Who Got All of My Personal Data? Enabling Users to Monitor the Proliferation of Shared Personally Identifiable Information

Sebastian Labitzke

Who got all of my personal data? Enabling users to monitor the proliferation of shared personally identifiable information

Sebastian Labitzke

Karlsruhe Institute of Technology (KIT)
Steinbuch Centre for Computing (SCC) & Institute of Telematics
Zirkel 2, 76131 Karlsruhe, Germany
sebastian.labitzke@kit.edu

Abstract. The risk involved when users publish information, which becomes available to an unintentional broad audience via online social networks is evident. It is especially difficult for users of social networks to determine who will get the information *before* it is shared. Moreover, it is impossible to monitor data flows or to control the access to personal data *after* sharing the information. In contrast to enterprise identity management systems, in which provider-engineered processes control the access to and flow of data, the users of social networks themselves are responsible for information management. Consequently, privacy requirements have become important so that users can control the flow of their personal data across social networks and beyond. In particular, this kind of user-based information management should provide the capability to control data flows in a *proactive* manner, as well as *reactive* components to monitor the proliferation of data. In this conceptual paper, we motivate the necessity of a dedicated user-based information management on the basis of studies that we conducted on information that users share publicly in online social networks. Moreover, we outline the building blocks of user-based information management on the basis of existing approaches, which support users in managing data flows and an investigation that we did on the linkability of social network profiles. Furthermore, we contrast user-based information management with our experiences in developing and operating federated identity management services at the Karlsruhe Institute of Technology (KIT).[1]

1 Motivation

Today's users of online social networks (OSNs) are often unduly generous in sharing personally identifiable information (PII) via their OSN profiles. This fact is confirmed by the results of recent studies that we carried out [15], [14], as well as by many other previous investigations (e.g., [7], [16], [13]).

[1] We published a similar, but less comprehensive position paper on the workshop on the Federated Social Web (FSW), June 2011, Berlin, Germany.

In [15], we report, inter alia, which specific pieces of information OSN users share publicly. We analyzed 180,000 profiles of four popular OSNs for this (see Section 2 for more details), however, results showed two things. The first was that a great deal of information is publicly available despite the fact that privacy settings can be adjusted; secondly, the availability of specific pieces of information differs according to the OSN. We showed, for instance, that people tend to share information dedicated to business contacts via a business-driven social network and more private information through a network in which private contacts are gathered. The assumption could be made that users are aware of the target group of the shared information because of the type of network they are using.

However, it already seems to be difficult for users to determine who will be able to access a given piece of information before sharing it. To emphasize this, "Dunbar's number" says that the maximum number of people that humans are cognitively able to keep in touch with in terms of stable social relationships is 150 [5]. Keeping this figure in mind, Facebook states that an average user has 130 friends.[2] However, we found out that the standard deviation of the number of friends is very high (at about 216 regarding Facebook). In addition, in every network analyzed, we found some users with many more than 5,000 friends. At least, all of these friends have access to shared information, therefore information that was shared without giving much thought to it may be accidentally accessible to users who were not originally intended to get the information. Thus, OSNs should provide users with easy and comprehensible (proactive) features for choosing the group of receivers of a shared piece of information in a fine-grained manner.

Furthermore, it is essential to provide users with the ability to monitor who has access to which personal information over time, which information can be accessed by third parties, and which pieces of information can be linked to one another and in the end to the user as a physical person. On the one hand, this monitoring facility enables users to maintain an overview of their publicly available PII, i.e., an overview of the availability of their personal data *after* sharing the information. On the other hand, this monitoring capability has the potential to alert users to privacy risks and could be a motivation to use privacy settings more adequately. However, reactive components are not yet provided and users are not able to monitor the flow of their personal data.

We refer to a facility that combines the aforementioned proactive features with reactive capabilities to monitor and control data flows as an *Information Management Assistance System (IMAS)*. We are aware of the fact that the idea of supporting users in preserving their privacy is not new, particularly in light of the ideas and prototypes grown in the EU research projects PRIME[3] and PrimeLife[4] and in terms of privacy and transparency enhancing technologies. However, the concept presented in this paper covers a novel perspective of the

[2] https://www.facebook.com/press/info.php?statistics.
[3] https://www.prime-project.eu/.
[4] http://www.primelife.eu/.

requirements of such support features. The difference between this concept and existing approaches is discussed in Section 2 and the following parts of the paper.

