IDIS (2009) 2:81–93
DOI 10.1007/s12394-009-0016-4

A comparison of privacy issues in collaborative workspaces and social networks

Martin Pekárek · Stefanie Pötzsch

Received: 21 November 2008 / Accepted: 8 June 2009 / Published online: 28 July 2009

Abstract With the advent of Web 2.0, numerous social software applications allow people to publish and share information on the Internet. Two of these types of applications – collaborative workspaces and social network sites – have a number of features in common, which are explored to provide a basis for comparative analysis. This basis is extended with a suitable definition of privacy, a sociological perspective and an applicable adversary model in order to facilitate an investigation of similarities and differences with regard to privacy threats. Practical examples are derived from the use of Wikipedia and Facebook. Analysis suggests that a combination of technical, legal, and normative solutions should be considered to counter privacy issues. A number of potential solutions that may mitigate these issues are proposed.

Keywords Collaborative workspaces · Comparison · Facebook · Privacy · Privacy issues · Social network sites · Social software · Wikipedia

Introduction

With the advent of the so-called Web 2.0 social software applications gain more and more users. People actively participate in discussions and the creation of content on the Internet. They create profiles with personal data and manage their relationships on the Web. This offers a variety of possibilities to make new friends and business connections, to share knowledge and to get support from an online community. In

M. Pekárek (✉)
TILT - Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg, Postbus 90153, 5000 LE, Tilburg, The Netherlands
e-mail: m.e.pekarek@uvt.nl

S. Pötzsch
Faculty of Computer Science, Technische Universität Dresden, 01062 Dresden, Germany
e-mail: stefanie.poetzsch@tu-dresden.de

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 et al. 2005, Hogben 2007, Wong 2008).

As part of the European Community's Seventh Framework Programme (FP7/2007–2013), one of the topics of the PrimeLife project is the investigation of privacy issues of collaborative workspaces and social network sites (PrimeLife 2008). Both types of platform have a number of elements in common. People participating in these platforms provide and adapt content, and divulge personally identifiable information in the process, thus leading to (potential) privacy issues. This paper investigates whether and to what extent social networks and collaborative workspaces can be treated equally when trying to solve privacy threats, and suggests a number of potential solutions that may mitigate these issues. The scope of the analysis is relatively general, as it is not the objective to solve one particular privacy problem with one specific solution. Rather, the goal is to outline possible types of solutions that may be considered based on the particular features of collective workspaces and social network sites.

The structure of the paper is as follows. After a brief introduction of social software, we focus on the similarities and differences between collaborative workspaces and social network sites. This description of general features is supplemented with a suitable definition of privacy, a sociological perspective and an applicable adversary model in order to have a theoretical basis for the comparison of both types of social software. The mainstay of the paper is formed by an analysis of the privacy issues arising in collective workspaces and social network sites, and it concludes with a number of suggested improvements.

Social software

The term social software characterises infrastructures, platforms and applications that enable users to communicate, collaborate and coordinate themselves via networks, to establish and maintain relationships and thus in some way map social aspects of real life to an online environment. Schmidt defines social software as web-based applications that support management of information, relationships and representation of one's self to (a part of) the public in hypertextual and social networks (Schmidt 2006). Therefore three primary functions of social software can be identified (Richter and Koch 2007) and are indicated in Fig. 1:

- Information Management: finding, evaluating and administration of information
- Self Management: present aspects of yourself on the Internet
- Relationship Management: represent and maintain contacts to others via Internet

Considering these functional differences, we distinguish between different types of social software applications. On the one hand we consider collaborative workspaces, which encompass applications that are primarily focused on documents that are created in a collaborative manner (Panoke-Babatz and Syri 1997), and that aim to support *information management* (cf. top corner of the triangle in Fig. 1). Technical systems that can be used for establishing collaborative workspaces are

