Identity Management through "Profiles": Prototyping an Online Information Segregation Service

Julio Angulo and Erik Wästlund

Karlstad University,
Universitetsgatan 2, 651 88 Karlstad, Sweden
{julio.angulo,erik.wastlund}@kau.se

Abstract. Whereas in real everyday life individuals have an intuitive approach at deciding which information to disseminate to others, in the digital world it becomes difficult to keep control over the information that is distributed to different online services. In this paper we present the design of a user interface for a system that can help users decide which pieces of information to distribute to which type of service providers by allowing them to segregate their information attributes into various personalized profiles. Iterative usability evaluations showed that users understand and appreciate the possibility to segregate information, and revealed possible improvements, implications and limitations of such an interface.

Keywords: Usability, identity management, privacy preferences, partial identities, audience segregation, digital transactions.

1 Introduction

In everyday life individuals are frequently and naturally playing different social roles, as family members, professionals, hobbyist, activist, etc. Typically, people do not reveal all of their personal information to all of their different social groups, but rather they inadvertently and intuitively select the information that is suitable to share with members of a certain group depending on the context of a situation. Such phenomenon was first referred in the 1950's as *audience segregation* by sociologist Erving Goffman [15].

However, it can be claimed that in their 'digital lives' Internet users do not yet have the appropriate tools that help them manage their partial digital identities which let them segregate the information they distribute to different Internet services. For this reason, users tend to present similar identifiable attributes to many different service providers and to send more attributes than are actually needed to complete a transaction. Besides, nowadays users create different accounts with different services, which makes is hard for them to maintain and control which information is shared with whom. All these traces that users leave on the Internet could lead to higher probabilities of user impersonation, identity theft, profiling, and linkability attacks. A method for empowering users with control over their own personal information is needed as a way to minimize these risks.

M. Kurosu (Ed.): Human-Computer Interaction, Part III, HCII 2013, LNCS 8006, pp. 10–19, 2013.

Therefore, in our work we try to tackle the challenge of designing an interface for what we refer to as *information segregation*, or the act of encapsulating different pieces of personal identifiable information in order to present only those attributes to deliberately chosen online service providers.

In this paper we first look at some work related to audience segregation and the usability of Identity Management (IdM) systems. We then present an overview of the process of design for a system supporting the idea of information segregation along with the performed usability evaluations. Finally we list some implications and conclusions about our work.

2 Related Work

Attention has been given to the challenge of letting users select the audiences to with whom they wish to share the content in social network sites (SNS), seen for instance in [6] [7] [12] [16] [18] [20] [29]. Google+ is a SNS that makes its audience segregation features explicit through the use of so called *circles*. It has been argued that Google+'s users have a "clear understanding of circles, using them to target information to those most interested in it" [31], and it can be said that the circles' interface offers further desired properties of interactive systems, such as consistency, playability, pliability, learnability, affordance, and others, as suggested, for instance, by Löwgren & Stolterman [21] and other design heuristics.

However, there is a distinction between the act of segregating audiences in SNSs, which creates a tension between the "desire for controlling our own information and the desire for unplanned social interaction" [17], and the act of distributing personal information for receiving commercial online services or products, which is motivated by a need or desire of the service or product being requested or the experience it provides.

For this reason, some attempts have been done at allowing users to act under different identities while communicating online. These include the efforts from Mozilla's Persona[1] and Google's Multiple Chrome Users[2], as well as the obsolete Microsoft's CardSpace and Firefox's plugin "Sxipper". Nevertheless, these existing systems are either at a proof-of-concept stage, have limited functionality, acting mainly as role-based access controlled or password management systems, or are hard to understand and therefore hard to adopt by regular users.

Regarding the usability of IdM systems, the research done by Jøsang et al. [19] discusses different models for IdM and suggest a user-centric approach for the management of user identities. Similarly, Eap et al. [13] recognize the need to provide users with more control over their identities distributed over different service providers, stating that IdM systems should assist users in their adoption of identity management practices. Moreover, a prototype called DRIM (Dresden Identity Management) [10] tried to integrate identity management concepts on Internet browsers, and subsequent work carried out as part of the PRIME

[1] `http://www.mozilla.org/en-US/persona/`
[2] `http://www.chromium.org/user-experience/multi-profiles`

project[3] has also realized the need for interfaces that support the notion of partial digital identities [23]. Furthermore, Dhamija & Dusseault [26] list seven concrete observations taken from their experience dealing with the design and analysis of security systems, trying to inform the reader why such systems often fail and ways to improve them. Alpár et al. [1] present some of the security, privacy and usability issues encountered in current IdM systems and propose recommendations for their improvement in each of these areas.