In this paper, we start by contrasting user-based information management in terms of the aforementioned IMAS and "conventional" enterprise identity management. The aim of this comparison is to figure out the parallels of both management perspectives. Moreover, we formulate the requirements for an IMAS transferred from the experiences that we gained by developing and operating enterprise identity management systems at KIT. In addition, we relate these requirements to existing features, which support users in the management of their PII as well as identify existing gaps. This paper is more of a conceptual than technical paper that, inter alia, motivates and introduces a novel perspective on the requirements for privacy preserving features. In particular, we point out that the aforementioned reactive part of an IMAS is not yet in place. However, we demonstrate a building block of a reactive component that could serve as a basis to enable users to reactively monitor the proliferation of shared PII. In summary, the contributions of this paper are:

- Comparison of enterprise identity management processes with "user-based" information management with respect to monitoring and control of data flows
- Requirement analysis regarding proactive and reactive information management assistance
- Comparison of identified requirements with the status quo of provided features that allow the management of personal data flows
- Identification of the building blocks for reactive monitoring capabilities, which are not available today

The paper is structured as follows. Section 2 provides more insights into our previous investigation of publicly available information of OSN users. Furthermore, this section highlights related work, as well as recent statements of researchers working in the field of OSN analysis. Section 3 starts by introducing identity management concepts implemented at the Karlsruhe Institute of Technology (KIT). Subsequently, these concepts and related experiences are contrasted with the current opportunities available to OSN users for monitoring and controlling the proliferation of personally identifiable information in OSNs. Section 4 introduces the concept of an information management assistance system (IMAS), which could tackle the requirements that have been identified to support users in managing the proliferation of their data. Section 4.1 differentiates the capabilities of an IMAS from existing user-centric mechanisms, whereas Section 4.2 outlines the building blocks of such a system, which does not yet exist. Section 5 concludes the paper.

2 Related work

Many studies have been published that deal with user behavior and self-disclosure with regard to personal data in OSNs (see [14] and [15] for a detailed

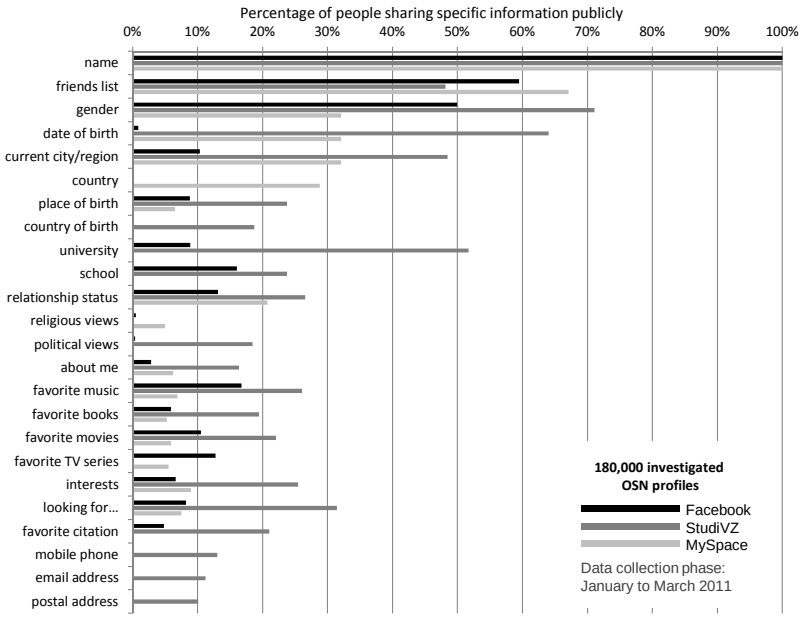

Fig. 1. Publicly available attributes of OSN users

discussion on related work). In particular, the availability of specific pieces of information in the OSN profiles were investigated. Recently, we showed that the date of birth is available in between 0% and 64% of user profiles depending on the OSN. The current residence is available in up to 48% of all analyzed user profiles. Up to 51% of users reveal the name of their university and up to 18% of users share their political and/or sexual orientation publicly. See Figure 1 and [15] for further results of this investigation. However, we also discovered that friends lists are available in a huge amount of OSN profiles (between 48% and 67% depending on the OSN) and we showed that such friends lists can be (ab-)used to gather and link various pieces of information about a single user shared in different OSN profiles.

