterion. The underlying assumption is that contacts that are mutual friends on the SNS are more likely to belong to the same social sphere (see Fig. 9). For instance, it is likely that classmates in my list of contacts have a mutual relationship, whereas it is more unlikely that one of my classmates is also friends with my parents who are also in my list of contacts. Once the algorithm has been executed, the clusters are presented to the user for refinement and approval [13].

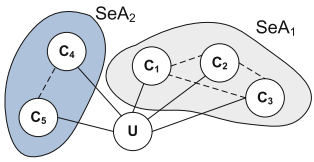


Fig. 9. Relationship between contacts [13]

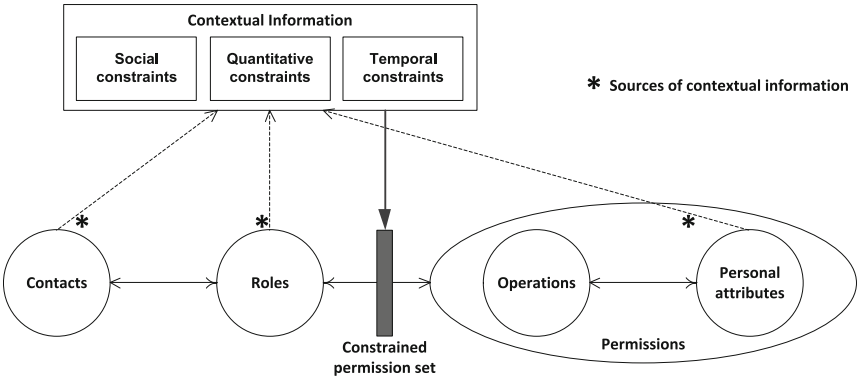


Fig. 10. Context-aware access control model [12], based on the Core RBAC model [7]

Managing Visibility: A Trust-Based Access Control Model. Besides managing contacts, one of the main drawbacks of existing SNSs is the underlying access control model which is used to define which contacts can see a particular item. Existing SNSs commonly use an access control model similar to the role-based access control (RBAC) [7] model. However, as stated by Grimmelmann "[people] think about privacy in terms of social rules and social roles, not in terms of access-control lists and file permissions" [8]. In order to incorporate the different levels of trust SNS users have in their contacts, in [12] we propose to extend the existing access control models by incorporating contextual information such as trust and time. Figure 10 depicts the extended access control model. For instance, the model allows to assign a trust value to each contact. Each time the SNS users share a new item, they define a minimum trust value required to see the item. Once a contact wants to access this item, the previously defined contextual constraint is evaluated. If the contact's trust value is higher than the trust value required to see the item, access is granted while otherwise access is denied [12].

4 Conclusions

The rise of SNSs and the accompanied change in our social lives and communication habits have not only brought along benefits but also worrying developments and considerable threats. Since then, privacy in SNSs has been an important

topic both for academia and the general public. In this paper, we presented our research efforts concerning privacy in SNSs in general. First, we emphasized the need for improving SNS privacy by presenting the results of a user study we conducted. In this regard, we conceptualized privacy as awareness and control. Subsequently, we pointed out solutions to address these issues. Focusing on privacy awareness, we discussed the differences between SNS data types, introduced a novel matrix-based visualization to facilitate the users' understanding of their social roles, and presented a serious game to educate especially the younger users about the implications of their privacy settings. Regarding privacy control, we outlined a global and provider-independent social identity model to enable users to consistently manage their identities across multiple platforms, proposed a clustering algorithm discovering segregated audiences to assist the users in managing their contacts, and introduced a trust-based access control model to facilitate the management of the visibility of the users' items.

