Designing privacy-aware online social networks - A reflective socio-technical approach

Andreas Poller
Fraunhofer-Institute for
Secure Information Technology
64295 Darmstadt, Germany
poller@sit.fraunhofer.de

Petra Ilyes
Goethe University
60123 Frankfurt, Germany
ilyes@em.uni-frankfurt.de

Andreas Kramm
Goethe University
60123 Frankfurt, Germany
akramm@rz.uni-frankfurt.de

Abstract

Current empirical studies of online social networks comprehensively describe users' experiences with interactional privacy management but provide only little concrete software design assistance to address identified privacy issues. We argue that the scarceness of practical guidelines to tackle privacy issues through software design might be due to the research approach. We suggest focusing more on the interplay between user and technology to understand the design options we actually have. In this contribution we first present our research concept based on the mapping of relations between users and technology, and we then describe the challenges for privacy frameworks and privacy metrics involved in this approach.

Keywords
User studies, online social networks, Facebook, socio-technical system, socio-technical design

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous

Introduction

While online social networks (OSNs), notably Facebook, attract millions of users around the globe, their downsides are increasingly discussed. Indeed, a large body of empirical studies highlights users' difficulties to manage their interactional privacy in OSNs, that is, between the users, and between users and the interface. Many studies have tried to explore how to support users' privacy management with appropriate and feasible OSN software features. [3]

However, results in this respect are comparatively meager so far: although available studies allow valuable insights into users' practices and concepts, design suggestions are often rather general, describing overall goals or calling for new solutions, but rarely expound

CSCW '13 Measuring Networked Social Privacy Workshop, February 23 – 27, 2013, San Antonio, Texas, USA.

concrete steps or strategies on how to get there. This raises the question as to how we can extend our current research approaches in order to provide more tangible guidelines to the design of OSN software that is supportive of interactional privacy management.

To tackle this question, we first have to deal with an epistemological issue: qualitative research methods we use to investigate into users' privacy issues are inherently interpretive but do not provide "hard facts". [1] Our interpretation depends on the definition of our research problem and the research approach we take. Hence, we have to reflect carefully what we need to actually observe for guiding software design. Moreover, we have to factor in software design into the definition of our research problem from the very beginning, and have to align it with our research approach.

But what is the research problem we must focus on? A good starting point is to bear in mind that software developers can support (or obstruct) users' privacy management solely through the technological artifact, i.e., through the OSN software they produce. However, this seemingly obvious observation has far-reaching consequences: users and technology are entangled and mutually constitute the OSN as a socio-technical association. The technological design of OSN software shapes users' concepts of its functioning and purpose, and these concepts, in turn, shape how users actually employ the software to share personal data and to act within the OSN community. On the other hand, once particular user practices emerge in the OSN, users may again change their concepts of the socio-technical association.

To understand how software design may effect users' concepts and practices, we suggest to investigate and map the interplay between users and technology, e.g., how user practices are reflected in technical processes (technical data flows and events), and how, in turn, these processes shape users' concepts and practices. Existing empirical studies often neglect this interplay, and at best loosely describe relations between use practices and technical data. Such studies are appropriate to answer a variety of important research questions, e.g., how new technology changes the way people communicate and interact. They can certainly deliver valuable starting points for further investigations. But for software design, we argue, they miss the socio-technical perspective.

For instance, researchers often observe that users emphasize privacy concerns as a central issue instructing their OSN use. However, upon examining these users' privacy settings researchers may discover rather permissive configurations. Many researchers may interpret this situation as contradictory, concluding that users are not sufficiently aware of the available privacy settings, and may suggest making privacy settings more visible, intelligible, and user-friendly. We want to argue, however, that all we may deduce from this observation is that data entered by a user are visible to a large audience, while the user claims to be privacy-aware. Now, our concern is that users engage workarounds to protect their privacy because they consider the given privacy settings as unsuitable for their purposes, e.g., by obscuring, or withholding, data, which, at worst, may restrict their use options. [2,4,7] This finding imposes challenges to software design that go beyond questions of, e.g., how to improve the visibility of privacy settings.