With privacy settings, OSNs enabled users to restrict access to shared information. In comparison with the results of earlier studies([7], [16], [12], [19]), the results of [15] showed that an increasing number of OSN members are making use of privacy settings. However, we showed that only 7% to 22% of the users of the four OSNs analyzed have hidden their profile *completely* from strangers. Thus, we revealed that many users still do not make adequate use of the privacy settings provided or do not use them at all. As early as 2004, Acquisti stated that the provided *technology* is not effective if the *risk awareness* of users is not yet in place [1]. Recently, Krishnamurthy said, "from an awareness point of view, the situation is pretty bad" [11]. These statements provide the motivation for developing an IMAS, a system which has the potential to establish an appropriate awareness on the user side.

The aim of the European research project *digital.me* is to implement capabilities that are similar to those that we defined as the requirements for the proactive part of an IMAS [17]. With digital.me, users will be empowered to keep an overview of the pieces of information they provided to integrated services, such as OSNs. Within other projects, like the EU projects *PRIME* and *PrimeLife*, researchers have also investigated features that support users in keeping track of third parties to which they provided specific pieces of information. As early as 2005, in the context of the PRIME project, the authors of [3] assessed the idea of a system that supports users in preserving their privacy. Inter alia, in [2], the privacy-enhanced social network site *Clique* is introduced. This site provides users with the capability of segregating the audience of PII that is to be shared. It also provides options to define the accessibility of shared PII in a fine-grained manner. The authors of [6] investigated a user interface called Data Track to support people in maintaining an overview of their provided PII. In 2009, XML co-developer Eve Maler,[5] presented a similar mock-up (called *CopMonkey*) at the European Identity Conference (EIC). CopMonkey represents a system that serves as a tool for assessing the given privacy status of a user. In particular, the design and investigation of such mock-ups, as well as related implementations, such as the Clique tool, are essential for assessing the usability of such features and providing support in maintaining an overview of the services and audiences with whom a user has shared PII. However, all of these approaches only cover the proactive part of the requirements identified for an IMAS. An exception to this is the PrimeLife Data Track that provides also capabilities to get online access to PII stored by a service provider. This capability goes beyond proactive control and could constitute a building block for reactive user support. Apart from that, the mentioned approaches only comprise granting control who will have access to the PII in an intended sharing procedure, as well as the capability to maintain an overview of which service or what audience a user has provided specific pieces of PII to.

In this paper, we would like to go one step further than the aforementioned approaches. We assess the requirement of being able to keep track of the *proliferation* of provided data in a reactive manner, i.e., a concept that aims at providing a feature to show users the PII that they have made available and their resulting current virtual appearance in OSNs, or rather the Internet. Of course, the idea of such a monitoring system is not completely new. In 2009, in the scope of the EU research project *PICOS*[6], the "control over usage and proliferation of PII" was identified as a major concern regarding the implementation of privacy-preserving social networks [21]. As well as in projects mentioned above, the proactive perspective of this concern is also discussed in several publications of the project PICOS (e.g., [10], [20]). On the contrary, the authors of [8] described an approach to preserve privacy in a reactive manner. They proposed a system that would allow users to view the log files of a specific provider. This would allow users to get information about third parties that received their PII

[5] http://www.xmlgrrl.com.
[6] http://www.picos-project.eu/.

from this provider. In contrast to this, the concept of an information management assistance system is different in that a provider is not required to allow access to internal information regarding forwarded PII. With the IMAS concept, information about the virtual appearance of a user is also not based solely on data gathered during the communication processes between a user and services, but rather it is based on analysis of data that is publicly available on the Internet and linkable to a specific user. In fact, the information about a user's virtual appearance consists of an aggregation of any accessible PII that is linkable to a user. Hence, the information is not limited to what happens with specific pieces of PII revealed to a specific provider. In point of fact, an IMAS provides a similar perspective on a user's own PII, which is proliferated through Internet services, such as a third party that is able to gather it and link it to a physical person. In Section 4.2, we discuss existing knowledge that could serve as a basis for such a reactive capability to monitor flows of PII.