3 Conceiving an Interface for Information Segregation

3.1 Assumptions and Requirements

While conceiving an interface of a system that supported the idea of information segregation, we made assumptions about the architecture and the role that different parties would play in this envisioned system. For one, we assumed that an architecture is in place similar to the one suggested in the European projects PRIME and PrimeLife [8]. This implies that the system could be equipped with anonymous credentials technology (such as the one suggested by IBM's IdeMix [9]), and with a privacy policy matching engine (similar to the Platform for Privacy Preferences (P3P) [27] or the PrimeLife Policy Language (PPL) [5]) which can empower users to provide informed consent at the moment of releasing personal information.

However, in contrast to the architecture proposed in PrimeLife, it is assumed that the users' personal information is not stored locally on their devices, but instead it is stored centrally in a secure and privacy-friendly manner, for example in a cloud service provider.

It is also assumed that the proposed system can come in contact with different identity providers that are able to provide users with certified proofs of their identity. Similarly, online retailers would be able to offer their customers the possibility to complete a digital transaction using the certified or non-certified attributes contained within the customers' partial identities.

3.2 Design Approach

By following an iterative process of design, we created a series of sketches and lo-fi prototypes during three initial iteration cycles. The aim was to evaluate the use of different segregating metaphors, terminologies used, users' understanding of the concept of information segregation, as well as the intuitiveness of the interactive elements, look-and-feel of different design layouts and other visual aspects of the interface. Early evaluations actually revealed that participants consistently used the word *profiles* to refer to partial identities; therefore, we decided to give the name of "Profiles" to the IdM service being prototyped.

[3] PRIME - Privacy and Identity Management for Europe. `www.prime-project.eu`

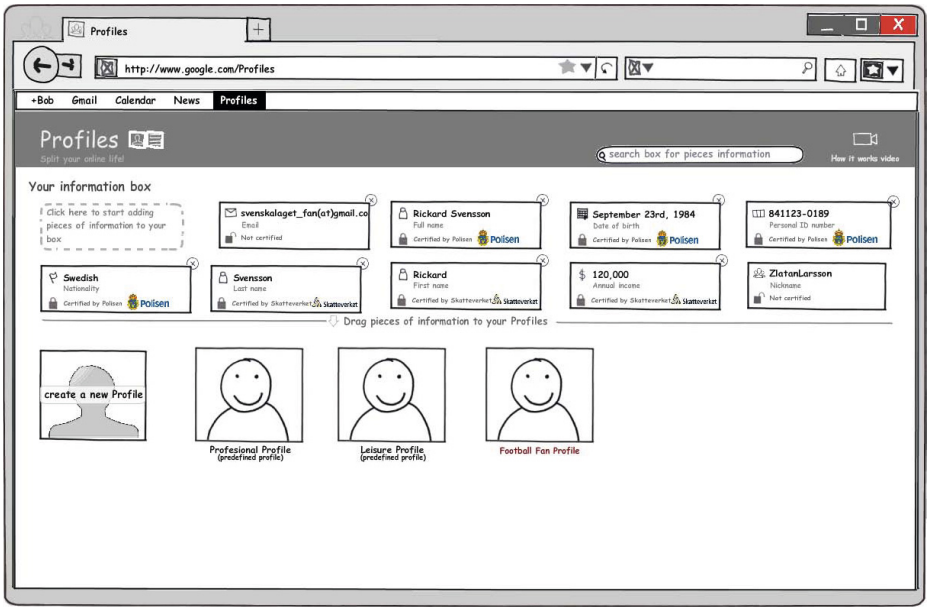


Fig. 1. A view of the "Profiles" prototype allowing users to manage their pieces of information at the top and their profiles at the bottom

Final Design Proposal. The final design proposal of the interface (depicted in Figure 1) can be briefly described as being divided into two panels. The top panel has a prominent label that reads '*Your information box*" conveying to users that it is a *place* where they can add, remove and manipulate their different pieces of information. Figure 2 represents an example of the look-and-feel of a piece of information, where users can see the attribute value of the information (the actual credit card number), the type of information (credit card), whether it is certified or not, and by which third party it has been certified. When users want to add a piece of information a dialog pops-up, where users can choose to either add non-certified attributes by typing them manually (Figure 3(a)) or to download certified attributes from a trusted identity provider (Figure 3(b)). As mentioned earlier, it is assumed that a list of trusted identity providers is already populated.

