A Digital Rights Management approach to privacy in online social networks

Eva Rodríguez, Víctor Rodríguez, Anna Carreras, Jaime Delgado

Universitat Politècnica de Catalunya (UPC)
Jordi Girona 1-3, E-08034 Barcelona, Spain
{evar, victorr, annac, jaime.delgado}@ac.upc.edu

Abstract. Information shared in online social networks is subject to privacy policies specified in each network. These privacy terms protect users to some extent and grant them some basic rights on the information they share. In the near future, and according to the Web 2.0 philosophy, social networks members will be able to choose their privacy preferences more richly, and perhaps with techniques derived from existing Digital Rights Management (DRM) principles. Moreover, the protection and governance DRM provides may improve the enforcement of the current policies, which currently are imperfectly executed.

Keywords: Privacy, social networks, information sharing.

1 Introduction

It is not new the observation that protocol rules in human relationships become more complex in densely populated societies –take the Japanese one as an example– where close human contact is more frequent and not easily avoidable. This has been said to be a mechanism to preserve an intimacy circle behind the formalism. The Internet Age and its ultimate hit, the Web 2.0, have brought closer than ever human interaction, and have set up an expression means –the internet social networks– where one´s information is potentially available for all in a planetary scale. While still its formality may be rude because it is still in its infancy, it looks reasonable to think that more refined interaction procedures will appear before sharing or accessing user generated information.

Currently, members of internet social networks can decide to some extent which part of the information they publish is available to others –and to whom–, but they implicitly accept that the social network provider could make some use of it – perhaps to allow marketers to send personalized advertising. Social network members are not always aware of the potential extension of the information they share but consciousness of its dangers will probably root in internet users in a near future. The expression of the scope and the audience definition of the shared information will probably be refined and converge among the different social networks.

As a first step, social networks provide a privacy policy page always in their sites – and almost always accessible from a link in the bottom line of the welcome webpage-,

but this narrative expression should evolve –just as CreativeCommons symbols replaced verbose texts in copyright statements in web resources. With the time, users will perhaps express their privacy preferences in a standardized way too, across the different social networks.

Today, the privacy page in the social network web sites looks like the transposition of a narrative contract clause from a text paper to a webpage, but this arrangement sounds artificial. As new technology changes both the content and the expression forms, an electronic counterpart of the privacy statement is likely to appear. This paper shapes some hints on which direction may these changes point, which we believe have relationship with the way information is managed in Digital Rights Management systems.

All the information the user gives, including the one the user provides consciously and the one that is picked up by the servers (time and location of connection, browsing habits, etc.) is liable to be protected. The latter is sometimes referred as "use data", and has great economic value, but this paper will focus on the information the user shares intentionally.

2 Current privacy policies in social networks

Most of social networks have acknowledged the importance of the privacy policies they follow. This concern initially came from the fear of the site owners of suffering legal prosecution, but later on they acquired the consciousness that an unpopular policy might erode their public image. This is the case of Facebook, when it intended to change the terms of service to retain in perpetuity the rights on published images and other data: soon after Facebook had to retract due to the noisy controversy that was arisen[1]. This concern of the site owners has materialized in the neat clarification of the privacy policies, which has to be read and acknowledged by the network members –at least in theory- when registering for the first time. The way these terms are presented has also changed, passing from an initial small-font semi-hidden privacy disclaimer to a well visible and explained policy terms.

To assess an outlook of the social network current privacy policies, some networks have been chosen and their terms analyzed. Table 1 shows the most relevant generalist social networks, according to the web traffic ranking provided by Alexa[2]:

Table 1. Top general social networks

Network	Ranking in Alexa
Facebook	4
MySpace	11
Hi5	33
Twitter	36
Orkut	41

[1] "*Facebook Withdraws Changes in Data Use*", The New York Times online, 19 February 2009

[2] This information fluctuates daily. Data was considered as of 2nd of June 2009 available from http://www.alexa.com/topsites

Other topic-oriented social networks take relevant positions in this ranking, like LinkedIn focused on professional profiles (96th in the ranking) Flickr for the photographs exchange (30th in the ranking) or movies recommendations sites, but they essentially share the features with generic-oriented networks.

