Position paper for the W3C Workshop on the Future of Social Networking

Barcelona, January 15-16, 2009

Privacy and Social Network Sites: Follow the Money!

Martin Pekárek, MSc.
Ronald Leenes, PhD
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University
The Netherlands

Introduction

Over the past years, social software applications have undergone tremendous growth. One of the protagonists of the Web 2.0 revolution are Social Network Sites (SNSs), that are estimated to have more than 272 million users worldwide (Universal McCann 2008). SNSs offer a variety of possibilities to make new friends and business contacts, to share knowledge and to get online support. In the process, users leave more and more information traces online, which may cause privacy issues. This insight is not new, and much research is carried out investigating this topic (e.g. (Grimmelmann 2009), (Gross, Acquisti et al. 2005);(Hogben 2007); (Wong 2008)).

In combating the loss of privacy on SNSs, privacy protectors usually lament the carelessness with which users publish personal information. Their first suggested remedial action is often to raise user awareness of potential privacy issues. Subsequently, they propose a number of security measures, ranging from automated partial identities to advanced anonymous credentials. All these solutions have in common that they underestimate the innate social aspect of SNSs and how these platforms perfectly meet the social needs of their users. People use SNSs because they want to interact socially, and anything that stands in the way of that use will be either neglected or circumvented (Grimmelmann 2008).

Effective privacy protection on SNSs is better served if we take a more fundamental approach, in which we primarily focus on understanding social dynamics. First, we have to reassess an important goal of privacy protection: the prevention from harm. After we have established the particular types of harm that can be caused by the use of SNSs, it has to be investigated who is potentially harming SNS users. A targeted protection effort can only be conceived if the possible privacy infringers are clearly identified.

Prevention from harm

Why do we want to protect the privacy of SNS users in the first place? Van der Hoven (Hoven and Weckert 2008) distinguishes four types of harm that can be incurred when privacy protection is compromised. We will concisely describe these, including an example within an SNS setting.

1. Information-based harm: others could abuse the mobile phone number you have listed in your profile to harass you.

2. Information inequality: information about purchases and preferences can be used for purposes of marketing and/or price discrimination without the SNS user being aware of or able to influence this process.

3. Informational injustice: when information presented in one context (e.g. a risqué photographic report of a party) is used in another, unintended context (e.g. an appraisal of a job application), informational injustice is said to have occurred

4. Restriction of moral autonomy: with the omnipresence and pervasiveness of SNS information, people are effectively restricted from presenting different "faces" in different contexts, thus limiting their options of self-representation.

These harms may occur in different stages of the information interchange with the SNS, either at the stage of information collection, information processing or information dissemination, as described by (Solove 2006). An interesting combination of these two approaches into a privacy risk assessment tool applied in the SNS realm can be found in (Riphagen 2008).

Attacker model

After having assessed the types of harm that become possible through the use of SNSs, it is interesting to see who would be able to inflict this harm. It is appropriate to look at all the parties who have access to and can (mis)use the different types of information that are collected and stored by SNSs. Three types of attackers can be discerned:

- Other users: these are people who also have an account on the SNS, and have access to the profile information of an SNS user. Depending on the existence and the nature of a connection between SNS members, another user can harvest more or less personal information from the profile page of an SNS user. In principle, other users only have access to private information when the user explicitly allows it. Privacy settings on SNSs become increasingly sophisticated, giving SNS users more and more levers to fine-tune the access of other users to personal information.

- Third parties: people and organisations who have no user account and therefore have no or only minimal access to the system. They can legitimately only access publicly available data. Third parties often take the form of automated solutions, such as mashups, that combine information from a wide range of sources (SNSs, Google searches, photo sites, etc.) and present the end result in one (web) location.

- Platform providers: the owners and operators of the SNS itself. Because the predominant technical implementation of SNS is a client-server architecture, in which the platform provider manages the server, the provider has full access to all information stored by users and generated by their use. On top of that, they can also store the information for an indefinite period, thus enabling them to determine longitudinal changes in SNS use on individual user level.

Motivations

We have thus seen four types of harm that can be inflicted when privacy protection is not upheld, and three types of attackers who could cause such harm. But before such harm would occur, there needs to be a motivation to do so. This section discusses the two most important motivations.

The first motivation is social. Members of SNSs are building social capital through the accumulation of connections. The value of the social network increases when the platform is used more intensively: not only the number of connections is a determinant, but also the use of the services the platform offers (e.g. blog, wall, pictures). The richer the profile, the more interesting one becomes as a contact.

The network effect encourages SNS providers to offer more tools for members to increase the amount of information on the SNS. This process is cyclically reinforced: the more information people leave on the SNS, the richer the profiles become, the more attractive they are for both commercial use and social use by other (potential) SNS members. Finally, there is a lock-in effect: users are more likely to limit their SNS use to the SNS in which they already have invested much time and effort.