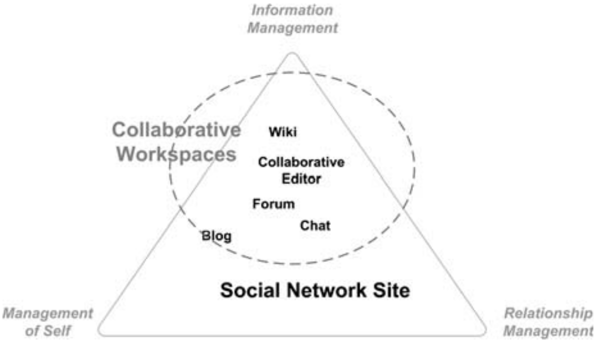

Fig. 1 Functional triangle of social software according to (Richter, Koch 2007)

wikis, collaborative real-time editors, forums, chats, weblogs, or further groupware systems. A well-known example of collaborative workspaces realised by a wiki system is Wikipedia (Wikipedia 2008a). On the other hand we find social network sites (e.g. Facebook (Facebook 2008a), LinkedIn (LinkedIn 2009), Hyves (Hyves 2009), MySpace (MySpace 2009)), which stress the self-portayal of social network site members, and the management of the relations between them (boyd and Ellison 2007). Social network applications are therefore positioned in the middle between the lefthand and the righthand corner towards the bottom of the triangle (cf. Fig. 1).

Differences and similarities between collaborative workspaces and social network sites

Social network sites and collaborative workspaces both aim at supporting users in online collaborations; however they follow two different approaches.

The essential feature of a social network site is the provision of user profiles and connections between them (c.f. *relationship management* in Fig. 1). It is focused on the individual, and users can create additional content—usually related to their profiles (private messages, listed groups, wall)—to present themselves within a group of connections. Collaborative workspaces work the other way around. The key functionality in this case is the collaborative editing and creating of contents (c.f. *information management* in Fig. 1). The co-authors in a collaborative workspace form a social network, but this social network is not the essence of the collaborative workspace: the focal point is the jointly created content, whereas the value of a social network site lies in the network itself.

Table 1 provides an overview about features that both types of applications have in common and points out differences and similarities in realisation.

The first two features—*Content Creation and Management* and *User Administration*—are inversely important for the particular applications. Theoretically, collaborative workspaces can be realised only with features for creating and managing content and without any user administration. For example, a wiki system can allow everybody to read and modify all articles without any restriction. Vice versa an application that allows people to create profiles and indicate connections fulfils all mandatory requirements of a social network site without providing additional features for communication and producing content in addition. *Access*

Table 1 Comparison of features for collaborative workspaces and social network sites

	Collaborative workspaces "Content is important."	**Social network sites** "The network, supported by user information and relationships, is important."
Content Creation and Management	Collaborative creation and editing of content is the key feature.	Subordinate feature.
User Administration	Subordinate feature.	Management of user profiles and their connections is the key feature.
Access Control	If restricted, AC to documents is identity-based, depending on the goal of the document and the knowledge of the user.	If restricted, AC to profiles is relationship-based, depending on the connection between the user and the profile owner.
History Service	User gets newest version per default, all former versions of content may also be available.	User gets only current version of others profiles and connections. Providers may have former versions stored in databases.
Event Service	Users can be informed, in case of changes on certain contents or when new content is available.	Users can be informed, in case of changes on certain contents or when new content is available.

Control, *History Services* and *Event Services* are realised slightly differently in current applications from both types. In any case, these features are subordinate functionalities.

Collaborative workspaces and social network sites are both automated tools to support interactions between participants. The underlying goals of these interactions may vary considerably. Members who have an account on a social software application aim to maintain social connections or to share information with others. In order to become part of such a community, it is necessary to disclose at least some personal data that shows who you are, what skills you have and what you are interested in. This disclosure is facilitated directly by profile pages that contain basic information, such as name and age, but also other identity related data, like hobbies and interests, images, and personal opinions as expressed in blogs. Further, personal data is indirectly disclosed when content is provided by the user. This encompasses semantically included information, e.g. someone who writes his real name or place of residence in a forum, as well as writing style, habits of technology usage and other information. The digital availability of this data leads to potential privacy risks, since copying of data and tracing of users is simple and data, once disclosed, is out of control of the data supplier.