In our research, we want to refine existing research approaches to factor in the socio-technical perspective: We try to observe, specifically, the user-technology interplay to inform software designers. In particular, we investigate use practices and their technical manifestation concurrently. Thus, we are able to relate technical data and events to actual use practices, including practices users perceive as privacy infringements. On the basis of these mutually explicative data, software developers can specify software solutions to mitigate privacy issues. Examples for such solutions are automatic algorithms based on the technical data, semi-automatic algorithms supplemented by additional data such as configuration data, ratings, polar decisions, or algorithms that observe network interactions and search for privacy risk indicators.

In the case of users applying workarounds instead of the available privacy controls of the software described above, a software designer might use our approach to learn, e.g., whether software algorithms could detect and evaluate workarounds, and how software algorithms could suggest alternative solutions to users that serve the same purpose as the workaround without restricting use.

An interdisciplinary research approach to study the user-technology interplay

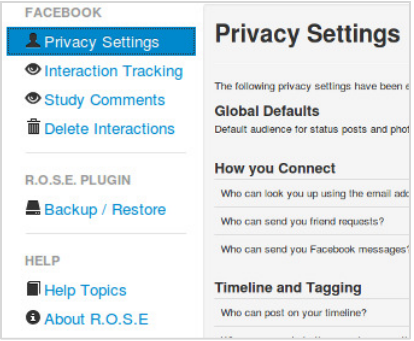
Methodology and Tool Development

Our practical approach to mapping the interplay between users and technology is to use a mixed-method approach, and apply it to questions of actual OSN usage, including the capture of in situ data on how user practices manifest on a technical level (“technical footprint”). To capture in situ data we developed a software tool - we call it ROSE (Research Tool for Online Social Environments) - that can be added to the web browser of our study participants. ROSE not only captures the technical footprint of user actions but also allows users to comment in situ on what they think of their own actions, and those of other users.

We developed ROSE in a long-term co-operation between computer scientist and anthropologists by establishing a mutual design framework. The anthropologists collect qualitative data about what users want to use OSNs for, and on users’ concepts of privacy issues ensuing from particular use practices. The computer scientists use these qualitative data for adapting ROSE so that it captures technical data that may be related to identified “privacy hotspots”. Privacy hotspots are situations or software functions often mentioned by users in the context of privacy issues. The anthropologists, in turn, use the collected technical data to refine their research design, and to investigate discrepancies between users’ concepts and actual technology use.

Research Procedure

For our empirical inquiry, we first ask our research participants to use ROSE for about two weeks. ROSE automatically captures their interactions in Facebook along with the effective privacy settings. It also captures in situ participants’ comments on their own and others’ sharing behavior. Except for the in-situ comment function, ROSE operates invisible in the background, but does not provide feedback to the users. ROSE differs from other browser tools that assist users in enhancing their privacy, or that increase their privacy awareness, e.g., tools visualizing privacy settings. [5] Unlike other observation techniques such



Privacy Settings

The following privacy settings have been e

Global Defaults

Default audience for status posts and phot

How you Connect

Who can look you up using the email adc

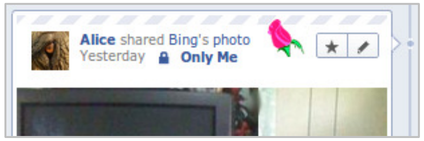
Who can send you friend requests?

Who can send you Facebook messages?

Timeline and Tagging

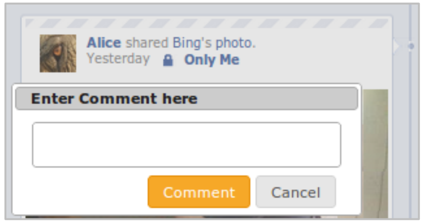
Who can post on your timeline?

Figure 1: User interface of ROSE displays the data collected during the observation phase of the study



Alice shared Bing's photo
Yesterday Only Me

Figure 2: ROSE icon embedded into a “Facebook Timeline” item; the study participant can click it to open a comment dialog



Alice shared Bing's photo.
Yesterday Only Me

Enter Comment here

Figure 3: ROSE comment dialog allows study participants to comment actions in situ

as screen capturing, ROSE is less intrusive as it aims to minimize interferences with the field. ROSE captures only basic technical events in a perfectly privacy-preserving manner (e.g., names and pictures are not recorded), provides the user with a human-readable list of the collected data, and allows the user to decide whether to provide the researchers with all the data or edit them, and supply only a subset thereof.

