Privacy in Social Media

In brief

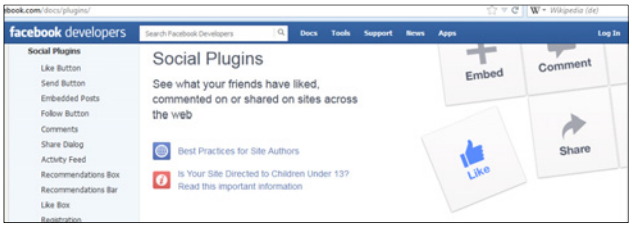
- Nowadays, social network sites (SNS) such as Facebook or Twitter are ubiquitous. They increasingly develop into platforms combining many services.
- SNS endanger privacy to a large extent as the relationships, contents and interactions displayed there can be matched to individuals.
- The right of informational self-determination – that is the right to decide oneself about the disclosure and usage of one's personal data – can hardly be exercised in a world characterised by SNS. In addition, this is aggravated by providers' terms of use and business models, which favour large-scale linking-up.
- Not least the recently discovered surveillance scandals underline the pressing need to design SNS in a privacy-enhancing manner. Privacy-by-design is essential when it comes to re-establishing the trust of the users.

What is it about?

Social network sites (SNS) have become a ubiquitous and decisively popular phenomenon of the Internet since the foundation of Facebook in 2004. They enable in a relatively easy way to establish and cultivate social relationships. Use ranges from purely personal (e.g. exchange about hobbies) to professional uses (e.g. job-seeking, marketing), individual contacts as well as group activities. SNS offer a broad range of communication tools and support the networking of the users via sophisticated algorithms in the background, e.g. via automated proposals of contributions on the basis of interests shown hitherto.

Use of social media always leads to the exchange of personal data and information such as photographs or personal preferences. This does not only take place amongst the users but also with the SNS provider. These data are used by the provider not only with a view to optimise the services, but also to generate money (e.g. via targeted advertisement). The users consider this disclosure of personal information only partly as wanted and helpful. In essence, we can speak of a forced and deep intrusion into privacy via comprehensive storage, processing and interlinking of data.

The desire to be able to control in a self-determined way, i.e. who is allowed to do what and when with what personal data, is therefore in opposition to the business models of the SNS providers. Users have practically no influence on the terms of use. The example of Facebook shows that the automatic (default) settings render publicly visible practically everything that has not explicitly been labelled as private; some data cannot even be labelled as private.



Social plugins in Facebook

Further challenges for the protection of privacy stem from increased interlinking of SNS with other online services. Numerous 'apps' enable third party providers to offer, for instance, games and goods. In addition, 'social plugins' form an interactive bridge between SNS and other Internet platforms. Facebook's 'Like' button, for instance, is often integrated in many websites and allows users to share external web content on SNS.

Basic data

Project title:	Social Network Sites: Potentials, Impacts and Major Privacy Challenges
Project team:	Strauß, S., Nentwich, M., in the framework of the European TA Group (ETAG)
Duration:	04/2012 – 12/2013
Funded by:	European Parliament/STOA

Analysis

Several studies revealed that most users of SNS share a large quantity of personal data. Nonetheless, for the majority of users protection of their privacy is important. While awareness-raising measures such as educational articles are certainly important, they do not suffice given the very limited options to exercise one's right of informational self-determination: data protection settings on SNS are not only endangering privacy, they are also non-transparent, very complex to manage and, generally speaking, do not allow for comprehensive protection. Alternative platforms, such the privacy-friendly SNS Diaspora, lack attraction so far.

Diaspora – a privacy-friendly network

Protection of direct personal data is particularly hampered because of apps and social plugins: implicit data collected via these services, i.e. data not actively entered but produced automatically simply by using the SNS, can be condensed to a meaningful profile of the users. In this context, the rapid development of biometrics (e.g. face recognition) and continued increase of mobile use of SNS (including localisation via GPS) play an important role.

On the one hand, protecting privacy on an individual level is supported by a variety of tools (that block certain types of data access). On the other hand, whether and how these tools are applied, largely depends on the different skills of the individual users. Consequently, a special type of digital divide, a 'privacy divide' is developing. One solution is the '"privacy-by-design'" approach: from a technical as well as organisational point of view social media may be designed in a way so that the protection of the user's privacy is built in from the start and does not exclusively depend on their behaviour.

What to do?

Social network sites endanger privacy to a large extent as the relationships, contents and interactions displayed on them can be matched to individuals. In order to cope with this problem, which is increasing because of recent developments, awareness raising is not sufficient. Instead, the following measures are required:

- Privacy protection as default setting: a privacy-friendly design ('privacy-by-design') could replace the standard of free access to all data. The encryption of content and the establishment of respective standards would be essential.
- Limiting the life-span of data and an option to permanently delete the data would consolidate informational self-determination.
- If personal data were not centrally stored as a matter of principle, information that identifies persons could then not be linked up as easily outside of its original context.
- The data protection authorities should be supported in their control function and given more resources in order to supervise the implementation of privacy standards.

In any case, critical public discourse on privacy, freedom of information, and transparency could strengthen trust in SNS and other web-based communication infrastructures.

Further reading

Strauß, S., Nentwich, M. (2013) Social Network Sites – Privacy and the blurring boundary between public and private spaces. Science and Public Policy, Bd. 40 (6), S. 1-9

Contact

PD Dr Michael Nentwich

Email: tamail@oeaw.ac.at

Phone: +43(1)51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Strohgasse 45/5, A-1030 Vienna; http://www.oeaw.ac.at/ita/en. | Frequency: The ITA Dossiers are published irregularly and publish the research results of the ITA. The ITA Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal 'epub.oeaw': http://epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: http://creativecommons.org/licenses/by/4.0 | ITA Dossier no. 5en, December 2013 | http://epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier005en.pdf | Co-author: Strauß, S.