Investigating informational privacy in social software

When discussing the privacy aspects of collaborative workspaces and social network sites, an appropriate definition of privacy is indispensable. We limit ourselves to informational privacy, which can be defined as the freedom from unreasonable constraints on the construction of one's own identity (Agre and Rotenberg 1997). The availability of personal information in the hands of unintended others may cause such constraints, which calls for equipping the user with control over his personal data in order to minimise misuse of information. The ability of the user to actively influence the access to and the use of his personal information is key.

This can be interpreted with a strictly technical focus, which would imply that all privacy issues would be solved when the necessary technical requirements have been met and implemented. The observed disparity between expressed data protection attitudes and actual behaviour (e.g. Norberg et al. 2007, Oomen and Leenes 2007) already limits the potential of technical solutions to absolve all privacy issues. In practice, there are other matters that have to be considered if privacy is to be respected. The first of these are applicable legal rules, such as the Terms of Use of a particular platform, or relevant data protection legislation. Another essential type of rules are social norms that apply to social software implementations. The sociological perspective is discussed below.

Sociological perspective

When interacting with other people or organisations, every individual plays a role that is appropriate in a particular situation. The behaviour of someone who is surrounded by close family members may differ substantially from the one displayed at work when interacting with colleagues or management. According to Goffman it depends on the context what part of one's identity someone is prepared to show to the environment, where it is essential to keep these contexts separate: the term 'audience segregation' is coined for this phenomenon. Audience segregation can be defined as the ability of the user to have different partial identities to play different roles and portray the self to others in a way he chooses (Goffman 1959). Thanks to the careful segregation of the different audiences, the partial identities can be allowed to co-exist. Rachels states that this audience segregation "is an essential characteristic of modern (western) societies and allows for different kinds of social relationships to be established and maintained" (Rachels 1975).

The sociological theory concisely introduced above was drafted long before the advent of social network sites or collaborative workspaces, but the concepts hold up well online. On social network sites, the user profile is the image someone presents to his environment, and it forms the basis for his interactions with the other members of the social network site. However, the image someone presents is often only directed at a certain audience (e.g. someone's closest friends), and may cause embarrassment when accessed by others. The theory behind context segregation and the risk of collapsing contexts form a powerful means to analyse the privacy issues in both social network sites and collaborative workspaces.

Another sociological perspective deals with the specific norms users of social software bring to the table. It was theorised that every social network comes with its own set of social norms (Tönnies 1965). Actions of members of these networks are based on assumptions about the norms that regulate the interactions. The mismatch between the user's expectation of social norms and the existing practices in a particular network or workspace could be another source of arising privacy issues.

The extent to which stakeholders in a network or workspace act in accordance with the normative expectations of other stakeholders forms a useful basis for analysis.

Adversaries

To structurally assess potential privacy threats, we have to establish what entities are exactly threatening the privacy of the users of social network sites and collaborative workspaces. Knowledge about the application and the available options to observe and control data flows differs depending on the type of adversary (Evans et al. 2004). Another aspect that needs consideration is whether it can be assumed that all parties 'play by the rules', i.e. only perform actions that they are allowed to do according to the technical protocols, social norms or legal rules. It is necessary to distinguish between privacy issues arising from authorised access to personal data (i.e. in compliance with the law, with social norms and/or with technical protocols) and access against these conditions (Schultz 2002). Examples of the latter are hacks of personal profiles, or use of offered services contrary to the conditions set out in the Terms of Use. In order to circumvent technical protocols, adversaries will need some computing expertise, whereas legal rules and social norms do not require any special knowledge or skills. Quite the opposite is the case, since violations of the law or social norms can also be unintentional and simply due to ignorance.