The second motivation is monetary. When looking at the potential attackers, it is mainly the application providers and third parties that have this motivation. Examples to monetise are targeted advertising, but also information trade to specialised companies (personal credit rating agencies, marketing companies). More examples will undoubtedly come to light during the Barcelona workshop. The exact sums of money that are concerned with these types of information transactions are hard to substantiate, since they take place behind the storefront of privately owned companies that are generally unwilling to disclose financial details. However, money must be a powerful motivator, especially if we regard the sums paid for stakes in SNSs. Just recall News Corporation's $580 million cash takeover of MySpace[1], or Microsoft's $240 million payment for a 1.6 percent stake in Facebook, theoretically valuing the SNS provider at a staggering $15 billion[2].

What we see is that the social incentive to publicize personal information is overwhelmingly strong. Although users are aware of the potential privacy risks, they still use the SNS services, apparently preferring the short-term tangible social benefits over the long-term effect of limiting potential privacy infringements. Even when SNS users are privacy aware, they do not tend to use available privacy tools(Oomen and Leenes 2008). It appears that, in practice, individuals disclose more information than they intend to(Norberg, Horne et al. 2007). Stronger still, research suggests that any tool or technique limiting the social aspects of SNSs is doomed to fail: users are simply not interested in them(Grimmelmann 2009).

After having established that users overwhelmingly choose to divulge huge amounts of personal information, no matter how aware they are of potential privacy risks, we

[1] <http://www.newscorp.com/news/news_251.html>, last accessed November 18, 2008

[2] <http://www.nytimes.com/2007/10/25/technology/25facebook.html>, last accessed November 18, 2008

conclude that it doesn't make any sense to make it harder for users to publish personal information. Although raising the awareness of users of the potential impact of divulging information (e.g. pertaining to the distribution and persistence of information on the Internet) may occasionally convince SNS users to limit the amount of information to publish, by and large this is unlikely to structurally adjust information divulging practices.

Cutting out the middleman?

SNSs in their current form will continue to exist, gradually adapting themselves to changing consumer needs and emerging commercial opportunities. Users will continue to disclose personal information in order to meet their social needs, information that may be used for unintended purposes. If we cannot prevent users from this type of behaviour, it may prove to be fruitful to look at other attackers: the platforms and third parties themselves. When we aim to prevent harm, restraining the monetary incentive to harvest information use may be more effective. A transfer of SNS use to non-commercial platforms, specifically limiting the unintended use of personal information, is an alley that could be explored. The fact of the matter is, that the current terms of service of large SNS providers grant virtually unlimited rights to platform providers to use personal information released by SNS users.[3]

There are already examples of these types of non-commercial networks. Open source SNS platforms are available, such as Elgg[4]. Preferably, such a platform would function on a peer-to peer basis that would limit the power of an omnipotent platform provider. At the current stage, however, these solutions are no match for the slick commercial SNSs ruling the marketplace.

Of course, the main obstacle for the widespread adoption of such platforms is the entrenched position of the current SNS platforms: SNS users have devoted considerable time and energy to build their current profile on one their favourite SNSs, and it will take them once again much effort to build a comparable profile on the new network. More important is, however, that transferring an individual profile is not enough: the value a user derives from an SNS is chiefly based on the user's network. The profile is just a means to an end, since one does not have access to a network without a profile. Whether the incentive of improved privacy protection of a new SNS network will be sufficient to seduce users to a new social network environment remains to be seen. Research into non-commercial social networks, and their applicability in the current SNS landscape is a prerequisite for any potential further steps. Only after establishing one or more of these SNSs, the take-up of their services can be tested in practice. This is one of the research strands of PrimeLife, the EU 7th Framework program bringing sustainable privacy and identity management to future networks and services.

Grimmelmann, J. (2008). "Accidental Privacy Spills." Journal of Internet Law(July 2008).

[3] See for instance <http://www.facebook.com/terms.php?ref=pf>, last accessed November 20, 2008

[4] < http://elgg.org/index.php>, last accessed November 18, 2008

Grimmelmann, J. T. (2009). "Facebook and the Social Dynamics of Privacy." Iowa Law Review **95**(4).

Gross, R., A. Acquisti, et al. (2005). Information revelation and privacy in online social networks. ACM Workshop on Privacy in the Electronic Society, New York, NY, ACM.

Hogben, G. (2007). Security Issues and Recommendations for Online Social Networks, ENISA, European Network and Information Security Agency.

Hoven, J. v. d. and J. Weckert (2008). Information technology and moral philosophy /; edited by Jeroen van den Hoven, John Weckert. New York [etc.] :, Cambridge University Press.

Norberg, P. A., D. R. Horne, et al. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." The Journal of Consumer Affairs **41**(1): 100-126.

Oomen, I. and R. Leenes (2008). Privacy risk perceptions and privacy protection strategies. IDMAN'07 – IFIP WG 11.6 working conference on Policies & Research in Identity Management. S. Fischer-Hübner, Springer, Dordrecht**:** 121-138.

Riphagen, D. (2008). The Online Panopticon. Faculty of Technology, Policy and Management. Delft, Delft University of Technology.

Solove, D. J. (2006). "A Taxonomy of Privacy." University of Pennsylvania Law Review **154**(3): 477.

Universal McCann (2008). Power to the people - Social Media Tracker Wave 3.

Wong, R. (2008). "Social Networking: Anybody is a Data Controller!" Nottingham Law School.