The privacy issues derived from the four wikinomics principles identified in the next section of the paper are addressed most satisfactorily, at least in theory.

Open protocols are not actually followed, although some of the sites allow the user to export their profile data as RDF data (using FOAF, with the well known Friend-Of-A-Friend elements). Furthermore, audit trails, monitoring and enforcement are granted by the seal of the TRUSTe group in two of the five analyzed networks (Facebook and MySpace). TRUSTe certifies the compliance of the sites with the EU Directive on Data Protection (the Directive prohibits the transfer of European citizens' personal data to companies in doubtful non-European Union nations). The TRUSTe seal grants that a site satisfies the seven "Safe Harbor Privacy Principles", the framework agreed by US and EU to qualify companies to share information across US and EU. This quality distinction has been accused, however, of being useless given that once conceded it is not promptly removed upon changes in the company policies.

Current social networks allow users to specify quite richly who is able to access their personal data –and which data. This specification can be given in terms of all/nobody but also with more nuances: some information may be visible to other members, or to the some of the other members (those who belong to groups, to the group of friends, to the group of "friends of my friends", etc.). The implementation of this privacy policy seems to be in general in the good course.

Worldwide privacy policies standardization is still missing, but this would help the work of the social network owners in order to improve privacy. In any case, whenever something similar to a standard has been made available (Safe Harbor Privacy Principles, or the Children's Online Privacy Protection Act), they seem to have adopted it diligently. Going beyond, social network providers have agreed on self-regulating themselves, as it can be seen in the declaration approved a few months ago by some of the social network providers in Europe[3]. This good situation in theory is less perfect in practice, so there is still the need for new standardization initiatives easier to implement.

For example, technical protection measures are given by the site owners as a grace, and none of them takes responsibility to grant their perfect functioning. Thus, each of these networks is liable to suffer virus attacks and data theft and no responsibility is taken –at least according to the policy terms they publish, given that judges may say different.

Secondly, the execution of some user rights is not immediate and requires a human intervention which might delay fatally its effectiveness. Currently, millions of photographs are being uploaded daily, and in most of them some other people appear different from the person that is making the upload and of course has not been given any consent.

[3] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Thirdly, the terms of privacy also unanimously reflect the exceptions provided by governmental interventions[4]. As long as it is not forbidden, information dumped on social networks may appear encrypted or hidden with steganography techniques. Naturally, this goes against the interest of marketers and site owners are not willing to provide help to the users in this respect.

Some of these privacy flaws might have been avoided with mere technological measures. Information management strategies derived from those already existing in DRM (Digital Rights Management) systems may fix them. Thus, automatic complaint management and preventive deletion as default policy may have worked for some cases or data encryption might prevent state intromission in the citizens' private life.

3 Privacy in the Web 2.0

As already pointed out, the success of online networking sites during the last years has resulted in a considerable increase of the amount of data that users of these sites share and social networking applications manage. In this context, a key issue is to assure privacy to personal information, i.e. personal data and contents, on online social networking sites. During the FDIS/IFIP workshop session on "Privacy and identity in social networks and online communities" [1], it was discussed if traditional privacy approaches were suitable to assure privacy for personal data in social networking sites. Traditional privacy approaches focus on protection and disguise user's identity information. It was agreed that a new approach is needed for privacy in the Web 2.0, giving more control to users.

Different models and principles have been elaborated to define Web 2.0 dynamics, for example the Web 2.0 Meme Map [2] or the Wikinomics [3]. The principles of the later one are: Openness, Peering, Sharing and Acting Globally (see Table 2).

Table 2. Wikinomics principles

Principle	Description
Openness	In online social networking sites, personal data is exchanged and processed openly in applications based on open standards
Peering	Users determine the success or failure of the online social networking site, since these sites are self-organised by a group of individuals.
Sharing	Users of online social networking sites will share data with others.
Acting globally	Individuals act globally in the new global platform for collaboration that provides the Web 2.0

[4] With or without judge authorisation: claiming to protect America in the cyberspace, President Obama announced the creation of a military agency (the "Cyber Command") to patrol the Internet in the war against terror (CNN online, "*Obama creates top job for guarding online security*", May 29, 2009).