To structure our work, we define three types of adversaries which may infringe user privacy. These adversaries are:

- Third parties

Third parties are 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 and are therefore considered to have only minimal knowledge about the application and its members.

- Other users

Other users in the role of an adversary have an account for the collaborative workspaces or the social network site and a similar or higher level of legitimate knowledge about the application as third parties.

- Providers of the collaborative workspaces/social network site application

Providers of the collaborative workspaces or social network site are insiders with the most comprehensive insight in the application since they are the ones who are responsible for implementation, delivery and maintenance of the software.

Privacy issues in collaborative workspaces and social network sites

Since it is not possible to take into consideration all available social network sites and collaborative workspaces, we have done a detailed analysis of potential privacy issues in Wikipedia (Wikipedia 2008a) as a popular example of collaborative workspaces and Facebook (Facebook 2008a) as well known instance of a social network site. The following sections discuss similarities and differences with regard to privacy issues that we found for both applications, viewed from the perspective of the three different adversary types.

Privacy issues caused by third parties

On both platforms, Wikipedia and Facebook, it is quite simple for third parties to gain access to personal data without infringing the technical rules set out for the use of the systems. In the case of Facebook this is due to the settings which are applied by default and which are rarely customised by the user since users believe these are the optimal settings or they have no interest in privacy settings at all (Gross et al. 2005). For users of Wikipedia customisation is simply not foreseen by the application. As a result the general public is often allowed access to at least a limited set of personal information (a basic profile or the user page). These very open access control settings make it possible for third parties to collect information on individual users, which can be used for profiling purposes. The user-created content may also be lifted from the original context and combined into an overarching view of the individual, for which purpose an increasing number of so-called mashups are available. Mashups are a genre of interactive Web applications that draw upon content retrieved from external data sources to create entirely new services (IBM 2006). In this case, personal data publicised in different locations on the web may be brought together on one new web page. This use of personal information leads to the collapsing of contexts that was introduced in the section titled Sociological Perspective, which in turn may impede individuals to construct their identity differently for each separate context, thus causing privacy infringements. Third parties like tax authorities may also link publicly available information on social network sites to check information on tax returns (McDonagh 2008).

In Wikipedia, where due to the minimal access control options, each third party has access to user pages[1], the issue is not only limited to the confidentiality of personal data. Since third parties are also allowed to modify user pages from Wikipedia members, it also concerns the correctness and integrity of the published data on an individual's personal page. In addition it is easily possible to search for all articles, to which a user has contributed and therefore gain a good profile of his interests. It needs to be mentioned that Wikipedia does not require from people to have an account with username and password in order to contribute. However, it is also possible to search for all articles from the same IP address, which is stored if the contributor does not provide a registered username.

Besides legitimate access, third parties may also gain access to personal data though deceitful conduct, e.g. hacking the system's databases (e.g. Valleywag 2008). In both collaborative workspaces and social network sites, information collected by such means may cause severe privacy issues, ranging from embarrassment to identity theft, which affects many users. Security breaches at the root of these problems are similar for both platforms.

[1] User pages are special pages on Wikipedia, which allow each user to present himself to the community (cf. http://en.wikipedia.org/wiki/User_page).

Privacy issues caused by other users

Other users of Wikipedia and Facebook have at least the same potential to cause privacy issues as third parties. The issues identified in the previous section are therefore equally applicable when other users act as the adversaries. Many privacy issues can be traced back to the out-of-context use of personal data. On Facebook the impact of these infringements is generally higher when trusted contacts are involved, since these normally have legitimate access to more personal data than the general public. It holds true for both platforms, that even when all technical rules are respected, the lack of enforceability of social norms concerning the publication of personal information in other, unsolicited contexts lays at the root of these privacy issues. Legal provisions attempting to stem these privacy issues, e.g. the prohibition to use fake identities when constructing social network site profiles, are hard to uphold in practice.