3 Contrasting provider- and user-based information management

The following section distinguishes between data flows controlled by identity management (IDM) systems, developed for and operated in an enterprise environment, and the proliferation of PII in the area of OSNs. First, we outline the concepts of identity management systems implemented at the Karlsruhe Institute of Technology (KIT), as well as related experiences to provide examples of provider engineered identity management processes. Subsequently, we try to identify parallels and differences between IDM systems and OSNs with respect to flows of data, as well as capabilities for monitoring and controlling such flows. Finally, we determine how we can learn from the experiences in implementing IDM in an enterprise environment to implement effective technical solutions to help users maintain privacy in OSNs.

3.1 Identity management and related experiences at KIT

At KIT, we started to establish identity management systems and services within a project called Karlsruhe Integrated Information Management (KIM).[7] Today, we operate a federated data provisioning that provides user attributes to IT services of the KIT [18]. Federated provisioning constitutes a comprehensible, manageable and scalable identity management infrastructure. The distribution of PII and other attribute values is designed in a hierarchical fashion in order to maintain the independence and flexibility of the organizational units of the KIT. Figure 2 visualizes this federated provisioning approach. Authoritative resources provide user attributes to a central IDM system and this system prepares the data for sub-IDM systems and central services. Afterwards, the central IDM system distributes the data to the IDM systems of several organizational units, as

[7] http://kim.cio.kit.edu/.

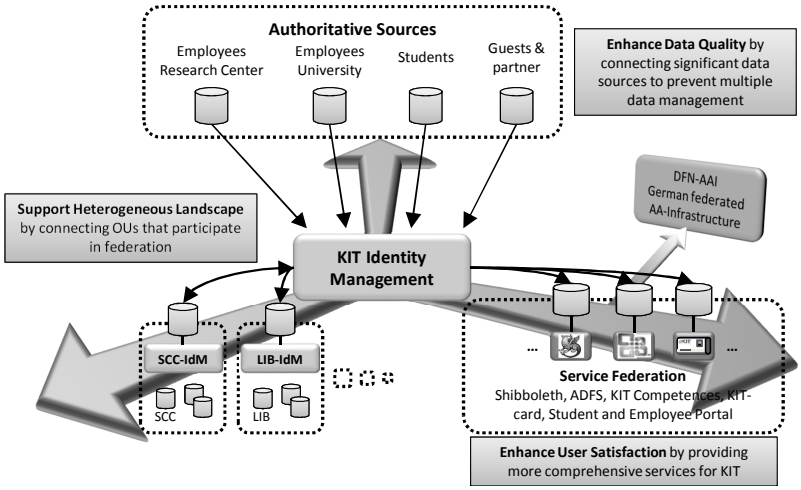

Fig. 2. Identity Management at Karlsruhe Insitute of Technology (KIT)

well as to cross-organizational services. This system also makes the intended attributes available to SAML-based authentication and attribute delivery services in the form of a Shibboleth identity provider (IdP). This IdP is, inter alia, part of the largest German Authentication and Authorization Infrastructure (AAI) for academia, which is operated by the German National Research and Education Network.[8] Additionally, we provide an inner organizational service federation at KIT and we have recently become involved in a new identity management project of the state of Baden-Württemberg, Germany (bwIDM). This bwIDM project aims at expanding web-based authentication and authorization federations, such as Shibboleth AAIs to support federated access to non-web-based services, such as SSH consoles. In this context, SSH consoles are needed to access high performance, grid, and cloud computing resources.

Based on experiences related to the development of introduced components, we learned how to implement identity management systems and services so that data flows can be controlled and managed in an appropriate manner to maintain privacy and compliance. Furthermore, drawing from our experiences, we found that technical issues are often less challenging than issues regarding the coordination and control of implementing IDM-related business processes. In this regard, communication and interaction between federation participants within provider-based federations play an important role. Furthermore, data protection regulations (that are absolutely necessary) often lead to enormous overhead during process designs. In short, the implementation of provider-based federations takes time due to the overhead with regard to the extensive coordination required and the design of compliant processes. Moreover, due to the absence of

[8] Das Deutsche Forschungsnetz (DFN).

standardized coordination structures to implement provider-based federations, some amount of overhead is unavoidable today.

