PHYS.ORG

Effective privacy protection in social networks

June 5 2013

User-friendliness versus privacy protection: SIT is investigating ways of developing user-friendly software tools for social networks. Credit: Fraunhofer

Researchers are working on new methods to help them gain a better understanding of the usage habits of participants in social networks. The results will be incorporated in the development of userfriendly tools for privacy protection.

In principle, social networks such as Facebook are a good things: users can communicate with other people around the globe, contacting their closest friends in all places and at all times to share experiences with them in real time. Yet many users have problems publishing posts and photos in a way that will protect them from the undesirable side effects to their online identities. To support users' desire for "interactional privacy" - protection of the user's private sphere in online dealings with other people - suggested improvements have already been made for networks such as Facebook. In a practical setting, however, these improved means are either too rigid to do justice to users' multifaceted habits, or they are very complicated to manage because they try to solve a host of different problems all at the same time.

"If we want to develop truly user-friendly tools, we have to understand users better," according to Andreas Poller of the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt. Together with researchers at Goethe University in Frankfurt am Main, for five years, now, he has been working on a project, "Software Design for Interactional Privacy within Online Social Networks," that will create new methods of collecting and evaluating data on usage habits in online social networks (dipo.sit.fraunhofer.de/). In contrast to previous studies, researchers not only want to identify the weak spots in privacy management but also want their work to support the design of more effective privacy tools.

Ingenious study design

Initially, researchers focused their attention exclusively on qualitative interviews. Since then, they have begun combining their surveys with analytical software developed at SIT to document Facebook activities by study participants (code.google.com/p/rose-browser-extension/). "To make sure that this tool does not influence user behavior – as would be the case, for instance, if a study participant felt he or she was being monitored by the software – we have intentionally designed it to give study subjects full control over their data," Poller explains. The software runs on the user's computer, and not on an external server. Content is not recorded - only the technical functions used. A special commentary function provided by the software inserts itself into the Facebook user interface to give users an opportunity to comment directly, "on site," on their usage behavior and experiences. Data are not automatically transmitted; instead study participants must forward them to the researchers. In a form of protocol, they can first review the documentation and modify it wherever they wish.

"Thanks to the close dovetailing of the two research methods, we can interpret technical facts from the user's perspective," Poller points out. While qualitative interviews often reveal interesting aspects and statements of the problem, they cannot be implemented on a one-to-one basis in specific software design. "You also have to know what problems are specifically a result of the technology involved," Poller says. Designs developed purely on the basis of technological expertise, on the other hand, lack any reference to users' habits. A knowledge deficit about the ways in which people and technology interact can also lead to false conclusions – as in the case of the "privacy paradox" in which users indicate that they attach great importance to their privacy but have selected very open settings for their Facebook account. "At first glance, this looks like a contradiction. In fact, though, it may well be that the user has only provided spare information in his or her profile and doesn't post anything and thus needs no restrictive protective settings at all," Poller explains.

With their work, the researchers want to help improve the design process of software for social networks. The results of the study are regularly presented to the community of researchers, and the analytical tool is available as open source software. In March of last year, the project team was presented with the coveted Google Faculty Research Award for their efforts on behalf of improved privacy protection.

Provided by Fraunhofer-Gesellschaft

Citation: Effective privacy protection in social networks (2013, June 5) retrieved 26 April 2024 from https://phys.org/news/2013-06-effective-privacy-social-networks.html