The interactions between users, however, lead to some other potential privacy issues. In both example applications it is possible to leave remarks or comments on the personal site of other members (the so-called Wall on Facebook, user pages on Wikipedia). On Wikipedia it is even possible to create a new public article about an individual as central topic (e.g. Wikipedia 2008b). Some control of the information flow is relinquished to other people and can lead to the result that unwelcome information generated by other users is shown to the public. An example of this are third parties trying to gain access to private information through other users on social network sites. When someone installs an application as an add-on to his profile, it may harvest data from the available network, even without the concerned user being aware. The application may be granted rights to access profile information when installed. Such an application acquires the privileges of the profile owner and can query personal information of the user and members of the user's network (Felt and Evans 2008).

Concerns regarding the confidentiality, correctness and integrity of personal data have already been discussed in the previous section for the example of Wikipedia, and is also appropriate for social network sites when other users are considered as potential adversaries.

Both applications do not request any proof of identity for registration, which provides users with some anonymity, but on the other hand enables malicious users to perform social engineering attacks by creating an account with false data. By pretending to be someone else, e.g. a friend or a relative of the target, it opens ways to spoof out personal data from members of Facebook or Wikipedia. Further, it is possible to compose embarrassing contributions under the name of someone else in both applications.

Privacy issues caused by providers

Although the Facebook user can regulate which other users have access to personal information, the platform provider is omnipotent in this respect. In both examples the providers of the platform have full access to user data, regardless of any privacy settings. There are no technical obstacles barring them from access to user information. From a legal perspective, while posting information on Facebook and on Wikipedia, the user in both cases grants license for further use of the personal and content data to others as clearly stated in the Terms of Use. In the case of Facebook, the provider is allowed to utilize this information as they see fit (Facebook 2008c) whereas all data on Wikipedia are licensed under the GNU Free Documentation License (Wikipedia 2008c). This means not only providers, but anybody is allowed to re-use this data as long as the result is also put under the same license. In both cases the user agrees to share his personal data at least with the provider and maybe with further parties as well. However, the presentation of the personal data is different. Facebook requires an account, through which individuals have to provide some personal data in a structured, predefined format. Users of Wikipedia get their own user page per default, however it is completely up to them which data they provide and how they present this information. Thus, automated evaluation and further processing of users' personal data is easier in the case of Facebook than in Wikipedia. Besides, providers of both platforms have insight to technical information about their users, such as IP address, operating system, browser version, particular pages someone has visited, etc.

Social norms are currently the only forces effectively delimiting the unabridged use of personal information. When these norms are not respected, users perceive this as a breach of privacy. A good example of this is Facebook's use of Beacon, technology collecting information about the use of certain commercial websites which is relayed back to Facebook (Facebook 2008b). A public outcry of privacy advocates and negative press coverage (e.g. Malik 2007, wikiHow 2008) led Facebook to the decision to review its position (Zuckerberg 2007). Effectively, the social pressure from the public and the risk of popularity loss are interlinked and may restrain platform providers to extensive use of personal information in commercial settings.

Conclusion on similarities and differences concerning privacy issues

The main conclusion from the previous sections is that both collaborative workspaces and social network sites suffer from the same potential privacy issues. Both types of platform store a mix of personal data and content, where the balance between these two is mainly dictated by the goal and actual use of the system. Third parties and other users have comparable means to access personal information of platform users, which are technically only restricted by the limitations imposed by the system and the access control settings that have been established.

The access to personal data that the providers enjoy thanks to their direct access to the supporting systems is essentially the same for collaborative workspaces and social network sites. In short, platform providers have full access, assuming that the social network site or collaborative workspaces are realised as a client-server application, which is the case for today's popular applications. The subsequent use of the available information for new purposes is only limited by self-imposed norms on behalf of the provider. Effective technical and legal means to limit provider data access are virtually absent.