Thus, from a technical point of view, today's developers know how to implement compliant IDM solutions. Furthermore, they are able to implement systems that guarantee user privacy inside organizational borders. Issues having to do with IDM in an enterprise environment are more or less concealed in the area of organization, the development of policies, and the collaboration of service providers and providers of IDM systems and services. In a broader sense, the real issues are shifting away from provider-based IDM to the federated management of services and, consequently, to a less technical area.

3.2 User-based federations

In turn, underlying difficulties and delays in implementing IDM services have inspired the popularity of services, in which the providers only offer the service itself, i.e., services that are provided without pre-configured data flows, such as in an enterprise IDM. Therefore, the configuration of data flows is not accompanied by the identified overhead of the provider-engineered IDM. In the following, we use the term *user-based federation* to include services and underlying processes that are not engineered solely by a provider, i.e., users are involved in the "implementation" of data flows and, therefore, in the proliferation of PII. For instance, Facebook provides the OSN as a service, users are responsible for the connections between entities. Therewith, they are "configuring" the underlying data flows. Moreover, user-based federations can be provided instantaneously because the users involved often do not have to communicate with each other to participate and interact. The operability of user-based federations does not depend on the functionality of the whole federation, i.e., the interconnectivity of every participant and the coordination of all participants at once. This might also be the reason why such user-based federations have recently become more popular.

The following example illustrates the user-based character of these services: It is possible to link the contacts stored on a smartphone with Facebook friends. If the friends update their email address, telephone number or other contact information via Facebook, this information is updated on every linked smartphone. This kind of feature forms a user-based federation because the implementation of the associated update functionality (a typical identity management service) largely takes place without the involvement of a provider. The corresponding processes, or rather the data flows, are not pre-engineered by a provider. Users initiate such processes, therefore, they may be involuntarily allowing such data flows.

3.3 Contrasting *inside* and *outside* perspectives

Figure 3 visualizes the organized, consolidated, and provider-engineered data flows managed and controlled *inside* organizational borders or within a distinct

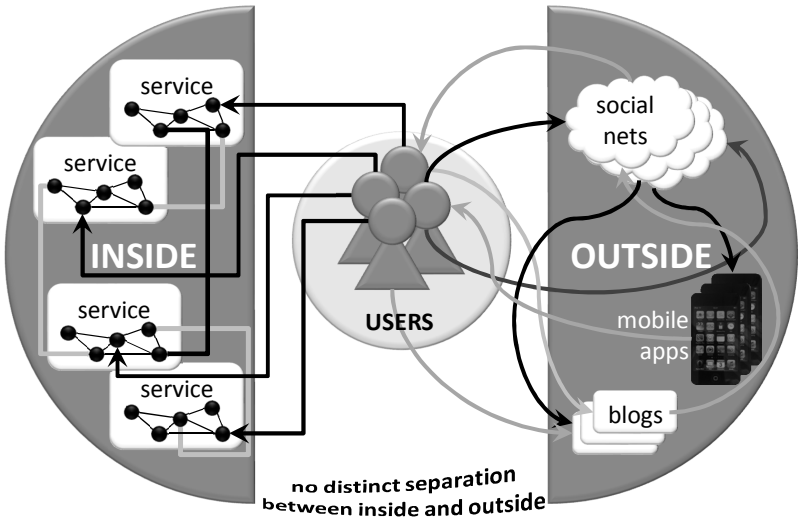

Fig. 3. Provider-engineered versus user-based services

federation on the left side of the picture. In contrast, the right side outlines user-based and incomprehensible data flows outside the borders of any organization or organizational federations, respectively. However, users are part of both sides, therefore the distinction between *inside* and *outside* becomes blurred. Thereby, the attractiveness of the *outside* is the simplicity of connecting to and exchanging information with other participants, which is completely the users' responsibility. The overhead regarding compliance and organizational efforts, as well as the communication between participating entities is reduced from the perspective of an OSN provider, as well as from the user's point of view. Otherwise, consolidated data flows *inside* organizational federations would be indispensable, particularly in light of the requirement to comply with data protection laws. The main similarity between provider-engineered and user-based federations is obvious as well: The implementation of both kinds of federations results in data flows that have to be monitored and controlled.