Following the data collection phase, we retrieve distinct action patterns for each of our study participants from the technical footprints gathered with ROSE. To this end, e.g., we count how often a user triggers an OSN function, and identify preferred privacy settings. Users' in-situ comments provide us with first insights into use contexts of the actions effecting the technical footprints, e.g., the reasons (context) for why a user shared a particular item (action) with close friends instead of a broader audience. This first analysis paves the way for the subsequent qualitative interviews with our participants.

In the interviews we ask our participants what they intended to achieve with those actions made visible by our tool. Also, we ask them to explain why they believe those actions will lead to the intended result.

In the final analysis, we compare user actions made visible through technical footprints with the meaning the users attribute to those actions. In this way, we can understand the status quo in terms of (a) how misconceptions of the available technical functions can lead to privacy issues, and (b) which privacy strategies users implement by creatively bending functions not intended for privacy protection purposes. Furthermore, we gain insights as to how we might redress the status quo by suggesting technical options based on our findings. How our insights can be applied depends on the concrete research question; in the following we provide two cases from our research work.

Privacy hotspots to investigate
We currently focus on two privacy hotspots that we - and other researchers - have identified:

Our ongoing research project pertains to the privacy hotspot we discussed above: privacy strategies and workarounds that users contrive rather than applying the standard privacy controls provided by the given OSN. With the aid of ROSE we are able to investigate users' workarounds at a technical level, and the consequences of these workarounds for their actions in the OSN, e.g., whether workarounds may actually impede a user's intention to interact, and share data in the OSN.

The analysis will help us to make design suggestions on how software can support those users whose privacy practices highly depend on workarounds. For example, we may advise whether, and under which circumstances, it is appropriate for software to suggest alternative privacy settings that do serve the same purpose as the user's workaround but do avoid their shortcomings.

Next, we want to research the second hotspot mentioned. It pertains to situations where different users have contradictory opinions about what sensitive information is, i.e., whether disclosing or sharing something is appropriate or not. Technical footprints, and the qualitative data from in-situ comments and interviews, allow us to search for technical indicators distinctive for conflicts in the interactional privacy of the OSN users. These indicators may serve as a basis for software algorithms supporting users in recognizing potential conflict situations.

Conclusion and Outlook

We argue that for designing software privacy features for OSNs conceived as socio-technical associations, our empirical research must aim at mapping the interplay between users and technology, a mapping we can achieve with our socio-technical research approach. We aim at refining this approach towards socio-technical design methodology, where computer scientists and anthropologists co-design privacy mechanisms in an open and iterative research process on the basis of a mixed-method approach interrelating technical data and qualitative data from the field. [6]

However, analyzing privacy issues through the socio-technical lens raises some challenging issues that consistently need attention in our future efforts: How can we consider, and highlight the user-technology interplay in our privacy frameworks? Can we distinguish between technical and non-technical factors contributing to interactional privacy issues? How can we be sure whether a particular software reinforces or mitigates privacy issues, that is, how do we know whether our findings are actually the result of the software design? And finally, can we better explain alleged contradictions between privacy concerns and researchers' interpretations of use practices through the lens of socio-technical associations?

Acknowledgements

We would like to thank Oliver Hoffmann, Sebastian Ruhleder and Steven Arzt for their exceptional programming work on ROSE. We would also like to thank Laura Kocksch for comprehensive ROSE testing, as well as all the students who have, at some point, and in some way, contributed to our research.

References

[1] P. Dourish. Implications for Design. In *Proc. CHI 2006*, ACM (2006).

[2] P. Kelley, R. Brewer, Y. Mayer, L. Cranor, and N. Sadeh. An Investigation Into Facebook Friend Grouping. In *Proc. INTERACT 2011*, Springer (2011).

[3] A. Lampinen, F. Stutzman. "Privacy for a Networked World": Bridging Theory and Design. In *CHI Extended Abstracts 2011*, ACM (2011).

[4] P. G. Lange. Publicly private and privately public: Social networking on YouTube. *In Journal of Computer-Mediated Communication* (2007).

[5] T. Paul, M. Stopczynski, D. Puscher, M. Volkamer, and T. Strufe. C4PS - Helping Facebookers Manage Their Privacy Settings. In *Proc. SocInfo '12*, Springer (2012).

[6] W. Scacchi. Socio-technical design. In *The Encyclopedia of Human-Computer Interaction*, Berkshire (2004).

[7] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor. ”I regretted the minute I pressed share”: A Qualitative Study of Regrets on Facebook. In *Proc. SOUPS ’11*, ACM (2011).