Access to personal information that contravenes the established rules—be they technical, legal, or social—is also similar between collaborative workspaces and social network sites. Breaking technical access restrictions (also known as hacking) is possible on both platforms, just like the infringement of legal constraints surrounding the use of the applications. Social phenomena cause most privacy issues: information originally presented in one context that is presented in a new, unintended context form a large portion of all privacy intrusions. Especially when the norms of people divulging information and parties using information do not match up, the perceived impact on privacy can be substantial.

After having concluded that similar privacy issues exist in both collaborative workspaces and social network site, the question remains what the differences are. The prime difference is caused by the design and use of the systems, for which we refer back to Table 1. The focus of collaborative workspaces is the management and manipulation of content whereas social network sites primarily provide management of user profiles and connections. Therefore, collaborative workspaces contain much less isolated personal data items than social network sites, where it is a key feature for users to build up an own profile with much well structured personal information. The bulk of information in collaborative workspaces is content, which also may contain personal data; however this data is less structured and requires semantic analysis for extraction. It is therefore easier to collect users' personal data automatically from social network sites than from collaborative workspaces.

Finally, the analysis of the two example applications demonstrated differences in the currently available user-determined access control settings. The fewer means of access control are available, the more adversaries have opportunities to cause privacy issues.

Suggested improvements

Because of the high degree of similarity between the privacy issues originating from the use of both collaborative workspaces and social network sites, it is likely that a number of potential improvements will be applicable to both platforms. This section discusses a number of potential improvements that help to mitigate a number of privacy issues in collaborative workspaces and social network sites.

Technical improvements

Technical instruments are the only means that cannot be simply ignored or violated accidentally as may happen with social norms and legal rules. The improvements suggested below aim to limit the possibilities adversaries have to gain access to information without compromising technical security measures. Possible solutions include—but are not limited to—the following mechanisms and protocols.

- **Fine-grained, user-determined access control policies** to enable users as owners of their data to define who can access what personal data (e.g. Franz et al. 2006).
- **Group encryption** to prevent access from anybody outside the group (e.g. Camenisch and Damgard 2000).
- **Open source peer-to-peer networks** to prevent all data being stored on a central server under the control of one provider (e.g. Noserub 2008).

- Allow **use of multiple pseudonyms** to enable some level of unlinkability for users between different contexts (cf. Pfitzmann and Koehntopp 2001).
- **Digital signatures** to ensure the integrity of personal data and the authenticity of the sender (cf. Chaum 1985).

Social improvements

Although technical and cryptographic measures can serve to form a security baseline, they come along with constraints for primary functions and convenience of use. In social network sites and collaborative workspaces many privacy issues have non-technical causes, i.e. adversaries disregard social norms—by accident or intentionally. Especially since there is growing evidence that users will not use technical security measures if these hamper the full social use of the applications (Grimmelmann 2009), we also have to look at social improvements, which are outlined in short in the following.

- Awareness

Often users are not aware of the pervasiveness of information entrusted to social network sites and collaborative workspaces. Increasing users' awareness of these issues is an option to be considered. Numerous methods may be employed here, ranging from classroom based education efforts to online tools visually presenting the unabridged flow of information through online networks and workspaces.

- Social norms

As we have seen one of the main causes for privacy issues is that personal information from one context is shifted to a new context without the consent of the user. On top of that, the user has lost control of the use of her personal information in this new context, quite often because she is not even aware of the information shift. There is a distinct lack of shared social norms concerning the acceptability of the use of personal information in new contexts. It will be a challenge to facilitate the forming and the acceptance of social norms in collaborative workspaces and social network sites. The Wikipedia community denotes a good example for the development of social norms in collaborative workspaces. Having no rules before 2001, the community since then discussed and introduced a set of policies and guidelines that serve as standards or advisory, respectively (Wikipedia 2009).