However, if users are responsible for the configuration of data flows outside of organizational borders, to some extent, they are also responsible for ensuring privacy. On the other hand, if users establish federations in the above described manner, they have to be provided with features similar to those that developers and administrators are provided with. This implies that before a user-based federation is provided, the participants should be able to have an overview of the consequences of their participation. This feature would be similar to the overview that a developer has of the design and implementation of identity management processes. Compared to the monitoring and management capabilities available to administrators of provider-based federations, users also have to be provided with reactive features for the control of data flows after the implementation of a user-based federation. We stress the point that an *Information Management*

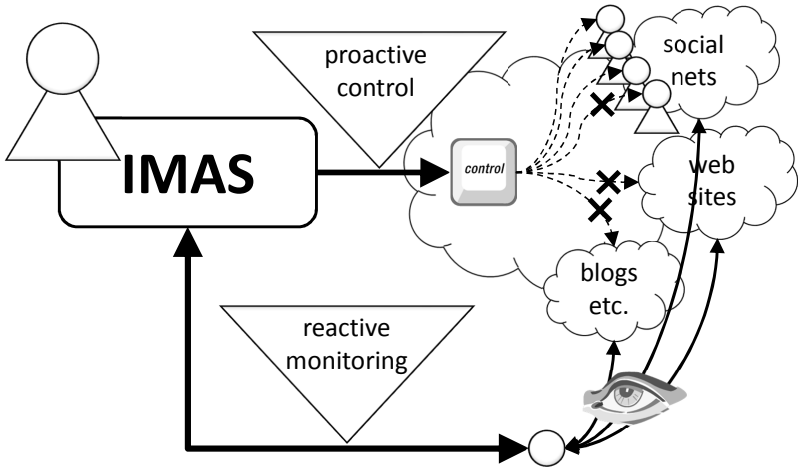

Fig. 4. Structure of an Information Management Assistance System

Assistance System (IMAS) with proactive and reactive components has to be available to users to support them in the implementation of comprehensible data flows in terms of user-based federations and the ability to monitor the data flows afterwards.

4 Information Management Assistance System

As mentioned before, the requirements for an Information Management Assistance System are very similar to the requirements in the field of enterprise identity management systems, apart from the fact that the roles of developer and administrator are not separate. In particular, the support required by users is similar to the technical support for people involved in the development and operation of enterprise IT.

Figure 4 shows the concept of an IMAS. The user is able to restrict the audience receiving the shared pieces of information. In the example given, a user shares information with a subset of his social network contacts, however, the information will not be spread via websites, blogs, etc. Moreover, the user is able to monitor the proliferation of shared information by use of the reactive components of an IMAS (also shown in Figure 4).

Since an IMAS has not yet been implemented, the question is whether there are disadvantages with such a system. A system that is able to reveal the proliferation of personal data could probably be used to link shared pieces of information to one another and to the user as a physical person. This function may constitute a threat for users if third parties are able to use an IMAS on the shared information of an arbitrary user. An IMAS would run in an environment that is far more open to the public than an enterprise IDM that is implemented inside a closed and secured network segment. Hence, the security requirements of an

IMAS are different from the requirements of an enterprise IDM. The aim is to ensure that only the users themselves be able to gather their own proliferated PII and to link such pieces of information to one another.

Whether an IMAS could be implemented on a compliant basis is also questionable. In order to detect proliferating personal data, the shared information of several users would have to be analyzed to decide whether a specific piece of information is part of the data that a specific user has shared. The processing required of information shared by other users, who have not given their consent, would not be compliant with data protection laws, like the German Data Protection Act.

However, besides the aforementioned potential disadvantages, an IMAS includes a facility that could help users keep track of data proliferation and motivate them to apply their privacy settings more carefully. In the following, we discuss the differences between the required proactive features of an IMAS with user-centric approaches to identify the status quo of the capability of users to allow or deny access to PII before the data has been forwarded to a third party. Afterwards, we target the reactive facility of an IMAS and focus on what can be learned from our previous studies. In particular, we outline the building blocks for reactive components based on the results of the investigation presented.

4.1 Contrasting an IMAS with user-centricity and transparency enhancing technologies

As described above, an IMAS should have proactive and reactive components. Currently, the proactive part is more or less known in terms of the efforts regarding user-centricity [4]. Authentication and authorization frameworks of projects, such as the Kantara Initiative UMA,[9] OAuth,[10] and OpenID,[11] to name just a few, often include a proactive information management component, which can be adjusted to deny or allow third parties access to the PII requested.