References

1. Beato, F., Kohlweiss, M., Wouters, K.: Scramble! your social network data. In: Fischer-Hübner, S., Hopper, N. (eds.) PETS 2011. LNCS, vol. 6794, pp. 211–225. Springer, Heidelberg (2011)
2. Bortoli, S., Palpanas, T., Bouquet, P.: Decentralised social network management. Int. J. Web Based Communities **7**(3), 276–297 (2011)
3. Buchegger, S., Schiöberg, D., Vu, L.H., Datta, A.: PeerSoN: P2P social networking - early experiences and insights. In: Proceedings of the 2nd ACM Workshop on Social Network Systems (SocialNets), pp. 46–52 (2009)
4. Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sänger, J.: Friend inspector: a serious game to enhance privacy awareness in social networks. In: Proceedings of the 2nd International Workshop on Intelligent Games for Empowerment and Inclusion (IDGEI) (2014)
5. Chen, C.H., Härdle, W.K., Unwin, A.: Handbook of Data Visualization. Springer, Heidelberg (2008)
6. Colantonio, A., Di Pietro, R., Ocello, A., Verde, N.V.: Visual role mining: a picture is worth a thousand roles. IEEE Trans. Knowl. Data Eng. **24**(6), 1120–1133 (2012)
7. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. **4**(3), 224–274 (2001)
8. Grimmelmann, J.: Saving Facebook. Iowa Law Rev. **94**(8), 1137–1206 (2009)
9. Kelley, P.G., Brewer, R., Mayer, Y., Cranor, L.F., Sadeh, N.: An investigation into Facebook friend grouping. In: Campos, P., Graham, N., Jorge, J., Nunes, N., Palanque, P., Winckler, M. (eds.) INTERACT 2011, Part III. LNCS, vol. 6948, pp. 216–233. Springer, Heidelberg (2011)
10. Kiili, K.: Digital game-based learning: towards an experiential gaming model. Internet High. Educ. **8**(1), 13–24 (2005)
11. Netter, M.: Privacy-preserving Infrastructure for Social Identity Management. Ph.D. thesis, University of Regensburg (2013)
12. Netter, M., Hassan, S., Pernul, G.: An autonomous social web privacy infrastructure with context-aware access control. In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) TrustBus 2012. LNCS, vol. 7449, pp. 65–78. Springer, Heidelberg (2012)

13. Netter, M., Riesner, M., Pernul, G.: Assisted social identity management - enhancing privacy in the social web. In: Proceedings of the 10th International Conference on Wirtschaftsinformatik (WI) (2011)
14. Netter, M., Riesner, M., Weber, M., Pernul, G.: Privacy settings in online social networks - preferences, perception, and reality. In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS), pp. 3219–3228 (2013)
15. Netter, M., Weber, M., Diener, M., Pernul, G.: Visualizing social roles - design and evaluation of a bird's-eye view of social network privacy settings. In: Proceedings of the 22nd European Conference on Information Systems (ECIS), pp. 1–16 (2014)
16. Peterson, C.: Losing face: an environmental analysis of privacy on Facebook. SSRN eLibrary (2010)
17. Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Bacon, K., How, K., Strong, H.: Expandable grids for visualizing and authoring computer security policies. In: Proceedings of the 26th SIGCHI Conference on Human Factors in Computing Systems (CHI), pp. 1473–1482 (2008)
18. Richthammer, C., Netter, M., Riesner, M., Pernul, G.: Taxonomy for social network data types from the viewpoint of privacy and user control. In: Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES 2013). IEEE (2013, accepted)
19. Richthammer, C., Netter, M., Riesner, M., Sänger, J., Pernul, G.: Taxonomy of social network data types. EURASIP J. Inf. Sec. **2014**(11), 1–17 (2014)
20. Riesner, M.: Provider-Independent Social Identity Management for Personal and Professional Applications. Ph.D. thesis, University of Regensburg (2013)
21. Riesner, M., Netter, M., Pernul, G.: An analysis of implemented and desirable settings for identity management on social networking sites. In: Proceedings of the 7th International Conference on Availability, Reliability and Security (ARES), pp. 103–112 (2012)
22. Riesner, M., Netter, M., Pernul, G.: Analyzing settings for social identity management on social networking sites: classification, current state, and proposed developments. Inf. Sec. Tech. Rep. **17**(4), 185–198 (2013)
23. Riesner, M., Pernul, G.: Maintaining a consistent representation of self across multiple social networking sites - a data-centric perspective. In: Proceedings of the Workshop on Security and Privacy in Social Networks (SPSN), pp. 860–867. IEEE (2012)
24. Riesner, M., Pernul, G.: Provider-independent online social identity management - enhancing privacy consistently across multiple social networking sites. In: Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS), pp. 800–809 (2012)