

Data Security and Privacy in Social Networks. Cognitive concepts and problem awareness of young users.

Position Paper March 2011*

Andreas Poller[†]
Fraunhofer Institute of IT Security SIT
Rheinstrasse 75
64295 Darmstadt, Germany
andreas.poller@sit.fraunhofer.de

Andreas Kramm[‡]
Department of Cultural Anthropology
Goethe University, Grüneburgplatz 1
60123 Frankfurt am Main, Germany
ilyes@em.uni-frankfurt.de

Petra Ilyes[§]
Department of Cultural Anthropology
Goethe University, Grüneburgplatz 1
60123 Frankfurt am Main, Germany
ilyes@em.uni-frankfurt.de

ABSTRACT

Our research is directed at the issue of privacy risk in technosocial settings. Although breaching the private sphere of a user in a technical system like a social network site is based on a technical process, a study on the origins of privacy breaches needs to understand how underlying technical processes and user behavior relate in order to suggest viable solutions for users to both improve their privacy protection, and be able to deploy the social functions expected from these types of network.

1. PRIVACY PROTECTION IN SOCIAL NETWORK SITES

In an interdisciplinary research cooperation, Fraunhofer Institute of IT Security (SIT), Darmstadt, and the Department of Cultural Anthropology, Goethe University Frankfurt am Main, conduct a study on motives, knowledges and attitudes of young users of social network sites (SNS). The study aims at contributing to improve privacy in SNSs, and at suggesting effective and pragmatic solutions by offering data on how users meet the specific technical challenges of SNSs, and on how privacy problems in SNSs are co-produced in the interplay between user behavior and technical setting.

*The study is in progress, and is partly embedded in the curriculum at the Department of Cultural Anthropology, Goethe University, Frankfurt am Main.

[†]Dipl. Ing. Andreas Poller is a computer scientist specialized on IT security. He is currently working as a researcher at the Fraunhofer SIT.

[‡]Andreas Kramm is a postgraduate student at the Department of Cultural Anthropology at Goethe University. He is currently working as a research assistant at the Fraunhofer SIT.

[§]Dr. Petra Ilyes is senior lecturer at the Department of Cultural Anthropology at Goethe University. She has been working as an IT consultant from 1996 to 2006.

We look at both the interactions between experiences of SNS users and the technical design of network applications. We start out from the premise that testing SNS privacy mechanisms with regards to privacy risks requires an understanding of both, the technical concepts behind the software used by young people on the internet, and the situated practice of users. We consider informational autonomy to be individually performed by users. As such it must be considered both as the premise and the guideline for finding technical solutions for privacy protection in IT systems.

The study consist of a qualitative user study as well as of technical testings of user statements. Both approaches are tightly coupled. In the sense of a theory-generating process, findings are fed back into the next research round in iterative research steps. In a first step, data on user practice are collected in an explorative, empirical user study using qualitative, ethnographically informed methods. The open, explorative approach is epistemologically particularly interesting because it does not start from prescribed categories. Instead, it allows insights into user practice from the viewpoint of the actors themselves, thus potentially offering new problem definitions and indicators.

In a second step, data collected this way are analyzed in order to assess their technical security implications by mapping them onto technical user scenarios, thus allowing for a better understanding of actual technical processes during usage. In a next step, these findings serve to focus the user study, the outcomes of which, again, are fed back into the next technical testing. This methodological approach aims at delivering empirically grounded assessments as to which practical options may be suggested to avoid or minimize privacy risks in SNSs.

2. NETWORK SOCIALITY

Recent studies suggest that common concepts of the public and the private sphere need to be being questioned in view of an increasing pervasiveness of new information and communications technology in all spheres of human life, particularly regarding distributed computer networks with networked information systems like the World Wide Web, as well as new techniques of profiling and data mining. [4] The classical dichotomy of private and public is reframed. Terms like “private public” (Privatöffentlichkeit) [1] or “publicly private” [3]

critically ask how private and how public social relations are in today's technicized world. [6]

New research explores how new media practice is embedded in a wider "social and cultural ecology". [5] It is argued that the embedding of digital media products and social media applications in everyday lives of young people is happening in a specific historical era which is characterized by a long-term and systemic shift to a "network sociality": from closed social systems to open social networks. Network sociality is defined as a technological sociality: it is deeply embedded in technology. [6]

The question is then raised what, under these new conditions, actually constitutes a privacy problem, and if digital technology can generate dangers that do not exist in "analog" life.