For each one of these principles a set of privacy research questions raised during the workshop, and the set of technologies and methods that can help to solve privacy issues were identified. Table 3 summarizes the principle, privacy issues related with the principle and technology or method under consideration.

Table 3. Privacy issues in online social networks

Principle	Privacy issues	Technologies
Openess	Privacy measures needs to assure authorised usage and accountability for the data	Audit trails Monitoring Enforcement
Peering	Individuals should be provided with solutions to determine the usage of their personal data	DRM techniques Policies
Sharing	Individuals should be able to determine who use/access to their data and under which conditions. Privacy safeguarding measures will associate usage rights to personal data.	Semantic web technologies Techniques from DRM solutions Watermarking
Acting globally	It is required future technology and privacy standards to work on a common ground.	Sticky policies Future privacy standardization initiatives

Although we are focussing on all these four principles in our research around online social networks, the rest of this paper presents a first insight into the Sharing principle and how DRM solutions may help to improve privacy. With this purpose, section 4 introduces the relevant DRM aspects, while section 5 points out some possible solutions.

4 DRM Systems

Current Digital Rights Management systems can manage digital assets in a controlled way, and according to the terms imposed by the content creators [5]. Web-based social networks do certainly manage content –user generated content– but do not attain all the goals achieved by DRM systems.

DRM systems enable the creation, adaptation, distribution and consumption of multimedia content according to the permissions and constrains imposed by content creators and rights issuers –much as it should be in information released on social networks. There are different initiatives, standard and proprietary, that specify a DRM system or the elements that usually form these systems. The elements that participate in a DRM system, compared to their counterparts in social network sites, are:

- **Digital objects**. The digital objects creation process involves the combination of the protected digital assets with associated metadata to create digital objects that include the usage rules, information regarding the

protection tools and other data as the creator of the asset, etc. User generated content in social networks does not differ from intellectual property protected content exchanged in DRM platforms, but tools to create content and to include usage rules are normally not provided.

- **Rights expressions**. Rights expressions govern digital assets through the complete digital value chain in DRM systems. They are presented to the different actors of the value chain as XML files, usually called licenses, which are expressed according to a specific and rich Rights Expression Language (REL). Licenses also can hold protection information, such as the keys needed to decipher the digital content. Licenses are usually digitally signed to ensure the integrity and authenticity of their content, and sensitive data within them is usually encrypted. In social networks, users can, in the best case, specify which is the intended audience (none, all, friends, friends of a friend, etc.), but cannot normally express their restrictions with conditions as it is possible with a REL.
- **Rights enforcement**. DRM systems have to guarantee that license terms governing digital assets are respected by the users of the digital value chain. For this reason, authorization tools are an important element of a DRM system. These license based authorization tools verify if a user has a license that grants him the right to perform the operation he is trying to exercise and if he fulfils the conditions specified within the license. In social networks, everything relies in the confidence the user has on the social network provider. His overall satisfaction of the enforcement is only vaguely granted by external audits.
- **Intellectual Property Protection Tools**. Different protection techniques are used by DRM systems. Usually, digital assets are protected using encryption and scrambling techniques, while other techniques as watermarking or fingerprinting are used for tracking or verification purposes. Usually, the information about the tools used to protect digital resources is associated to them in the digital objects creation process. Social networks do not provide protection tools, since in most cases they assume they are not needed.
- **Notification of Events**. Some participants of the distribution chain, as content creators or distributors, could want to monitor usage of their copyrighted material. Therefore, some mechanisms will be necessary to allow systems to share information about events referred to multimedia content and peers that interact with the content. Social networks provide only residual information on events: it is not always possible to track who has seen a picture, but at least in some of them it is possible to know how many people have seen it.
- **DRM players**: They consume digital objects according to the terms and conditions specified in the associated licenses. Then, DRM players make use of license based authorisation tools that resolve if users are authorized to consume digital assets. If the user is authorized, then the content is deciphered and rendered. Typically, DRM players have a secure local repository for the storage of licenses, protection information, offline operations reports and other critical data. Nearly the only way of rendering user generated content in social networks is browsing the social network site.

