

NewsLetter No.75 December 2007

Web 2.0: Social Networking Sites and Data Protection



By Martina Arioli, Attorney-at-Law, LL.M.
+41 44 498 95 46; marioli@wwp.ch

Social Networking Sites (SNS) allow people to communicate with their colleagues and friends, to exchange information and to find out who is acquainted with whom. SNS have become extremely popular and are considered to have significant business value because people voluntarily disclose detailed maps of their social relationships and personal interests. Thus, SNS have attracted attention for customized advertising.

MySpace is considered the largest Social Networking Site with currently over 110 million members and 230,000 more joining every day. In November 2007, the active membership of US-based Facebook was said to number more than 54 million people worldwide with 15 billion page views per month. The German business networking site, Xing, currently numbers 4 million registered users. In the hype surrounding SNS however, data protection, security and liability issues have sometimes been neglected. SNS convey a sense of intimacy among digital 'friends' which often leads to disclosures which are not appropriate in a public forum. This NewsLetter highlights some data protection/privacy issues that are important for users as well as SNS providers.

Join the network!

People join SNS to find existing friends or colleagues and to make new friends with people with similar interests and backgrounds and thus widen their network. To join an SNS, the user posts personal data in his or her profile, often including his or her name, pictures, current job and former employers, contact information, education, personal interests and other activities. On the SNS platform, people link together and interact based around their profiles. Users open their own personal address books to all other users of an SNS and disclose their own private network.

Access to Personal Data of the Users

The SNS providers strive to have the users provide as much data as possible to make the SNS attractive for new users. Considerable data protection issues arise since most members on SNS are not aware of the possible size of the audience that accesses the personal information they have voluntarily disclosed on an SNS. Information revealed on an SNS can be used for different purposes and in different contexts than those the user may have initially envisioned. Especially

outside the context of the particular SNS, such personal information can become embarrassing or even damaging. Pictures posted by the users may be used for face recognition. Users often are not aware of the fact that they convey secondary personal data every time they visit the SNS because SNS providers log data, such as frequency of access to the SNS, visits to other user profiles or messages sent to other users. Furthermore, non-personally identifiable information such as the user's IP address, browser type, duration of log-on etc. is registered by the SNS providers.

Customized Advertising

Advertising can be personalized to each individual user because the user has voluntarily disclosed to the community his or her profile.

Tagging

Many SNS allow users to tag images with metadata, e.g. links to SNS profiles of other users, without obtaining the consent of the tagged user. Such tagging may lead to more unwanted linkage to personal data.

Storage and Search Engines

Profiles on an SNS can – technically – be accessed, downloaded, and stored indefinitely. This may lead to the creation of a digital personal dossier. Even if the user deletes his or her profile on an SNS, caches and data traces linked to his or her profile always remain online. Furthermore, SNS profiles or parts thereof may appear in results of search engines. There are specialised person search engines that compile online data and search SNS platforms for individuals.

Data protection principles under Swiss Law

The Swiss Data Protection Act in particular requires that the data subjects on whom data is collected and processed need to be explicitly informed about:

1. The purpose for which the personal data is used (principle of transparency);
2. Any third party recipients of the personal data;
3. The means of access, rectification and deletion of their personal data (principle of control over personal data by the data subject).

Such information must be visible and easily understood, either by means of a privacy statement or in real time information on the SNS.

Obligation of SNS Providers in relation to Data Protection

Data protection should be treated as a priority by the SNS and they should create a high degree of transparency on how the data of the users is collected, maintained and disclosed to third parties. The following guidelines should be followed:

1. Data protection issues should not be hidden in general terms of use, but rather included on the SNS in real time as the users visit the SNS and undertake steps that could have an impact on the protection of their data.
2. Because the tagging of images without the consent of the tagged data subject may be problematic, SNS providers should enhance the data subject's control over the tagging of his or her images. The user should be able to decide whether his or her images may be tagged and should be able to remove tags.
3. It is crucial that the user is able to decide to whom, and to what extent, his or her profile is made accessible. These limits of the user's consent need to be ensured in particular when the user decides that only registered users shall be permitted to access his or her profile. Adequate technical measures should be implemented against unauthorised access to the SNS in order to prevent unauthorised perusal, copying, amendment or deletion of personal data. However, SNS providers cannot be obliged to verify the identity of the users during the registration process or even to track and trace their possible purposes when visiting profiles of other users or contacting them.
4. SNS providers should give the users the choice to explicitly opt-in for marketing activities. At a minimum, SNS providers should provide means for an opting-out of customized advertising campaigns on the SNS at any time. Furthermore, SNS providers should refrain from disclosing complete user group profile information to advertising agencies unless the users have voluntarily and explicitly consented to such disclosure.
5. SNS providers should inform the users explicitly about the possibility that their profiles may be

stored or made accessible by third parties in and outside of the country in which they are located, such as search engines or web archives. Users should be given the choice to opt-out, in particular by restricting the access to their profiles to registered users. As an alternative, SNS providers should at least anonymise the data.

6. SNS providers should permanently delete all data linked to a user if such user wishes to exit the platform. Not only the deletion of the profile information should be ensured, but as far as possible, the user also should be permitted to edit or delete secondary information, such as comments posted on forums and guest books of other users.
7. SNS providers should implement tools to facilitate the reporting of abuse and lapses in data protection.

Summary

Web 2.0 platforms such as SNS challenge conventional principles of data protection. Users should carefully reflect on what personal data they wish to share to a possibly large and anonymous audience for an unlimited period of time. SNS providers, on the other hand, should carefully assess what to do with the personal data and ensure compliance with data protection laws in the countries where their members are located.

The ww&p NewsLetter provides comments on new developments and significant issues of Swiss law. These comments are not intended to provide legal advice. Before taking action or relying on the comments and the information given, addressees of this NewsLetter should seek specific advice on the matters which concern them.

© Walder Wyss & Partners, Zurich, 2007



Walder Wyss & Partners
Attorneys at Law

Seefeldstrasse 123
P.O. Box 1236
CH-8034 Zurich
Phone +41 44 498 98 98
Fax +41 44 498 98 99
reception@wwp.ch
www.wwp.ch