The aim of our study is to illuminate the issue of the private sphere in "technosocial settings" [2] by conducting an empirical inquiry on situated user practice. It contributes to current discussions on why young users make their personal data public, and offers assessments on how awareness of new aspects of the public sphere in a digital world can be enhanced.

3. DIVERGING PRIVACY CONCEPTS

SNSs are particularly suited for observing privacy issues because they technically comprise all applications of the Web 2.0, and are dynamically structured. Thus, they allow for research on issues of a re-ordering of the relations between public and private.

Clearly, breaching the private sphere of a user in a technical system like an SNS is based on a technical process. However, a study on the origins of privacy breaches requires to look at how underlying technical processes and user behavior relate. The question could be raised whether users' individual privacy concepts are compatible with the technical privacy concept of a given technical system. Users may not be able to express their wish for privacy in an SNS (a) because its functionalities do not fit their individual concepts, or (b) because they do not, or only insufficiently, understand specific technical terms or the functional processes of the system at large.

Our research, therefore, aims at (1) privacy concepts and risk assessment capabilities of young user and (2) the meaning user concepts have from a technical perspective, in order to identify contradictions between technical concepts and users' privacy concepts, and, ultimately, addressing resulting privacy risks by suggesting viable solutions. We think that a promising way to achieve this is by continually feeding the findings of the empirical user study into a technical analysis of the SNS, and vice versa. This way, we are able to test at what points, and in which ways, privacy concepts of users and those of the SNS diverge.

The non-standardized inquiries supply us with information on user concepts, whereas the technical data (data on the actual configurations) supply us with information on whether users actually succeeded in technically making their concepts work. The technical data allow to build technical user mod-

els, the privacy risks of which are explored on the basis of a technical analysis of the SNSs functionalities. The derived model-based risk expectations are then compared to the actual level of protection users believe to have achieved. Our findings gained so far suggest that the methods users employ in order to protect their privacy are often not adequate to achieve the intended protection level.

Feeding back the data into the empirical user study is essential to our methodological approach. It allows us to explore in depth why user models and technical models diverge, and to understand how the divergences produce privacy risks. Both parts of the research process—the technical analysis and the user study—depend on each other. This way, we hope to be able to produce findings that (a) serve users to identify technical risks, and (2) point to possible pragmatical solutions congruent with users' conceptions and experiences. We expect our findings to point to viable solutions for users to improve their privacy protection, and, at the same time, safeguard the social functions expected from social network applications.

Privacy protection problems resulting from user behavior observed in the context of the technical design of social networks may be countered, we believe, by technical tools that users can easily implement. However, we also expect that a series of privacy issues can only be met by providers of SNS services.

4. ACKNOWLEDGMENTS

We would like to thank Léa Perraudin and Bernhard Karakoulakis for prior research work and intellectual input into the study. We also would like to thank all the students who have contributed to the study.

5. REFERENCES

- [1] S. Deterding. Metaprozesse posttraditionaler Gemeinschaftsbildung. In R. Hitzler, A. Honer, and M. Pfadenhauer, editors, *Posttraditionale Gemeinschaften. Theoretische und ethnografische Erkundungen*, pages 115–131. VS-Verlag, 2009.
- [2] M. Ito and D. Okabe. Technosocial Situations: Emergent Structurings of Mobile Email Use, November 2003.
- [3] P. G. Lange. Publicly Private and Privately Public: Social Networking on YouTube. *Journal of Computer-Mediated Communication*, 13(1):article 18, 2007.
- [4] H. F. Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1):101–139, 2004.
- [5] D. Y. Project. Living and Learning with New Media: Summary of Findings from the Digital Youth Project. The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, November 2008.
- [6] A. Wittel. Auf dem Weg zu einer Netzwerksozialität. In A. Hepp, F. Krotz, S. Moores, and C. Winter, editors, *Konnektivität, Netzwerk und Fluss. Konzepte gegenwärtiger Medien-, Kommunikations- und Kulturtheorie*, pages 163–188. VS-Verlag, 2006.