30th International Conference of Data Protection and Privacy Commissioners
Strasbourg, 17 October 2008

Resolution on Privacy Protection in Social Network Services

Resolution

Social network services[1] have become very popular in recent years. Among other things, these services offer means for their subscribers to interact based on self-generated personal profiles, which support an unprecedented level of disclosure of personal information about the individuals concerned (and others). While social network services offer a new range of opportunities for communication and real-time exchange of all kinds of information, the use of these services can also place the privacy of its users – and others – at risk: Personal data about individuals become publicly (and globally) available in an unprecedented way and quantity, including huge quantities of digital pictures and videos.
Individuals face the possible loss of control over how data will be used by others once they are published on the network: While the "community" basis of social networks suggests that publishing one's own personal data would just resemble sharing information with friends as it used to be face-to-face, profile information may in fact be available to an entire subscriber community (numbering in the millions).

Very little protection exists at present against copying any kind of personal data from profiles – by other network members, or by unauthorised third parties from outside the network – and using them for building personal profiles, or re-publishing the data elsewhere. It can be very hard – and sometimes even impossible – to have information thoroughly removed from the Internet once it is published: Even after deletion from the original site (e.g. the social network), copies may rest with third parties or with the social network service providers. Personal data from profiles may also "leak" outside the network when they are indexed by search engines. In addition, some social network service providers make user data available to third parties via application programming interfaces, which are then under control of these third parties.

One example of secondary uses that has gained wide public attention is the practice of company personnel managers crawling user profiles of job applicants or employees: According to press reports, one third of human resources managers already admit to use data from social network services in their work, e.g. to verify and/or complete details of job applicants.

Profile information and traffic data are also used by providers of social network services for delivering targeted marketing messages to their users.

It is very likely that other unexpected uses for the information in user profiles will emerge in the future.

Other specific privacy and security risks already identified include increased risks of identity fraud fostered by the wide availability of personal data in user profiles, and by possible hijacking of profiles by unauthorised third parties. The 30th International Conference of Data

[1] "A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others […]. Most services are primarily web based and provide a collection of various ways for users to interact […]". Quoted from Wikipedia: http://en.wikipedia.org/wiki/Social_network_service .

Protection and Privacy Commissioners recalls that these risks have already been analyzed in the "Report and Guidance on Privacy in Social Network Services" ("Rome Memorandum")[2] of the 43rd meeting of the International Working Group on Data Protection in Telecommunications (3-4 March 2008), and in the ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks"[3] (October 2007).

The Data Protection and Privacy Commissioners convened at the International Conference are convinced that it is necessary, in the first place, to carry out an in-depth information campaign involving all public and private stakeholders – from governmental authorities to educational institutions, such as schools, from providers of social network services to consumer and user associations, and including the Data Protection and Privacy Commissioners themselves – in order to prevent the multifarious risks associated with the use of social network services.

Recommendations
Given the special nature of the services, and short and long term privacy risks to individuals, the Conference offers the following recommendations to users and providers of social network services:

Users of Social Network Services
Organisations having an interest in the wellbeing of users of social networks – including service providers, governments and Data Protection Authorities – should help educate users to protect their personal data and communicate the following messages.

1. Publication of information
Users of social network services should consider carefully which personal data – if any – they publish in a social network profile. They should keep in mind that they may be confronted with any information or pictures at a later stage, e.g. in a job application situation. In particular, minors should avoid revealing their home address or telephone number.

Individuals should consider the usefulness of using a pseudonym instead of their real name in a profile. However, they should keep in mind that the use of pseudonyms offers limited protection, as third parties may be able to lift such a pseudonym.

2. Privacy of other individuals
Users should also respect the privacy of others. They should be especially careful with publishing personal information about somebody else (including pictures or even tagged pictures) without that other person's consent.

Providers of Social Network Services
Providers of social network services have a special responsibility to consider and act in the interests of individuals using social networks. In addition to meeting the requirements of data protection law they should also implement the following recommendations.

1. Privacy regulations and standards
Providers operating in different countries or even globally should respect the privacy standards of the countries where they operate their services. To that end, providers should consult with data protection authorities as necessary.

2. User information
Providers of social network services should inform their users about the processing of their personal data in a transparent and open manner. Candid and intelligible information should

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491
[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

also be given about possible consequences of publishing personal data in a profile and about remaining security risks, as well as about possible legal access by third parties (including e.g. law enforcement). Such information should also comprise guidance on how users should handle personal information about others contained in their profiles.

3. User control
Providers should further improve user control over the use of their profile data by community members. They should allow for restriction of visibility of entire profiles, and of data contained in profiles, and in community search functions.

Providers should also allow for user control over secondary use of profile and traffic data*;* e.g. for targeted marketing purposes. As a minimum, opt-out for general profile data, and opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data should be offered.

4. Privacy-friendly default settings
Furthermore, providers should offer privacy-friendly default settings for user profile information. Default settings play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes. Such settings must be specifically restrictive when a social network service is directed at minors.

5. Security
Providers should continue to improve and maintain security of their information systems and protect users against fraudulent access to their profile, using recognised best practices in planning, developing, and running their applications, including independent auditing and certification.

6. Access rights
Providers should grant individuals (regardless of whether they are members of the social network service or not), the right to access and, if necessary, correct all their personal data held by the Provider.

7. Deletion of user profiles
Providers should allow users to easily terminate their membership, delete their profile and any content or information that they have published on the social network.

8. Pseudonymous use of the service
Providers should enable the creation and use of pseudonymous profiles as an option, and encourage the use of that option.

9. Third party access
Providers should take effective measures to prevent spidering and /or bulk downloads (or bulk harvesting) of profile data by third parties

10. Indexibility of user profiles
Providers should ensure that user data can only be crawled by external search engines if a user has given explicit, prior and informed consent. Non-indexibility of profiles by search engines should be a default setting.