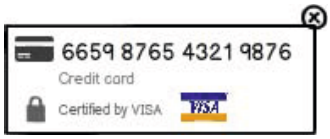
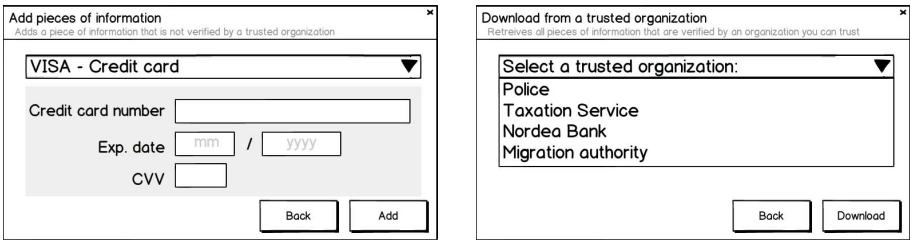


Fig. 2. The look of a piece of information

The bottom panel of the interface enables users to create and manage their different partial identities, or profiles. Results from the evaluations of earlier iterations indicated that users had a hard time giving relevant names to their profiles, therefore the interface provides a set of predefined profiles as a way to help first time users to get started and understand the purpose of the system. Profiles can be created and populated by clicking on the "create a new profile" icon, or by dragging one or many pieces of information onto them.



(a) Adding non-certified attributes manually

(b) Downloading certified attributes from a trusted identity provider

Fig. 3. Dialogs allowing users to add pieces of information

Every time pieces of information are added, users are given the option of selecting their preferences for the purposes for which service providers can use that information. For instance, users can specify that their credit card information should only be used for payment purposes. In this way, users can be informed if service providers respect their wishes during a digital transaction as explained in [3] [11]. Previous studies have shown the difficulty of users when stating their privacy preferences [11] [14] and to appropriately set privacy settings that would match their expectations to the reality of the protection of their privacy [22]. Given these observations, we realized through the different design iterations that the burden of setting such preference should be removed from users whenever possible, providing them with privacy-friendly default values as recommended, for instance, by data protection authorities. More importantly, the interface should promote the act of setting privacy preferences only in a moment that is relevant to the action at hand (as also suggested in [2]), for instance when information is added to a profile or when it is going to be distributed to service providers.

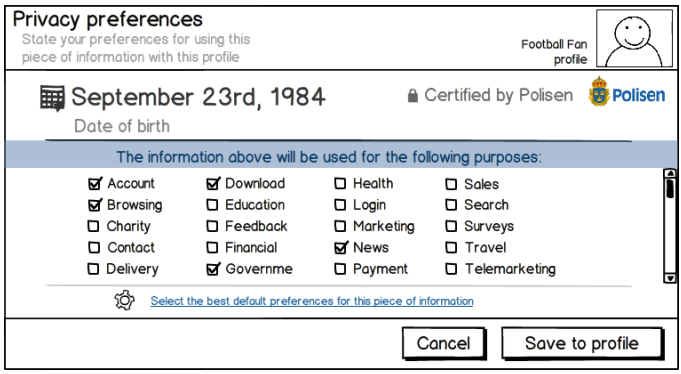


Fig. 4. Dialog allowing users to set the preferences of usage for the information pieces they add to a profile

3.3 Usability Evaluations

The initial design iterations were evaluated using different methods, such as eye-tracking technology, cognitive walkthroughs, thinking aloud protocols and questionnaires. Also, expert evaluations and feedback from professionals in the fields of e-commerce and identity management were taken into account. Results from these evaluations allowed us to identify possible improvements to the interface, and indicated that participants understood and appreciated the purpose behind information segregation.