Due to the multitude of proactive components that come up with the aforementioned approaches, adjusting the provided settings adequately can be a challenge to users. User-controlled Automated Identity Delegation (UCAID) is an extension of user-centric federated identity management systems. With UCAID, users no longer have to approve each dissemination of information manually. UCAID ensures user control by means of user-defined dissemination policies [9].

These tools and standards enable users to allow or to deny third party providers to get the specific information requested. However, the implications of granting permission to access personal data are often not clear to users because today's tools only show that data is to be shared. The intended purpose of shared data is not displayed and if it is, is only implicitly comprehensible. Moreover, third party providers often request most of potentially available information and users merely be able to accept these request in their entirety.

[9] http://kantarainitiative.org/confluence/display/uma.
[10] http://oauth.net/.
[11] http://openid.net/.

It is not possible to pick and choose which information will be shared with a third party. Furthermore, without sharing all of the information requested, most services cannot be used.

This is why the previously mentioned EU research projects determined that there is a need for transparency enhancing technologies (TETs). TETs provide more sophisticated possibilities for monitoring and adjusting *access rights* to PII compared to the current user-centric authentication and authorization frameworks. As discussed in Section 2, these projects developed several approaches to support users in maintaining an overview of the audiences and service providers that were given specific pieces of PII and who are potentially able to access this shared information. However, such capabilities cannot guarantee, or rather monitor, whether the PII is forwarded and re-posted by third parties, such as users or service providers who have access to the information. Due to the fact that shared PII proliferates through social networks and does not usually stay within the context of the intended audience or service, we see the need to monitor the proliferation of PII in a broader manner compared to previous approaches of TETs. In the following, we outline knowledge that could serve as a basis for a more sophisticated monitoring capability.

4.2 A building block for reactive IMAS components

In contrast to approaches of proactive capabilities to control data flows, reactive components are not implemented today. Currently, users are not able to maintain an overview of the providers and users who received their personal data and therefore cannot know who has access to it, respectively.

In [15], we investigated an approach to demonstrate to users that their OSN profiles can be linked. We showed that several OSN profiles of a single physical person can be linked by third parties on the basis of comparisons between user friends lists. We argue that profile linking could be used to show users their own virtual appearance. Hence, users will be able to get bold and simple insights to information that could be linked to themselves. Therefore, this feature shows that gathering comprehensive information about users also presents opportunities for third parties.

Today's OSN users are not aware of how much information they reveal to third parties, especially considering the aforementioned linkability. The efforts to federate the social web by conducting several OSNs could facilitate the linkability of OSN profiles and consequently the linkability of the PII of OSN users. As a result, users will be even less able to keep an overview of the information proliferating through OSNs. Thus, there will be an ongoing need to monitor the proliferation of shared information. In this context, the linkability study could form a building block for a reactive IMAS component.

5 Conclusions

In this conceptual paper, we pointed out that people are unduly generous in sharing personally identifiable information via online social networks and that

adequate risk awareness regarding privacy does not yet exist. Consequently, we stated the necessity of a personal *Information Management Assistance System (IMAS)*. An IMAS should enable online social network users to control who will receive their shared data before they share information and monitor the flows afterwards. In comparison to federated enterprise identity management systems, such an IMAS would have monitoring capabilities that are analogous to the administrator's view of data flows. Furthermore, an IMAS should include capabilities that are similar to those of developers to implement controlled federated processes. We related the approaches of user-centricity and transparency enhancing technologies even further with the vision of an IMAS. We discussed the disadvantages of approaches for proactive IMAS components and showed that the approaches of reactive components do not go far enough in supporting a user sufficiently according to the requirements discussed. To this end, we presented parts of the insights that we gained from a study on the linkability of online social network profiles [15]. On the basis of this information, linkability to a feature could be implemented, which helps users to maintain an overview of third parties that are authorized to access shared information. However, the current building blocks of an IMAS (proactive and reactive components) are more or less isolated applications that do not fulfill all of the requirements identified. The biggest challenge is to combine, as well as improve the applications, projects and efforts mentioned in an integrative manner.

6 Acknowledgement

We would like to thank the anonymous reviewers for their invaluable comments.