However, richer possibilities are open given that the APIs that these sites provide may eventually allow the construction of content players independent of the social network website. If enforcement techniques are to be applied, this could be integrated in a new site embedded player or in some software created through the available APIs.

5 DRM and personal data property rights

Online social networks have built their business models on the personal data that users freely share with others. This implies an increasing privacy risk on online social networking applications managing user's personal data. New privacy challenges and risks in the Web 2.0 have been studied in [1].

From the different privacy research questions in the context of online social networks addresses in [1], in this paper we are focussing on the Sharing principle and we take the personal data property rights privacy approach. For this purpose, we have analysed how to manage user's personal data in the Web 2.0 using current DRM techniques.

Sharing in online social networks means that users want to share data with other users. Currently, service providers make available collaborative tools to users for sharing data. However, in some cases, users cannot state the terms under which they want to share their data, for example only with a particular group of users and under certain conditions. In this scenario, privacy safeguarding measures need to associate usage rights to user's personal data to determine the conditions of use of this sensitive content. Current DRM technologies can help in providing this functionality, since licenses expressed according to a REL can be used to determine the terms and conditions under which user's data can be used by others. A license conveys to an entity the sanction to exercise a right against a resource, if the set of conditions previously specified within the license are fulfilled. In an online social network, users can use licenses to control the usage of their personal data and contents. Then, if Bob, a user of the social network, wants to share his contents only with some of his friends, he will be the issuer of the license. The principal to which rights are granted will be the friends that Bob has determined, the right of the license will be the view right, the resource for example the photos of Bob's last album.

On the other hand, sensitive personal data also needs to be protected, e.g. encrypted or access-controlled, to ensure that license terms are enforced. Another important component of DRM systems are the license based authorization tools, which prove if a user has the appropriate permissions to perform the operation they are requesting, i.e. an action against a digital resource. In an online social network, authorization tools will solve if the users of the network can view, edit, etc. personal data of other users of the social network.

Finally, event reporting techniques can help on the generation of personal data usage reports. Notification of events is an important part of a DRM system, since systems using event reporting mechanisms allow to content creators and distributors of multimedia content to be informed of the usage of the multimedia objects they have provided. By means of the chain of licenses defining the contractual

relationships between the actors of the value chain, they could be informed of the use of the content that they have created, adapted, distributed, etc. Afterwards, users illegally distributing content could be prosecuted by means of these activity records. MPEG-21 Event Reporting [4] standard provides a standardised means for sharing information about events amongst peers and users. Such events are related to multimedia content and peers that interact with them. In an online social network, event reporting tools can help users to monitor the usage of their personal data. In this way, they can determine if any other user of the network is using or distributing private data illegally.

4 Conclusions

This paper has presented a number of relevant issues about the sharing of information in social networks and its privacy.

We have analyzed the privacy policies of current platforms (such as Facebook or MySpace) to finally conclude that the use of Digital Rights Management (DRM) is suitable for protecting personal data in this scenario.

In the new Web 2.0 environment, we have used the four principles defined by the Wikinomics to identify specific privacy issues and the corresponding required technologies. In particular, after describing all the elements involved in a DRM system, the paper presents how licenses and Event Reporting could be used to improve privacy when sharing information in social networks.

5 Acknowledgments

This work has been partially supported by the European Commission IST FP6 program (VISNET II Network of Excellence, IST-2005.2.41.5) and partially by the Spanish government (MCM-LC project, TEC 2008-06692-C02-01).

6. References

1. Weiss, S.: The Need for a Paradigm Shift in Addressing Privacy Risks in Social Networking Applications. In IFIP International Federation for Information Processing, vol. 262, pp. 161–171. Springer Boston. (2008)
2. O'Reilly, Tim.: What is Web 2.0? – Design Patterns and Business Models for the Next Generation of Software. The Web As Platform. O'Reilly Media Inc. (2005).
3. Tapscott, D., Williams, A.: Wikinomics – How Mass Collaboration Changes Everything. Portfolio. (2006)
4. ISO/IEC, ISO/IEC IS 21000-15 – Event Reporting.
5. Delgado, J., Rodríguez, E.: Digital Rights Management Technologies and Standards. In Interactive Multimedia Music Technologies, pages: 249-283, Information Science Reference, New York, USA (2007).