Legal improvements

Until today, legal instruments have been at the core of privacy protection measures that govern social network sites and collaborative workspaces. The user has to agree with the Terms of Use at the moment of initial registration. In practice, however, these legal provisions are incomprehensible to the average user.

Instead of only focusing on the legal framework presented by the platform provider for improvements, it may be worthwhile to explore the wider legal landscape in addition. Intellectual property legislation, portrait rights or general privacy protection legislation may serve as alternative bases to prevent privacy issues in the future.

Conclusions and future work

This paper compared Wikipedia as an example of a collaborative workspace and Facebook as an example of a social network site. Similarities and differences concerning privacy issues of both social software applications have been identified. In general, the issues we have found arise mainly due to collapsing contexts, i.e. users' personal data used in contexts other than the original and intended one. The finding that social software lacks fine-grained and user-determined access control options aggravates this source of privacy issues.

Serious privacy issues are not only the result of the breach of technical implementations, but may also be brought about through the disregard of social norms and legal provisions. Therefore we conclude that solutions to address privacy issues in social software can neither be only technical, nor only legal, nor only based on upholding certain social norms: it is necessary to find a comprehensive approach. A combination of all three areas is needed in order to improve privacy protection on the one hand without losing important functionalities on the other hand, whilst safeguarding the social usability of the application for the average user. These aspects are considered by the PrimeLife project (PrimeLife 2008) and will be topic of our future research.

Acknowledgements The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007–2013) under grant agreement no. 216483 (PrimeLife 2008).

References

Agre PE, Rotenberg M. Technology and privacy: The new landscape. MIT; 1997.

boyd dm, Ellison NB. Social network sites: Definition, history, and scholarship. In: Journal of Computer-Mediated Communication, 13(1), October 2007, article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (last access 17 October 2008).

Camenisch J, Damgard I. Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes. In: Okamoto T, editor. Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (December 03–07, 2000). Lecture Notes In Computer Science, vol. 1976. London: Springer-Verlag; 1976. pp. 331–345.

Chaum D. Security without identification: transaction systems to make big brother obsolete. Commun. ACM 28. 1985;10:1030–1044.

Evans S, Heinbuch D, Kyle E, Piorkowski J, Wallner J. Risk-based systems security engineering: stopping attacks with intention. In: Security & Privacy 2(6), December 2004, pp. 59–62.

Facebook (2008a), http://www.facebook.com (last access 15 September 2008).

Facebook (2008b), Business Solutions. http://www.facebook.com/business/?beacon (last access 15 August 2008).

Facebook (2008c), Terms of Use. http://de-de.facebook.com/terms.php?ref=pf (last access 30 October 2008).

Felt A, Evans D. Privacy protection for social networking platforms. In: Proceedings of W2SP 2008: Web 2.0 Security and Privacy.

Franz E, Wahrig H, Boettcher A, Borcea-Pfitzmann K. Access control in a privacy-aware eLearning environment. In: Proceedings of the First International Conference on Availability, Reliability and Security (April 20–22, 2006). ARES. IEEE Computer Society, Washington, DC, 879–886.

Goffman E. The presentation of self in everyday life. Garden City, New York: Doubleday Anchor Books; 1959.

Grimmelmann JT. Facebook and the social dynamics of privacy. In: Iowa Law Review 95(4), May 2009, to appear. http://ssrn.com/abstract=1262822 (last access 17 October 2008).

Gross R, Acquisti A, Heinz HJ. Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. ACM, New York, NY, November 2005, pp. 71–80.

Hogben G. Security issues and recommendations for online social networks. Position paper, ENISA, European Network and Information Security Agency, October 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf. (last access 12 September 2008).

Hyves (2009), http://www.hyves.nl (last access 4 June 2009).