References

1. A. Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*, EC '04, pages 21–29, New York, NY, USA, 2004. ACM.
2. B. Berg, S. Pötzsch, R. Leenes, K. Borcea-Pfitzmann, and F. Beato. Privacy in social software. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, *Privacy and Identity Management for Life*, pages 33–60. Springer Berlin Heidelberg, 2011.
3. M. Bergmann, M. Rost, and J. S. Pettersson. Exploring the feasibility of a spatial user interface paradigm for privacy-enhancing technology. In *Proceedings of the Fourteenth International Conference on Information Systems Development (ISD2005)*, pages 437–448, Karlstad, Sweden, 2005. Springer Verlag.
4. A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer. User centricity: A taxonomy and open issues. *J. Comput. Secur.*, 15:493–527, October 2007.
5. R. Dunbar. Coevolution of neocortex size, group size and language in humans. *Behavioral and Brain Sciences*, 16(4):681–735, 1993.
6. S. Fischer-Huebner, H. Hedbom, and E. Waestlund. Trust and assurance HCI. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, *Privacy and Identity Management for Life*, pages 245–260. Springer Berlin Heidelberg, 2011.

7. R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM.
8. H. Hedbom, T. Pulls, and M. Hansen. Transparency tools. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, *Privacy and Identity Management for Life*, pages 135–143. Springer Berlin Heidelberg, 2011.
9. T. Höllrigl, H. Kuehner, J. Dinger, and H. Hartenstein. User-controlled automated identity delegation. In *Proceedings of the 6th IEEE/IFIP International Conference on Network and Service Management*, 2010.
10. C. Kahl, K. Boettcher, M. Tschersich, S. Heim, and K. Rannenberg. How to enhance privacy and identity management for mobile communities: Approach and user driven concepts of the picos project. In *Proceedings of 25th IFIP International Information Security Conference Security & Privacy – Silver Linings in the Cloud (IFIP SEC 2010)*, 2010.
11. B. Krishnamurthy. I know what you will do next summer. *SIGCOMM Comput. Commun. Rev.*, 40:65–70, Oct. 2010.
12. B. Krishnamurthy and C. Wills. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, WOSP '08, pages 37–42, New York, NY, USA, 2008. ACM.
13. B. Krishnamurthy and C. Wills. On the leakage of personally identifiable information via online social networks. *SIGCOMM Comput. Commun. Rev.*, 40:112–117, Jan. 2010.
14. S. Labitzke, J. Dinger, and H. Hartenstein. How I and others can link my various social network profiles as a basis to reveal my virtual appearance. In *LNI – Proceedings of the 4th DFN Forum Communication Technologies, GI-Edition*, June 2011.
15. S. Labitzke, I. Taranu, and H. Hartenstein. What your friends tell others about you: Low cost linkability of social network profiles. In *Proceedings of the 5th International ACM Workshop on Social Network Mining and Analysis*, SNAKDD'11, San Diego, CA, USA, 2011. ACM.
16. C. A. C. Lampe, N. Ellison, and C. Steinfield. A familiar face(book): profile elements as signals in an online social network. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '07, pages 435–444, New York, NY, USA, 2007. ACM.
17. S. Scerri, R. Gimenez, F. Hermann, M. Bourimi, and S. Thiel. digital.me - towards an integrated personal information sphere. In *Workshop on the Federated Social Web Summit (FSW)*, 2011.
18. F. Schell, T. Höllrigl, and H. Hartenstein. Federated identity management as a basis for integrated information management. *it – Information Technology*, 51(1):14–23, March 2009.
19. J. Schrammel, C. Köffel, and M. Tscheligi. How much do you tell? information disclosure behaviour indifferent types of online communities. In *Proceedings of the fourth international conference on Communities and technologies*, pages 275–284, New York, NY, USA, 2009. ACM.
20. M. Tschersich, C. Kahl, S. Heim, S. Crane, K. Böttcher, I. Krontiris, and K. Rannenberg. Towards privacy-enhanced mobile communities – architecture, concepts and user trials. *Journal of Systems and Software*, 84(11):1947 – 1960, 2011.
21. S. Weiss. Privacy threat model for data portability in social network applications. *International Journal of Information Management*, 29(4):249 – 254, 2009.