For the final design iteration two main evaluation activities were carried out: usability tests using an interactive prototype and a focus group session. During the usability tests, all participants ($n = 12$) first answered a pre-questionnaire about their Internet habits and familiarity with existing audience segregation features in popular SNSs. Then, in the form of a cognitive walkthrough [24] they were asked to perform a series of tasks using an interactive prototype representing a scenario in which they were supposed to setup the "Profiles" system in order to make a purchase with an online service provider. The participants opinions and interactions with the prototype were noted as they went through each task, and they were also asked whether they considered a task to be easy or difficult to accomplish. At the end, participants answered a post-questionnaire including questions about the usability of the program, their understanding of its information segregation features, and PET-USES Likert-scale statements which aim to measure the secondary goals of users when interacting with privacy enhancing technologies, as presented in [30].

During the focus group session participants ($n = 30$) were first shown a demonstration of the "Profiles" interface and its privacy features. In order to encourage discussions and minimize 'group think' [28] participants were divided into smaller groups of 5 to 8 people. They were asked to discuss possible uses and improvements of the proposed interface with the other group members.

Summary of Results. From 12 participants that completed the cognitive walktrough phase, 8 had a very good intuitive idea of the purpose of the prototype, stating for example that "*the top lets you write pieces of your information, the bottom lets you create a profile with some of the pieces you wrote already in the top.*" Adding non-certified pieces of information was understood easier than downloading certified information, probably because users' unfamiliarity with the concept of certificates. However, after having downloaded certified information the first time, 11 out of 12 participants understood it well the second time they were asked to add certified information into the system. Observations also revealed that users were able to set privacy preferences easily, however in the post-questionnaire they reported this task as being the hardest to accomplish, suggesting a paradoxical view of privacy settings.

Participants from the focus groups session expressed, among other things, their concerns about centralizing all pieces of information in a single program: "*if a hacker gets into the program, then they will have all that information from me given by the Police, the Bank, etc.*". Moreover, they discussed the usage of

such a system that would fit their current situation and address their needs at hand. For instance, they envisioned a scenario where having a series of profiles could facilitate the way a user can look for different job positions that might require different information.

The complete list of tasks that participants were asked to go through, the instructions given during the focus group session and a detailed account of the results of the evaluations can be found in the technical report presented in [4].

3.4 Implications

Based on the process of design and the results from the evaluations, the following points present some of the major considerations to be taken when designing an IdM system like the one suggested hereby.

Progressive and Contextual Formation of Partial Identities. Since the early stages of design it became obvious that one of the major challenges would be to conceive an interface that would encourage users to start interacting with such a technology and adopt it for their routinary digital transactions. Thus, it is important to keep in mind that the users' first interactions with the system should be effortless, intuitive and perceived as useful at a moment that is relevant to what they are trying to achieve (e.g., purchasing a product through an online service). As stated in [26], "identity management is not a goal in itself", thus forcing users to, for instance, populate the system with many personal attributes so that it can work effectively during a purchase, will most likely discourage users to continue using it.

Instead, a progressive approach should be adopted in which users start by forming a partial identity in a simple way, gradually adding pieces of information as they are needed and creating identities at their own pace. The system should resemble to some extent the way identities are formed in real life and the contexts in which real identities evolve [1], consisting of progressive steps and determined by relevant life events, such as getting married, changing jobs, or opening a new bank account.

Maintaining Different Profiles. Creating different profiles could have the disadvantage that those profiles have to be maintained over time, which can become a burdensome task if users need to continuously monitor and update the information and the online services that they have associated with each profile.

A centralized solution would allow users to maintain their profiles across different devices over the air, which could provide convenience and further promote the gradual development of these partial identities. In this way, users would be able to access their profiles whenever and wherever they wish to do so, continuously evolving their identities 'on the fly' under relevant contexts of use in a progressive manner (a similar approach has been suggested during the PRIME and PrimeLife projects as presented in [3]).

Setting Privacy Preferences. Designing interfaces for letting users set their privacy preferences proved to be a difficult challenge. It was not until the final design suggestion that we thought we had come up with a simple enough mechanism to achieve this (seen in Figure 4). However, results from the post-questionnaire indicated that users still perceived this as a difficult step to complete.

What we have learned is that a system handling privacy preferences should relieve users from having to set those preferences from scratch, and instead a good set of privacy-friendly preferences, as defined by a trusted authority, should already be selected by default. The option to set or modify those preferences should not be made a priority, but should be made available within a context that a user will understand; for instance, at the moment of having to disclose information to a service provider, where she could, if she is interested or concerned, specify the purposes of usage of her data and other conditions.