IBM (2006), 'Mashups: The new breed of Web app.' http://www.ibm.com/developerworks/library/x-mashups.html (last access 8 April 2008).

LinkedIn (2009), http://www.linkedin.com (last access 4 June 2009).

Malik O. (2007), 'Is Facebook Beacon a Privacy Nightmare?' http://gigaom.com/2007/11/06/facebook-beacon-privacy-issues (last access 10 June 2008).

McDonagh P. (2008), 'Taxman admits to facebook 'trawl'.' http://www.independent.ie/national-news/taxman-admits-to-facebook-trawl-1297118.html (last access 8 August 2008).

MySpace (2009), http://www.myspace.com (last access 4 June 2009).

Norberg PA, Horne DR, Horne DA. The privacy paradox: Personal information disclosure intentions versus behaviors. In: Journal of Consumer Affairs, 41(1), 2007, pp. 100–126.

Noserub (2008), http://noserub.com (last access 21 October 2008).

Oomen IC, Leenes RE. Privacy risk perceptions and privacy protection strategies. In: Fischer-Hübner S, editor. Proceedings of IDMAN'07–IFIP WG 11.6 working conference on Policies & Research in Identity Management, October 11–12, 2007, pp. 121–138.

Pankoke-Babatz U, Syri A. Collaborative workspaces for time deferred electronic cooperation. In: Proceedings of the international ACM SIGGROUP Conference on Supporting Group Work: the Integration Challenge, November 16–19, 1997, pp. 187–196.

Pfitzmann A, Koehntopp M. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In: Federrath H, editor. Proceedings Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009. Springer Verlag, Berlin, 2001, pp. 1–9.

PrimeLife (2008), http://www.primelife.eu (last access 30 October 2008).

Rachels J. Why privacy is important. In: Philosophy and Public Affairs, 4(4), 1975, pp. 323–333.

Richter A, Koch M. Social software—Status quo und Zukunft. Technischer Bericht Nr. 2007-01, Fakultät für Informatik, Universität der Bundeswehr München, February 2007.

Schmidt J. Social Software: Onlinegestütztes Informations-, Identitäts- und Beziehungsmanagement. In: Forschungsjournal Neue Soziale Bewegungen, 19(2), 2006, pp. 37–47.

Schultz EE. A framework for understanding and predicting insider attacks. In: Computers & Security. 21 (6), 2002, pp. 526–531.

Tönnies F. Einführung in die Soziologie. Stuttgart: Ferdinand Enke Verlag; 1965.

Valleywag (2008), 'Paris Hilton, Lindsay Lohan private pics exposed by Yahoo hack' http://valleywag.com/5012543/paris-hilton-lindsay-lohan-private-pics-exposed-by-yahoo-hack (last access 13 August 2008).

wikiHow (2008), 'How to Block Facebook Beacon.' http://www.wikihow.com/Block-Facebook-Beacon (last access 10 June 2008).

Wikipedia (2008a), http://en.wikipedia.org (last access 6 August 2008).

Wikipedia (2008b), 'Seigenthaler incident.' Version of 20 May 2007, 21:08. http://en.wikipedia.org/w/index.php?title=Seigenthaler%20%20controversy&oldid=132296396 (last access 17 July 2008).

Wikipedia (2008c), 'Editing GNU Free Documentation License.' http://en.wikipedia.org/w/index.php?title=GNU_Free_Documentation_License&action=edit (last access 30 October 2008).

Wikipedia (2009), 'Policies and Guidelines.' http://en.wikipedia.org/wiki/Wikipedia:Policies_and_guidelines (last access 19 March 2009).

Wong R Social Networking: Anybody is a Data Controller! Nottingham Law School, UK, revised version October 2008. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668 (last access 27 October 2008).

Zuckerberg M (2007), 'Thoughts on Beacon. The Facebook Blog', 5 December 2007. http://blog.facebook.com/blog.php?post=7584397130 (last access 10 June 2008).