4 Concluding Remarks

We have presented a design proposal for a system that enables users to group their information pieces into self-defined partial identities, or *profiles*. We refer to this act as information segregation. The suggested approach allows users to define the preferences for the data attributes contained within each profile, and to use those profiles at the moment of contacting specific applications or groups of online services with certain similarities, thus helping users protect their privacy by having a clearer approach to control their data and minimizing the personal information they disclose under certain application contexts.

We are aware of some of the limitations of the suggested interface. For one, difficulty of visualizing large amounts of pieces of information and managing more profiles than can be displayed on different screen screen sizes has not been fully considered. The level of complication can escalate when the formation of *sub-profiles* is taken into account (e.g., having a health profile that can be subdivided into pharmaceutical services, health clinic consultations, health clinic administration, etc.). Moreover, the users' understanding on how their information flows, where is it located (remotely or locally) and how it is handled by the IdM system is still unexplored (e.g., do users understand, or care about, what happens when they delete a piece of information?). Similarly, the possible steps to be taken to populate the system with trusted identity providers has not been considered. Additionally, we are aware of the privacy and security consequences that can arise from having all users' data in a centralized remote location; however, following a privacy-friendly architecture as presented in [25] can ensure users' privacy even towards the cloud service which stores the users' data.

Despite its limitations, we see this study as an exploratory approach towards useful privacy-friendly IdM systems. As part of future work we are working on creating scenarios where specific profiles might be employed (e.g., e-health or e-banking profiles) during a digital transaction. Also, we plan to work on adapting the interface to touch-screen devices of different sizes, and study the users' mental models of the location of their data as well as of the data flows

between devices and entities involved in a digital transaction. Moreover, in future iterations the mechanisms for specifying privacy preferences will be extended to not only include the purposes of data use, but also data retention periods, deletion obligations and other similar conditions.

Acknowledgments. This work is funded by a Google Research Award and the Swedish Knowledge Foundation (KK-stiftelsen) through the U-PrIM project. We would like to thank our colleagues Martin Ortlieb, Stephan Micklitz, Peter Gullberg, Simone Fischer-Hübner and Tobias Pulls.

References

1. Alpár, G., Hoepman, J.H., Siljee, J.: The identity crisis. Security, privacy and usability issues in identity management. Computer Research Repository (CoRR) (2011)
2. Angulo, J., Fischer-Hübner, S., Pulls, T., König, U.: HCI for Policy Display and Administration. In: PrimeLife - Privacy and Identity Management for Life in Europe, ch. 14, p. 261. Springer (June 2011)
3. Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E.: Towards usable privacy policy display & management. Information Management & Computer Security 20(1), 4–17 (2012)
4. Angulo, J., Wästlund, E.: Identity Management for online transactions - Using "Profiles" to segregate personal information. Tech. rep., Karlstad University, Karlstad, Sweden (April 2012), `http://www.is.kau.se/julioangulo/angulo/publications/2012/2012_IdentityManagementForOnlineTransactions.pdf`
5. Ardagna, C.A., Bussard, L., Di, S.D.C., Neven, G., Paraboschi, S., Pedrini, E., Preiss, S., Raggett, D., Samarati, P., Trabelsi, S., Verdicchio, M.: Primelife policy language. In: Proceedings of the W3C Workshop on Access Control Application Scenarios, Luxembourg (November 2009)
6. van den Berg, B., Pötzsch, S., Leenes, R., Borcea-Pfitzmann, K., Beato, F.: Privacy in social software. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity Management for Life, pp. 33–60. Springer, Heidelberg (2011)
7. van den Berg, B., Leenes, R.E.: Audience Segregation in Social Network Sites. In: Proceedings for the Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust, pp. 1111–1117. SocialCom/PASSAT, SSRN, Minneapolis, USA (2010)
8. Camenisch, J., Fischer-Hübner, S., Rannenberg, K.: PrimeLife - Privacy and Identity Management for Life in Europe, 1st edn., vol. 14. Springer (June 2011)
9. Camenisch, J., van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 21–30. ACM (2002)
10. Clauß, S., Kriegelstein, T.: Datenschutzfreundliches identitätsmanagement. Datenschutz und Datensicherheit 27(5) (2003), `http://dblp.uni-trier.de/db/journals/dud/dud27.html#ClaussK03`
11. Cranor, L.F., Guduru, P., Arjula, M.: User interfaces for privacy agents. ACM Trans. Comput.-Hum. Interact. 13(2), 135–178 (2006)
12. DiMicco, J.M., Millen, D.R.: Identity management: multiple presentations of self in facebook. In: Proceedings of the 2007 International ACM Conference on Supporting Group Work, GROUP 2007, pp. 383–386. ACM, Sanibel Island (2007)

13. Eap, T.M., Hatala, M., Gasevic, D.: Enabling user control with personal identity management. In: IEEE International Conference on Services Computing, SCC 2007, pp. 60–67. IEEE, Salt Lake City (2007)
14. Fischer-Hübner, S., Pettersson, J., Bergmann, M., Hansen, M., Pearson, S., Mont, M.: Human-Computer Interaction. In: Camenisch, J., Leenes, R., Sommer, D. (eds.) Digital Privacy. LNCS, vol. 6545, pp. 569–595. Springer, Heidelberg (2011)
15. Goffman, E.: The presentation of self in everyday life. Doubleday (1959)
16. Gonçalves, J.: Groupster: Narrowcasting on Social Networking Sites. Master's thesis, Madeira Interactive Technologies Institute, University of Madeira (2011)
17. Grimmelmann, J.: Saving Facebook. Iowa Law Review 94(4), 1137–1206 (2009)
18. Gross, R., Acquisti, A.: Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES 2005, pp. 71–80. ACM, New York (2005)
19. Jøsang, A., Zomai, M.A., Suriadi, S.: Usability and privacy in identity management architectures. In: ACSW Frontiers, pp. 143–152 (2007)
20. Kairam, S., Brzozowski, M., Huffaker, D., Chi, E.: Talking in circles: selective sharing in google+. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2012, pp. 1065–1074. ACM, New York (2012)
21. Löwgren, J., Stolterman, E.: Thoughtful Interaction Design: A Design Perspective on Information Technology. MIT Press (2007)
22. Madejski, M., Johnson, M., Bellovin, S.M.: The failure of online social network privacy settings. Tech. rep., Columbia University (2011), http://www.futureofprivacy.org/wp-content/uploads/2011/07/TheFailureofOnlineSocialNetworkPrivacySettings.pdf
23. Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauss, S., Kriegelstein, T., Krasemann, H.: Making PRIME usable. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS 2005, pp. 53–64. ACM, New York (2005)
24. Polson, P.G., Lewis, C., Rieman, J., Wharton, C.: Cognitive walkthroughs: a method for theory-based evaluation of user interfaces. International Journal of Man-Machine Studies 36(5), 741–773 (1992)
25. Pulls, T.: Privacy-friendly cloud storage for the data track. In: Jøsang, A., Carlsson, B. (eds.) NordSec 2012. LNCS, vol. 7617, pp. 231–246. Springer, Heidelberg (2012)
26. Dhamija, R., Dusseault, L.: The Seven Flaws of Identity Management: Usablity and Security Challenges. IEEE Security & Privacy Magazine 6(2), 24–29 (2008)
27. Reagle, J., Cranor, L.F.: The platform for privacy preferences. Commun. ACM 42(2), 48–55 (1999)
28. Rubin, J., Chisnell, D.: Handbook of usability testing : how to plan, design, and conduct effective tests. Wiley Publ., Indianapolis, Ind. (2008)
29. Tootoonchian, A., Saroiu, S., Ganjali, Y., Wolman, A.: Lockr: better privacy for social networks. In: Liebeherr, J., Ventre, G., Biersack, E.W., Keshav, S. (eds.) CoNEXT, pp. 169–180. ACM (2009)
30. Wästlund, E., Wolkerstorfer, P., Köffel, C.: PET-USES: Privacy-enhancing technology – users' self-estimation scale. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G. (eds.) IFIP AICT 320. IFIP AICT, vol. 320, pp. 266–274. Springer, Heidelberg (2010)
31. Watson, J., Besmer, A., Lipford, H.R.: +your circles: sharing behavior on google+. In: Proceedings of the Symposium on Usable Privacy and Security, SOUPS 2012, pp. 12:1–12:9. ACM, New York (2012)